

JP1 Version 13

JP1/Base User's Guide

3021-3-L09(E)

Notices

■ 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*.

JP1/Integrated Management 3 - Manager (for Windows):

P-2A2C-8EDL JP1/Integrated Management 3 - Manager 13-00

The above product includes the following:

P-CC2A2C-9MDL JP1/Integrated Management 3 - Manager 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (for Windows 10, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 11)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC2A2C-6LDL JP1/Base 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC842C-6LDL JP1/Base 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

JP1/Automatic Job Management System 3 - Manager (for Windows):

P-2A12-3KDL JP1/Automatic Job Management System 3 - Manager 13-00

The above product includes the following:

P-CC2A12-4KDL JP1/Automatic Job Management System 3 - Manager 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC2912-39DL JP1/Automatic Job Management System 3 - Web Console 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC8412-39DL JP1/Automatic Job Management System 3 - Web Console 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC2A12-3NDL JP1/Automatic Job Management System 3 - Print Option Manager 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC2A2C-6LDL JP1/Base 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

JP1/Integrated Management 3 - Manager (for Linux):

P-842C-8EDL JP1/Integrated Management 3 - Manager 13-00

The above product includes the following:

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9)

P-CC9W2C-9MDL JP1/Integrated Management 3 - Manager 13-00 (for SUSE Linux 12, SUSE Linux 15)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (for Windows 10, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 11)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC2A2C-6LDL JP1/Base 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC842C-6LDL JP1/Base 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

JP1/Automatic Job Management System 3 - Manager (for Linux):

P-8412-3KDL JP1/Automatic Job Management System 3 - Manager 13-00

The above product includes the following:

P-CC8412-4KDL JP1/Automatic Job Management System 3 - Manager 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC2912-39DL JP1/Automatic Job Management System 3 - Web Console 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC8412-39DL JP1/Automatic Job Management System 3 - Web Console 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC8412-3NDL JP1/Automatic Job Management System 3 - Print Option Manager 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC842C-6LDL JP1/Base 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

JP1/Automatic Job Management System 3 - Agent (for Windows):

P-2A12-33DL JP1/Automatic Job Management System 3 - Agent 13-00

The above product includes the following:

P-CC2A12-43DL JP1/Automatic Job Management System 3 - Agent 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

P-CC2A2C-6LDL JP1/Base 13-00 (for Windows Server 2016, Windows Server 2019, Windows Server 2022)

JP1/Automatic Job Management System 3 - Agent (for AIX):

P-1M12-33DL JP1/Automatic Job Management System 3 - Agent 13-00

The above product includes the following:

P-CC1M12-43DL JP1/Automatic Job Management System 3 - Agent 13-00 (for AIX)

P-CC1M2C-6LDL JP1/Base 13-00 (for AIX)

JP1/Automatic Job Management System 3 - Agent (for Linux):

P-8412-33DL JP1/Automatic Job Management System 3 - Agent 13-00

The above product includes the following:

P-CC8412-43DL JP1/Automatic Job Management System 3 - Agent 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC842C-6LDL JP1/Base 13-00 (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

■ Trademarks

HITACHI, HiRDB, Job Management Partner 1, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

AIX is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

AMD is a trademark (or registered trademark) of Advanced Micro Devices, Inc.

IBM is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

Intel is a trademark of Intel Corporation or its subsidiaries.

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

Microsoft is a trademark of the Microsoft group of companies.

Microsoft, Active Directory are trademarks of the Microsoft group of companies.

Microsoft, Internet Explorer are trademarks of the Microsoft group of companies.

Microsoft, Visual C++ are trademarks of the Microsoft group of companies.

Microsoft, Windows are trademarks of the Microsoft group of companies.

Microsoft, Windows Server are trademarks of the Microsoft group of companies.

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

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

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

UNIX is a trademark of The Open Group.

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

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation	Full name or meaning
Microsoft Cluster Server	Microsoft(R) Cluster Server
Microsoft Internet Explorer	Microsoft(R) Internet Explorer
	Windows(R) Internet Explorer(R)
Visual C++	Microsoft(R) Visual C++(R)
Windows 10	Windows(R) 10 Enterprise 64-bit
	Windows(R) 10 Home 64-bit
	Windows(R) 10 Pro 64-bit
Windows 11	Windows(R) 11 Enterprise
	Windows(R) 11 Home
	Windows(R) 11 Pro
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
	Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	Microsoft(R) Windows Server(R) 2019 Datacenter
	Microsoft(R) Windows Server(R) 2019 Standard
Windows Server 2022	Microsoft(R) Windows Server(R) 2022 Datacenter

Abbreviation	Full name or meaning
	Microsoft(R) Windows Server(R) 2022 Standard

Windows is sometimes used generically, referring to Windows 10, Windows Server 2016, Windows Server 2019, Windows Server 2022 and Windows 11.

■ Restrictions

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

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

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

■ Edition history

Jun. 2023: 3021-3-L09(E)

■ Copy right

Copyright (C) 2023, Hitachi, Ltd.

Copyright (C) 2023, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-L09(E)) and product changes related to this manual.

Changes	Location
<p>The following OSs were added to the supported OSs:</p> <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2022 • Red Hat(R) Enterprise Linux(R) Server 9 (64-bit x86_64) • Oracle Linux(R) Operating System 9 	--
<p>The following OSs were deleted from the supported OSs:</p> <ul style="list-style-type: none"> • Windows(R) 10 Enterprise 32-bit • Windows(R) 10 Home 32-bit • Windows(R) 10 Pro 32-bit • HP-UX 11i V3 (IPF) • Solaris 11 (SPARC) • Red Hat(R) Enterprise Linux(R) Server 6 (64-bit x86_64) • Oracle Linux(R) Operating System 6 (x64) • CentOS 6 (x64) • CentOS 7 • CentOS 8 	--
<p>The following functions were removed:</p> <ul style="list-style-type: none"> • JP1/SES compatibility function • SNMP trap conversion function <p>As a result, descriptions pertaining to the abovementioned functions were also deleted or changed.</p>	--
<p>A description of the procedure used to select JP1/Base included with media provided for JP1/AJS or JP1/IM was added to the description of the JP1/Base installation procedure (for Windows).</p>	3.2.1
<p>A precautionary note when overwriting an install of JP1/Base version 13-00 or later over a 12-50 or earlier version of JP1/Base was added.</p>	3.2.3(5) , 3.3.4(5)
<p>Explanations of the following items were added, and a description assuming the use of such in 2038 and later was provided:</p> <ul style="list-style-type: none"> • Enabling big timestamps when running in Linux • Preventing the ability to start command execution services • JP1/Base startup process definition file 	3.3.4(9) , 7.1.1 , 7.2 , Appendix A.1 , Appendix A.2
<p>UTF-8 was added as an English encoding available for use in Linux.</p> <p>The following files were added to the JP1/Base definition files:</p> <ul style="list-style-type: none"> • Character code mapping definition file • Language type mapping definition file <p>As a result, an additional procedure was added for changing the character code and language type mapping definition after installing an upgraded version of the software.</p>	3.4.2 , 3.4.2(3) , Appendix A.2
<p>The use of ECC-encrypted server certificates for SSL communication was enabled.</p> <p>As a result, the description on how to create a private key was changed as part of the setup procedure for establishing an SSL communication environment on the server. Additional descriptions were added to provide examples of the use of the <code>openssl</code> command when using elliptic-curve cryptography, and to describe how to specify private key file names in the SSL communication definition file.</p>	6.13.2 , openssl , SSL communication definition file

Changes	Location
<p>With regard to event filter syntax, the value range of condition statement attributes B . TIME (Registered time) and B . ARRIVEDTIME (Arrived time) was changed.</p> <p>As a result, descriptions of keywords for comparing condition statements, RANGE, TRANGE, and WITHIN were changed.</p>	<p><i>Event filter syntax</i></p>
<p>The type of the following parameters in the event server settings file was changed from required parameters to custom parameters:</p> <ul style="list-style-type: none"> • include • options v5-unused 	<p><i>Event server settings file</i></p>
<p>TLS1.3 was added as an SSL communication version that can be specified to the SSL communication definition file.</p> <p>An explanation on specifying an ECC-format encryption suite was added.</p>	<p><i>SSL communication definition file</i></p>
<p>AWS CLI-compatible scripts for use with auto-scaling linkage were added.</p>	<p><i>Appendix A.1, Appendix A.1(1) , Appendix A.2, Appendix A.2(1), Appendix L, Appendix L.1, Appendix L.1(3) , Appendix L.5, Appendix L.8(1) , Appendix L.8(4) , Appendix L.10</i></p>

Legend:

--: Not applicable

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

Preface

This manual describes the functionality and operation of JP1/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.

■ Intended readers

This manual is intended for:

- System administrators who are responsible for introducing and operating JP1/Base.
- System administrators and system operators who are responsible for introducing, configuring, and operating a system that incorporates JP1 products (such as JP1/IM, JP1/AJS, and JP1/Power Monitor) for which JP1/Base is a prerequisite.

■ Organization of this manual

This manual is organized into the following parts:

PART 1: Overview

This part gives an overview of JP1/Base.

PART 2: Functions

This part describes the functionality of JP1/Base.

PART 3: 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 4: Installation and Operation

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

PART 5: Reference

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

PART 6: Troubleshooting

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

■ 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
<i>JP1/Base User's Guide</i>	<ul style="list-style-type: none">• Overview and functionality of JP1/Base• Setup of each function• Commands, definition files, JP1 events• Troubleshooting

Manual	Content
	<ul style="list-style-type: none"> Processes, port numbers, operational logs
<i>JP1/Base Messages</i>	Messages
<i>JP1/Base Function Reference</i>	<ul style="list-style-type: none"> Methods for issuing or acquiring JP1 events by using user applications or JP1 programs. Functions

■ Conventions: "Administrator permissions" as used in this manual

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

■ Conventions: Directory names

Linux 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 Linux can use the same directory names.

When Linux 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	<p>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:</p> <ul style="list-style-type: none"> • From the File menu, choose Open. • Click the Cancel button. • In the Enter name entry box, type your name.
<i>Italics</i>	<p>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:</p> <ul style="list-style-type: none"> • Write the command as follows: <code>copy source-file target-file</code> • Do <i>not</i> delete the configuration file.
Code font	<p>A code font indicates text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none"> • At the prompt, enter <code>dir</code>.

Font	Convention
	<ul style="list-style-type: none"> • Use the <code>send</code> 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:

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

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: A B C means A, or B, or C.
{ }	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: {A B C} means only one of A, or B, or C.
[]	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: [A] means that you can specify A or nothing. [B C] means that you can specify B, or C, or nothing.
...	In coding, an ellipsis (...) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: A, B, B, ... means that, after you specify A, B, you can specify B as many times as necessary.
<u>perm</u>	Underlined characters indicate the default value.
△	This symbol is used to explicitly indicate a space. △ 0: Enter one or more spaces, or none (a space is optional). △ 1: Enter one or more spaces (a space is mandatory).
StoreDatabase	Code-font characters must be entered exactly as shown.
<i>database-name</i>	This font style marks a placeholder that indicates where appropriate characters are to be entered in an actual command.
SD	Bold code-font characters indicate the abbreviation for a command.

■ Conventions: JP1/Base installation folder

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

Product name	Installation folder	Location of installation folder [#]
JP1/Base	<i>installation-folder</i>	<i>system-drive</i> : \Program Files (x86)\HITACHI\JP1Base

[#]: The installation folders in this column are the default installation folders. For Windows Vista or later, 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 might differ depending on the environment.

■ Conventions: Version numbers

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

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

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

Contents

Notices	2
Summary of amendments	6
Preface	8

Part 1: Overview

1	Overview of JP1/Base	27
1.1	Overview of JP1/Base functionality	28
1.1.1	JP1/Base functionality supported by each OS (in Windows)	29
1.1.2	JP1/Base functionality supported by each OS (in UNIX)	30

Part 2: Functions

2	Details of JP1/Base Functions	32
2.1	Managing users	33
2.1.1	Authenticating users	33
2.1.2	User authentication block	36
2.1.3	Secondary authentication server	38
2.1.4	User authentication by linking with a directory server	40
2.1.5	Mapping users	45
2.2	Controlling the service start and stop sequences (Windows only)	47
2.3	Sending and receiving events with the event service	48
2.3.1	Event service	48
2.3.2	Event database	48
2.3.3	JP1 events acquired by JP1/Base	51
2.3.4	Forwarding JP1 events	51
2.4	Converting log messages and event log data into JP1 events	53
2.4.1	Converting application program log files	53
2.4.2	Prerequisites for a log file trap	54
2.4.3	Start and end of monitoring with a log file trap	54
2.4.4	Types of log files that can be monitored	55
2.4.5	Types of log files that cannot be monitored	62
2.4.6	The number of log files that can be monitored	64
2.4.7	Reattempting to monitor a log file when a trap fails	65
2.4.8	Reattempting to connect to the event service (log file trap)	67
2.4.9	Converting Windows event logs	67
2.4.10	Start and end of monitoring in event log trap	68

2.4.11	Reattempting to connect to an event service (event log trap)	68
2.5	Suppressing forwarding of large numbers of events	69
2.5.1	Large numbers of events	69
2.5.2	Precautions against large numbers of events	69
2.5.3	Using a manager to suppress event forwarding from an agent with large numbers of JP1 events	69
2.5.4	Setting a threshold to automatically suppress forwarding of large numbers of events	77
2.6	Collecting and distributing definitions (JP1/IM only)	83
2.6.1	Managing definitions by using IM configuration management	83
2.6.2	Checking information on the operation of services by using IM configuration management	83
2.6.3	Managing the system's hierarchical configuration by using commands	83
2.6.4	Collecting and distributing definitions for the event service by using commands	86
2.6.5	Collecting definitions of JP1 programs	87
2.7	Detecting a process hangup and abnormal termination	89
2.7.1	Flow of using the health check function to troubleshoot problems	89
2.7.2	Problems that can be detected by the health check function	89
2.7.3	Process monitoring with the health check function	90
2.7.4	Processes monitored by the health check function	90
2.7.5	Remote host monitoring with the health check function	92
2.8	Command execution triggered by a JP1 event	100
2.8.1	Conditions required for executing local actions	100
2.8.2	Commands for local actions	101
2.8.3	Execution status of local actions	101
2.8.4	Pausing local actions	102
2.9	Support for system configurations	103
2.9.1	Using JP1/Base in a cluster system	103
2.9.2	Using logical hosts in a non-cluster environment	103
2.10	Communication protocols of JP1/Base	104
2.10.1	Recommended communication protocol	104
2.10.2	Changes in communication waiting process between the ANY and the IP binding methods	105
2.10.3	Checking IP addresses corresponding to host names	107
2.10.4	Notes on communication protocols of JP1/Base	107
2.11	Managing JP1/Base as a JP1/Base administrator (UNIX only)	109
2.12	JP1/Base compatibility	110
2.12.1	Compatibility and connectivity with previous versions of JP1/Base	110

Part 3: Installation and Setup

3 Installation and Setup 112

3.1	Installation and setup overview	113
3.2	Installing JP1/Base (in Windows)	114
3.2.1	Installing JP1/Base	114
3.2.2	Uninstalling JP1/Base	115

3.2.3	Notes on installing and uninstalling JP1/Base	116
3.3	Installing JP1/Base (in UNIX)	125
3.3.1	Installing JP1/Base	125
3.3.2	Using the Hitachi Program Product Installer	126
3.3.3	Uninstalling JP1/Base	128
3.3.4	Notes on installing and uninstalling JP1/Base	128
3.4	JP1/Base setup	135
3.4.1	Setting the language (for Windows)	135
3.4.2	Setting the language (for UNIX)	135
3.4.3	Notes on running JP1 in a Chinese (Simplified) language environment	138
3.4.4	Adjusting the kernel parameters (UNIX only)	140
3.4.5	Extending regular expressions to be used	140
3.4.6	Setting the password save format	142
3.4.7	Setting a password policy	143
3.4.8	Syslog output when SUSE Linux 15 or later is used	145
3.5	Backup and recovery	146
3.5.1	Backup and recovery considerations	146
3.5.2	Backup and recovery (in Windows)	146
3.5.3	Backup and recovery (in UNIX)	153
4	Setup for Handling Possible Errors in JP1/Base	161
4.1	Setup for handling possible errors in JP1/Base	162
4.1.1	Range of process errors that can be detected by the health check and process management functions	162
4.2	Using health check function to detect process errors	164
4.2.1	Enabling the health check function	164
4.2.2	Checking the health check settings	165
4.2.3	Changing the health check settings	165
4.2.4	Disabling the health check settings	165
4.2.5	Notes on using the health check function	166
4.3	Detecting abnormal process termination and authentication server switching	167
4.3.1	Monitored processes	167
4.3.2	Triggering of JP1 events	167
4.3.3	Setup process for detecting abnormal process termination and switching of the authentication server	168
4.4	Restarting abnormally terminated processes managed by the process management function	169
4.4.1	Target processes	169
4.4.2	Setup procedure for restarting processes managed by the process management function	169
4.5	Restarting an abnormally terminated event service process (UNIX only)	170
4.5.1	Target processes	170
4.5.2	Setup procedure for restarting an abnormally terminated event service process	170
4.6	Setting Hitachi Network Objectplaza Trace Library (HNTRLib2)	171

4.7	Preparing to collect information when a problem occurs (Windows only)	172
4.7.1	Setting up user dump output	172
4.8	Setting a threshold to detect large numbers of events	173
4.9	Function for automatically re-organizing the command execution log file	174
5	Setting Up JP1/Base for Use in a Cluster System	175
5.1	Overview of using JP1/Base in a cluster system	176
5.1.1	Overview of a cluster system	176
5.1.2	Overview of using JP1/Base in a cluster system	177
5.2	Prerequisites for using JP1/Base in a cluster system and the support range	178
5.2.1	Prerequisites for a logical host environment	178
5.2.2	Prerequisites for a physical host environment	179
5.2.3	Specifying a logical host	179
5.2.4	The scope supported by JP1	181
5.3	Functions of JP/Base in a cluster system	182
5.3.1	Cluster operation with the log file trapping function	182
5.3.2	Cluster operation with the event log trapping function	185
5.3.3	Cluster operation with the health check function	186
5.4	Setting up the environment for a cluster system (in Windows)	188
5.4.1	Required environment settings	188
5.4.2	Installing JP1/Base	189
5.4.3	Setup	189
5.4.4	Registering services in the cluster software	196
5.4.5	Settings to configure both physical and logical host environments on the same host	196
5.5	Setting up the environment for a cluster system (in UNIX)	199
5.5.1	Required environment settings	199
5.5.2	Installing JP1/Base	201
5.5.3	Setup	201
5.5.4	Registering daemons in the cluster software	204
5.6	Follow-up tasks when changing settings in a cluster environment	207
5.6.1	Operations that result in changes to the common definition information on the primary node and how to apply the settings to the secondary node	207
5.7	Deleting logical hosts	212
5.7.1	Deleting logical hosts (in Windows)	212
5.7.2	Deleting logical hosts (in UNIX)	212
5.8	Notes on using JP1/Base in a cluster system	214
5.8.1	Notes on cluster use (common to all OSs)	214
5.8.2	Notes on cluster use (limited to Windows only)	215
5.8.3	Notes on cluster use (limited to UNIX only)	216
5.9	Setting up a logical host in a non-cluster environment	218
5.9.1	Considerations when using logical hosts in a non-cluster environment	218
5.9.2	Configuring a logical host in a non-cluster environment	218

5.9.3 Logical host operation in a non-cluster environment 219

6 JP1/Base Communication Settings According to Network Configurations 223

- 6.1 Using JP1/Base on a single network 224
- 6.2 Using JP1/Base on multiple networks 225
 - 6.2.1 Communication settings when JP1/Base is used on multiple networks 226
- 6.3 Setting up JP1/Base communication protocols 228
 - 6.3.1 Situations where the JP1/Base communication protocol must be changed 228
 - 6.3.2 Changing the JP1/Base communication protocol 228
 - 6.3.3 Specifying an ANY binding address 230
 - 6.3.4 Checking the JP1/Base communication protocol 231
 - 6.3.5 Setting a duplicate communication protocol using IM configuration management 232
- 6.4 Setting JP1-specific hosts information 234
 - 6.4.1 When JP1-specific hosts information is required 234
 - 6.4.2 Setting JP1-specific hosts information 234
 - 6.4.3 Behavior when both jp1hosts information and jp1hosts2 information are defined 235
 - 6.4.4 Differences between jp1hosts and jp1hosts2 information 235
 - 6.4.5 Migrating from jp1hosts information to jp1hosts2 information 238
 - 6.4.6 Checking jp1hosts or jp1hosts2 information 240
- 6.5 Using JP1/Base in an environment of distinct networks (with jp1hosts information) 241
 - 6.5.1 Issues when using JP1/Base in an environment of distinct networks (with jp1hosts information) 241
 - 6.5.2 Defining jp1hosts information 243
 - 6.5.3 Changing communication settings of event services 244
 - 6.5.4 Restarting JP1/Base 245
- 6.6 Using JP1/Base in an environment of distinct networks (with jp1hosts2 information) 246
 - 6.6.1 Issues when using JP1/Base in an environment of distinct networks (with jp1hosts2 information) 246
 - 6.6.2 Defining jp1hosts2 information 248
 - 6.6.3 Changing communication settings for event services 249
 - 6.6.4 Restart JP1/Base as needed 250
- 6.7 An example of communication settings when JP1/Base is not used in a cluster system (in an environment of distinct networks) 251
 - 6.7.1 Changing communication settings (with jp1hosts information) 251
 - 6.7.2 Changing communication settings (with jp1hosts2 information) 252
- 6.8 An example of communication settings when JP1/Base is used in a cluster system (in an environment of distinct networks) 254
 - 6.8.1 Changing communication settings (with jp1hosts information) 255
 - 6.8.2 Changing communication settings (with jp1hosts2 information) 257
- 6.9 Communication settings example when JP1/Base is operating within a specific network in an environment with multiple networks 260
 - 6.9.1 Changing communication settings (with jp1hosts information) 260
 - 6.9.2 Changing communication settings (with jp1hosts2 information) 263

6.10	Resetting JP1/Base to a single network after use on multiple networks	266
6.10.1	Resetting JP1/Base to single network use (with jp1hosts information)	266
6.10.2	Resetting JP1/Base to single network use (with jp1hosts2 information)	266
6.11	Using JP1/Base in IPv6 environments	268
6.11.1	Prerequisites for an IPv6 environment	268
6.11.2	Communication settings when using JP1/Base in an IPv6 environment	269
6.11.3	Checking IP addresses	271
6.12	Situations that require communication settings	273
6.12.1	Situations that require communication settings for definition files	273
6.13	Communication encryption in JP1/Base	276
6.13.1	Files required for SSL communication	278
6.13.2	Setting up an SSL communication environment on the server side	280
6.13.3	Setting up an SSL communication environment on the client side	281
6.13.4	Setting up the communication encryption function of JP1/Base	281
6.13.5	Notes on using event services	282

Part 4: Installation and Operation

7 Startup and Termination 283

7.1	Starting and stopping JP1/Base (in Windows)	284
7.1.1	Starting services	284
7.1.2	Confirming service startup	286
7.1.3	Stopping services	286
7.2	Starting and stopping JP1/Base (in UNIX)	287
7.2.1	Setting services to start and stop automatically	288
7.2.2	Confirming JP1/Base startup	291

8 User Management Setup 292

8.1	User management setup (in Windows)	293
8.1.1	Specifying the authentication servers to use	294
8.1.2	Setting JP1 users (standard users)	296
8.1.3	Setting JP1 user operating permissions	299
8.1.4	Copying settings from the primary authentication server	300
8.1.5	Assigning user permissions to OS users before setting user mapping	301
8.1.6	Using the GUI to set user mapping	303
8.1.7	Using commands to set user mapping	308
8.1.8	Notes on user management setup	311
8.2	Setup for user authentication linking with the directory server (Windows only)	313
8.2.1	Settings for the operation to use a linkage user	316
8.2.2	Settings for the operation to use a DS user	322
8.3	User management setup (in UNIX)	328
8.3.1	Specifying the authentication servers to use	328

- 8.3.2 Setting JP1 users 330
- 8.3.3 Setting JP1 user operating permissions 331
- 8.3.4 Copying settings from the primary authentication server 332
- 8.3.5 Setting user mapping 333
- 8.3.6 Notes on user management setup 334
- 8.4 Setup for handling the blocked status (using a secondary authentication server) 335
- 8.4.1 Blocked status settings using the GUI (Windows only) 335
- 8.4.2 Blocked status settings using commands 336

9 Setting the Service Start and Stop Sequences (Windows Only) 337

- 9.1 Setting the service start and stop sequences 338
- 9.2 Editing a start sequence definition file 339
- 9.2.1 Setting the service start sequence 339
- 9.2.2 Setting the service stop sequence 340
- 9.3 Setting the timing for starting services 342
- 9.4 Notes on using startup control 343

10 Setting up an Event Service Environment 344

- 10.1 Process for setting up an event service environment 345
- 10.1.1 Determining which JP1 events to forward 345
- 10.1.2 Determining if forwarding of a large numbers of events are suppressed 346
- 10.1.3 Setting up an event service environment 346
- 10.1.4 Modifying the event service operating environment 347
- 10.1.5 Modifying the settings for forwarding JP1 events 348
- 10.1.6 Checking whether the event service is active 349
- 10.1.7 Checking the settings for forwarding JP1 events 349
- 10.1.8 Using a manager to suppress event forwarding of large numbers of events 349
- 10.1.9 Setting a threshold to suppress forwarding of large numbers of events 350
- 10.1.10 Setting up an event server in a system that uses DNS services 351
- 10.2 Initializing the event database 354
- 10.2.1 Initializing an event database while the event service is active 354
- 10.2.2 Initializing an event database while the event service is stopped 354
- 10.3 Outputting the event database to a CSV file 356
- 10.3.1 Output format of a CSV file 356
- 10.3.2 Items output to the CSV file 356
- 10.4 Notes on using the event service 361

11 Setting Up the Event Converters 362

- 11.1 Converting application program log files 363
- 11.1.1 Checking the format of application program log files 363
- 11.1.2 Setting up a log file trap 365
- 11.1.3 Notes on log file trapping 368

11.2	Converting Windows event logs	371
11.2.1	Procedures for setting up event log trapping	371
11.2.2	Notes on event log trapping	372
12	Collecting and Distributing Event Service Definitions (JP1/IM Only)	374
12.1	Communication settings for definition and operation information (linked with IM configuration management)	375
12.2	Setting the system's hierarchical configuration	376
12.2.1	Specifying the method for distributing configuration definition information	376
12.3	Collecting event service definitions	377
12.3.1	Output format	377
12.3.2	Collection example	377
12.4	Distributing event service definitions	379
13	Setting Local Actions	380
13.1	Setting a local action	381
13.1.1	Defining a local action	381
13.1.2	Changing local action settings	381
13.1.3	Checking the operating status of a local action	382
13.1.4	Pausing a local action	382
13.2	Example of operating a local action	384
13.2.1	Setting the local action execution definition file	384
13.2.2	Setting the forwarding settings file	385
13.3	Notes on local actions	386
14	Modifying Settings During JP1/Base Operation	387
14.1	Modifying settings for JP1/Base	388
14.1.1	When changes take effect	388
14.2	Modifying settings on a JP1/Base host	391
14.2.1	Effects and follow-up tasks when changing host names	391
14.2.2	Effects and follow-up tasks when changing IP addresses	393
14.2.3	Follow-up tasks when changing the system time	393

Part 5: Reference

15	Commands	395
	List of commands	396
	JP1/Base administrator console (for Windows)	403
	cpysvprm (Windows only)	404
	hntr2conf	405
	hntr2getconf	408
	hntr2getname (Windows only)	411
	hntr2kill (UNIX only)	412
	hntr2mon (UNIX only)	413

hntr2util (UNIX only) 414
hntr2util (Windows only) 416
hntr2util2 (UNIX only) 419
hntr2util2 (Windows only) 421
jbs_killall.cluster (UNIX only) 424
jbs_log.bat (Windows only) 425
jbs_log.sh (UNIX only) 428
jbs_setup_cluster (Windows only) 432
jbs_spmd (UNIX only) 434
jbs_spmd_reload 435
jbs_spmd_status 437
jbs_spmd_stop 439
jbs_start (UNIX only) 440
jbs_start.cluster (UNIX only) 442
jbs_stop (UNIX only) 444
jbs_stop.cluster (UNIX only) 445
jbsaclint 446
jbsaclreload 447
jbsadduser 449
jbsadmin (Windows only) 451
jbsblockadesrv 452
jbscancellcact 454
jbschgds (Windows only) 455
jbschgpasswd 456
jbschkds (Windows only) 458
jbsgetcnf 461
jbsgetopinfo 463
jbsgetumap 466
jbshostsexport 467
jbshosts2export 468
jbshostsimport 469
jbshosts2import 472
jbslistacl 475
jbslistlcact 478
jbslistsrv 479
jbslistuser 481
jbsmkpass (Windows only) 484
jbsmkumap 485
jbsparamdump 487
jbspassmgr (Windows only) 496
jbsrmacl 497
jbsrmumap 499
jbsrmumappass (Windows only) 501
jbsrmuser 502
jbsrt_del 504
jbsrt_distrib 506
jbsrt_get 510

jbsrt_sync 512
jbssetacl 514
jbssetadmingrp (UNIX only) 516
jbssetcnf 518
jbssetumap 519
jbssetupsvr (Windows only) 522
jbssetusrsrv (UNIX only) 524
jbsumappass (Windows only) 525
jbsunblockadesrv 527
jbsunsetcnf 528
jcocmdconv 530
jcocmddef 532
jcocmddel 539
jcocmdlog 541
jcocmdshow 544
jevagtfw 547
jevdbinit 551
jevdbmkrep 553
jevdbswitch 555
jevdef_distrib 557
jevdef_get 561
jeveltreload (Windows only) 563
jevexport 564
jevextreload 568
jevlogdstart (UNIX only) 570
jevfwstat 571
jevlogdstat 573
jevlogdstop (UNIX only) 574
jevlogreload 575
jevlogstart 577
jevlogstart (cluster environment only) 584
jevlogstat 585
jevlogstop 586
jevlogstop (cluster environment only) 588
jevmessageid.bat (Windows only) 589
jevregsvc (Windows only) 590
jevreload 591
jevsend 593
jevsendd 596
jevstart (UNIX only) 599
jevstat 600
jevstop (UNIX only) 603
Jischk 604
Jiscond 606
Jisconv 608
Jiscpy 611
Jisext 612

- Jisinfo 614
- Jiskeymnt 616
- Jisktod 620
- Jislckclear (Windows only) 625
- Jislckext 626
- Jislckfree (Windows only) 628
- Jislckreg (UNIX only) 629
- Jismlcktr (Windows only) 630
- Jisprt 631
- Jirsdel (UNIX only) 633
- jp1base_setup (UNIX only) 634
- jp1base_setup_cluster (UNIX only) 635
- jp1bshasetup (Windows only) 638
- jp1ping 639
- openssl 642

16 **Definition Files 644**

- List of definition files 645
- Definition files required for each operational case 648
- Types of parameters 653
- Event filter syntax 654
- Start sequence definition file (Windows only) 661
- Service startup delay time / timer monitoring period definition file (Windows only) 667
- Event server index file 669
- Event server settings file 672
- Forwarding settings file 687
- API settings file 693
- Additional extended attribute settings files 697
- Action definition file for log file trapping 703
- Log-file trap startup definition file 714
- Log information definition file 719
- Action definition file for event log trapping (Windows only) 721
- Distribution definition file 731
- Password definition file (Windows only) 736
- User permission level file 738
- User permission definition file 740
- Directory server modification file (Windows only) 742
- Directory server linkage definition file (Windows only) 744
- User mapping definition file 749
- Password policy definition file 751
- Health check definition file 754
- Common definition settings file (health check function) 758
- JP1/Base parameter definition file 760
- Extended startup process definition file 762
- jp1hosts definition file 766
- jp1hosts2 definition file 768
- Host access control definition file 771

SSL communication definition file	773
Non-SSL communication host configuration file	777
Local action environment variable file	780
Local action execution definition file	781
Common definition settings file (local action function)	786
Collection information file	788
Common definition settings file (configuration management functionality)	790
Configuration definition file	792
Environment variable file	795
Host group definition file	797

17 JP1 Events 799

17.1	JP1 event attributes	800
17.1.1	Basic attributes	800
17.1.2	Extended attributes	801
17.2	List of JP1 events output by JP1/Base	803
17.3	JP1 event details	807
17.3.1	JP1 event details by event ID	807

Part 6: Troubleshooting

18 Troubleshooting 843

18.1	Troubleshooting procedure	844
18.2	Types of log information	845
18.2.1	Common message log information	845
18.2.2	Integrated trace log information	845
18.2.3	Log information of each process	848
18.2.4	Operation log	848
18.2.5	Log files and directories	848
18.3	Data that must be collected when a problem occurs	849
18.3.1	Data that must be collected when a problem occurs (in Windows)	849
18.3.2	Data that must be collected when a problem occurs (in UNIX)	853
18.4	How to collect data	859
18.4.1	How to collect data (in Windows)	859
18.4.2	How to collect data (in UNIX)	863
18.5	Troubleshooting different types of problems	867
18.5.1	Problems in Windows or UNIX	867
18.5.2	Problems in Windows	869
18.5.3	Problems in UNIX	872
18.5.4	Errors detected by the health check function	873
18.6	Notes on using JP1/Base	875
18.6.1	Notes on starting the system	875
18.6.2	Notes on starting the system operation	875

- 18.6.3 Notes on user authentication 877
- 18.6.4 Notes on controlling the start sequence 877
- 18.6.5 Notes on the files and directories used by JP1/Base 877

Appendixes 878

- A List of Files and Directories 879
 - A.1 List of files and directories (in Windows) 879
 - A.2 List of files and directories (in UNIX) 892
- B List of Processes 906
 - B.1 List of processes (in Windows) 906
 - B.2 List of processes (in UNIX) 908
- C List of Port Numbers 911
 - C.1 Port numbers for JP1/Base 911
 - C.2 Direction in which data passes through the firewall 911
 - C.3 Connection status 912
 - C.4 Settings for the Windows firewall 913
- D List of Limits 916
- E Estimating memory and disk space requirements 918
 - E.1 Memory requirements 918
 - E.2 Disk space requirements (in Windows) 918
 - E.3 Disk space requirements (in UNIX) 918
 - E.4 Disk space requirements for the shared disk in a cluster system 918
- F Syntax of Regular Expressions 919
 - F.1 Regular expressions that can be used by default 919
 - F.2 Extended regular expressions that can be used when regular expressions are extended 920
 - F.3 Comparison among regular expressions that can be used 921
 - F.4 Tips on using regular expressions 922
 - F.5 Examples of using regular expressions 923
- G List of Kernel Parameters 925
 - G.1 List of Kernel Parameters (in AIX) 925
 - G.2 List of Kernel Parameters (in Linux) 925
- H Handling Changes in Communication Settings 928
 - H.1 Changing the settings in the jp1hosts2 definition file 928
 - H.2 Changing the settings in the jp1hosts definition file 928
 - H.3 Changing the settings in the communication protocol settings files 929
 - H.4 Changing the settings for the ports parameter in the event server settings file (conf) 929
 - H.5 Changing the settings for the client-bind parameter in the event server settings file (conf) 929
 - H.6 Changing the settings for the remote-server parameter in the event server settings file (conf) 930
 - H.7 Changing the settings for the server parameter in the API settings file (api) 930
 - H.8 Changing the settings for the client parameter in the API settings file (api) 930
 - H.9 Functionality supported in communication settings 930

H.10	Parameters defined in the communication protocol settings file	931
H.11	Differences between communication protocols of JP1/Base 06-51 or earlier and JP1/Base 06-71 or later	932
H.12	Communication protocols in a cluster setup	934
I	Operation Log Output	935
I.1	Types of events recorded in the operation log	935
I.2	Storage format of operation log output	935
I.3	Operation log output format	936
I.4	Trigger conditions for operation log output	940
I.5	Settings for outputting operation logs	941
I.6	Operation log messages	944
J	Operating JP1/Base as a JP1/Base Administrator (UNIX Only)	946
J.1	Division of roles when operating JP1/Base	946
J.2	Setting up an environment in which JP1/Base administrators can use JP1/Base	949
J.3	Setting up an environment for JP1/Base administrators on a logical host	950
K	Operating a secure system	953
K.1	Prerequisites for a secure system	953
K.2	Restricting connections from unintended hosts	954
K.3	Definition for restricting connections from unintended hosts	955
K.4	Procedure for restricting connections from unintended hosts	956
K.5	Messages that are output when a request was denied by connection restriction	957
L	Using JP1/Base linked with the auto-scaling functionality	958
L.1	System configuration for using JP1/Base linked with the auto-scaling functionality	958
L.2	Prerequisites for using JP1/Base linked with the auto-scaling functionality	960
L.3	Adding hosts to the monitoring target during scale out	961
L.4	Terminating monitoring during scale in	962
L.5	Setup procedure for using JP1/Base linked with the auto-scaling functionality (for the manager host)	963
L.6	Setup procedure for using JP1/Base linked with the auto-scaling functionality (for agent hosts)	965
L.7	Configuring the Amazon EC2 service	967
L.8	Auto-scaling linkage script	968
L.9	Processing time required for configuring and clearing monitoring settings	973
L.10	Notes about using JP1/Base linked with the auto-scaling functionality	974
M	Notes on using Docker, Podman (Linux only)	975
M.1	Creating a Docker image	975
M.2	Notes on installing JP1/Base on a container	976
M.3	Notes on installing JP1/Base on the Docker host and container	978
M.4	Creating a Podman image	979
M.5	Notes on installing JP1/Base on a container	980
M.6	Notes on installing JP1/Base on the Podman host and container	982
N	Version Changes	983
N.1	Changes in 13-00	983

N.2	Changes in 12-50#	986
N.3	Changes in 12-10	987
N.4	Changes in 12-00	988
N.5	Changes in 11-50	989
N.6	Changes in 11-10	990
N.7	Changes in 11-00	991
N.8	Changes in 10-50	993
N.9	Changes in 10-10	996
N.10	Changes in 10-00	998
N.11	Changes in 09-00	1003
O	Reference Material for this Manual	1005
O.1	Related publications	1005
O.2	Abbreviations	1006
O.3	Acronyms	1007
O.4	Conventions for KB (kilobytes) and other units	1009
P	Glossary	1010

Index 1018

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 integrated management system and the JP1/AJS job 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**

JP1/Base manages the JP1 users, which are accounts dedicated to JP1 products. 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.

JP1/Base user management provides functionality for the following two tasks:

User authentication

User authentication manages permissions for users to access individual hosts on which JP1 manager products (such as JP1/IM - Manager and JP1/AJS - Manager) are installed, or to operate JP1 resources (such as jobs, jobnets, and events) on individual hosts.

User mapping

User mapping grants JP1 users (which are accounts dedicated to JP1 products) the permissions of OS users. A user who is registered as a JP1 user on the authentication server will be able to operate a host with the permission of an OS user registered on the host.

- **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.

- **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.

This functionality enables you to use the manager host to batch-collect information that is defined in the JP1/Base instances on individual hosts. Therefore, you can efficiently manage definition information. You can also edit definition information on the manager host, distribute the information to the JP1/Base instances on individual hosts, and update definition information.

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

You can use commands provided by JP1/Base to collect or distribute definition information in the definition files used for the event service or event conversion.

Collecting definitions of JP1 programs

You can collect definitions managed by JP1 programs, such as JP1/AJS jobnet definitions and JP1/SSO definitions. The collected definition information is managed as monitored objects within JP1/IM. For details, see the manual *JP1/Integrated Management 3 - 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 [15. 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.

1.1.1 JP1/Base functionality supported by each OS (in Windows)

Some of the JP1/Base functionality might not be supported by a particular OS.

The following table shows the functionality that each OS supports in Windows.

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

Functionality		OS (Windows)	
		2016, 2019, 2022	
User management	User authentication	Yes	
	User authentication by a directory server ^{#1}	Yes	
	User mapping	Yes	
Startup control for services	Start sequence control	Yes	
	Stop sequence control ^{#2}	Yes	
Event service		Part ^{#3}	
Event conversion	Log file trapping	Yes	
	Event log trapping	Yes	
Collecting and distributing definitions	Checking information on the operation of services and managing definitions by using IM configuration management	Yes	
	Collecting and distributing definitions for the event service by using commands	Yes	
	Collecting definitions of JP1 programs	Yes	
Process management		Yes	
Health check		Yes	
Local action		Yes	
ISAM-related utility commands		Yes	
Hitachi Network Objectplaza Trace Library (HNTRLib2)		Yes	
Communication with IPv4 addresses		Yes	
Communication with IPv6 addresses		Yes	

Legend:

2016, 2019, 2022: Windows Server 2016, Windows Server 2019, and Windows Server 2022

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: Version 5 compatibility events are not supported.

1.1.2 JP1/Base functionality supported by each OS (in UNIX)

Some of the JP1/Base functionality might not be supported by a particular OS.

The following table shows the functionality that each OS supports in UNIX.

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

Functionality		OS (UNIX)	
		AIX	Linux
User management	User authentication	Yes	Yes
	User authentication by a directory server [#]	No	No
	User mapping	Yes	Yes
Startup control for services [#]	Start sequence control	No	No
	Stop sequence control	No	No
Event service		Yes	Yes
Event conversion	Log file trapping	Yes	Yes
	Event log trapping [#]	No	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
Communication with IPv4 addresses		Yes	Yes
Communication with IPv6 addresses		No	Yes

Legend:

AIX refers to AIX.

Linux refers to Linux.

Yes: Supported

Part: Partly supported only.

No: Not supported

[#]: This functionality is not supported in UNIX.

2

Details of JP1/Base Functions

This chapter describes the functions of JP1/Base.

2.1 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 2.1.1 to 2.1.4. For details on user mapping, see 2.1.5.

2.1.1 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. Information on accessibility to JP1 resources or operating permission is called *JP1 authentication information*. The JP1 authentication information is managed and controlled as a set for each JP1 user on an *authentication server*.

For details on when each viewer connects to the authentication server, see the manual for each JP1 product that performs user authentication via JP1/Base.

(1) User authentication

User 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 user authentication is performed on the authentication server.

In Windows, by linking with a directory server, the directory server can be used to user authentication. For details on user authentication by linking with a directory server, see [2.1.4 User authentication by linking with a directory server](#).

(2) 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*.

(3) Password policy-based management

When an attempt is made to register a JP1 user or to change a JP1 user's password, a check is performed to verify if the set password is in line with the password policy. This helps maintain a high level of security by preventing users from registering weak passwords and by reducing the risk of unauthorized access to JP1.

The following table describes the items set in the password policy.

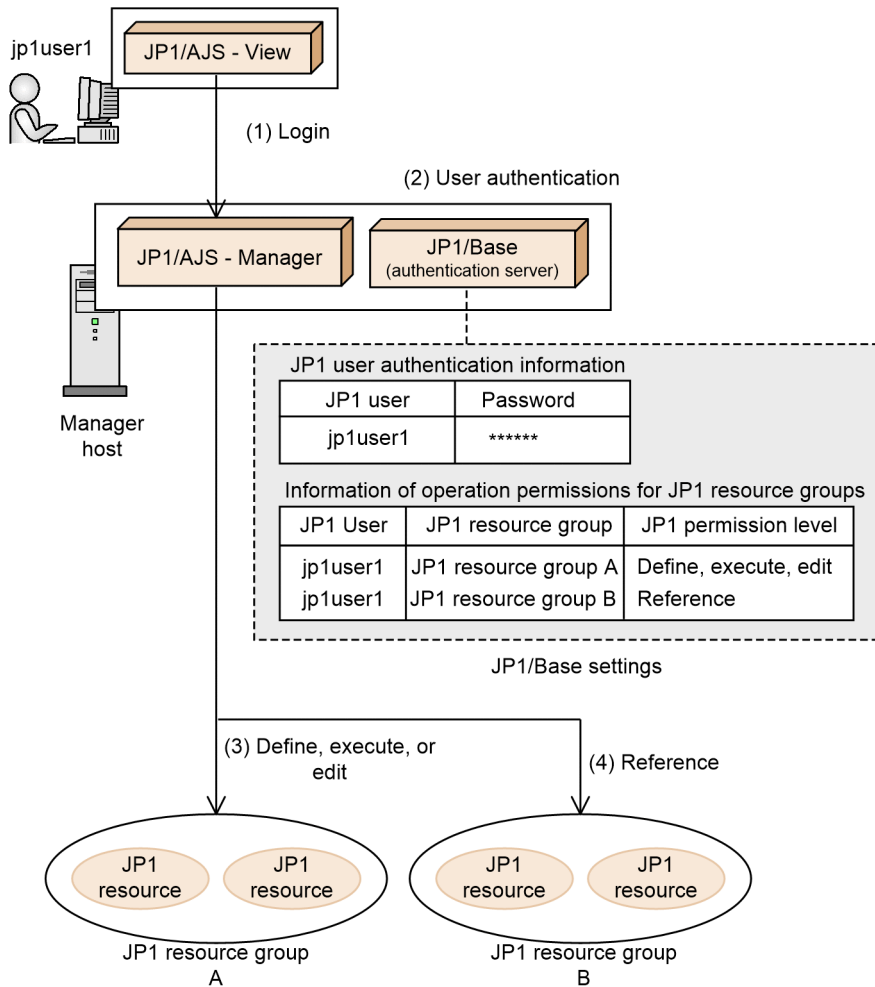
Set item	Range
Minimum number of characters	6 to 32 bytes
Minimum number of character types	One to four character types or special character types <ul style="list-style-type: none">• Numbers• Uppercase alphabetic characters• Lowercase alphabetic characters• Symbols (those that can be used in JP1 users' passwords)

To apply and use a more advanced password policy, link with a directory server (Active Directory) and set a password policy offered by the directory server.

(4) Example of user authentication

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

Figure 2–1: Example of user authentication

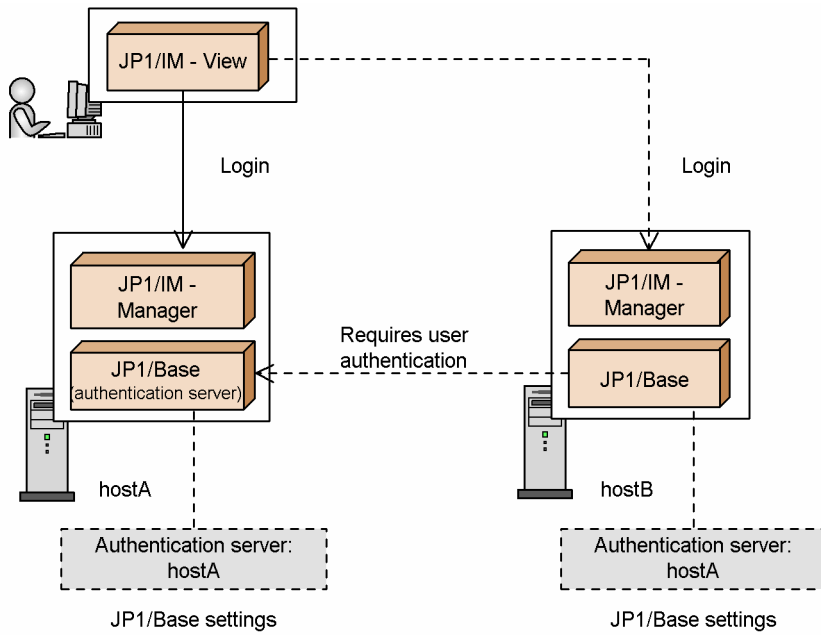


- (1) "jp1user1" logs in to JP1/AJS - Manager from JP1/AJS - View.
- (2) The authentication server performs user authentication for the logged-in "jp1user1". Based on the registered JP1 authentication information, the authentication server checks if "jp1user1" is registered. If there is no problem, the authentication server returns the operation permission information of "jp1user1" to JP1/AJS - Manager.
jp1user1's password is compliant with the password policy.
- (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 2–2: 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.



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

2.1.2 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.

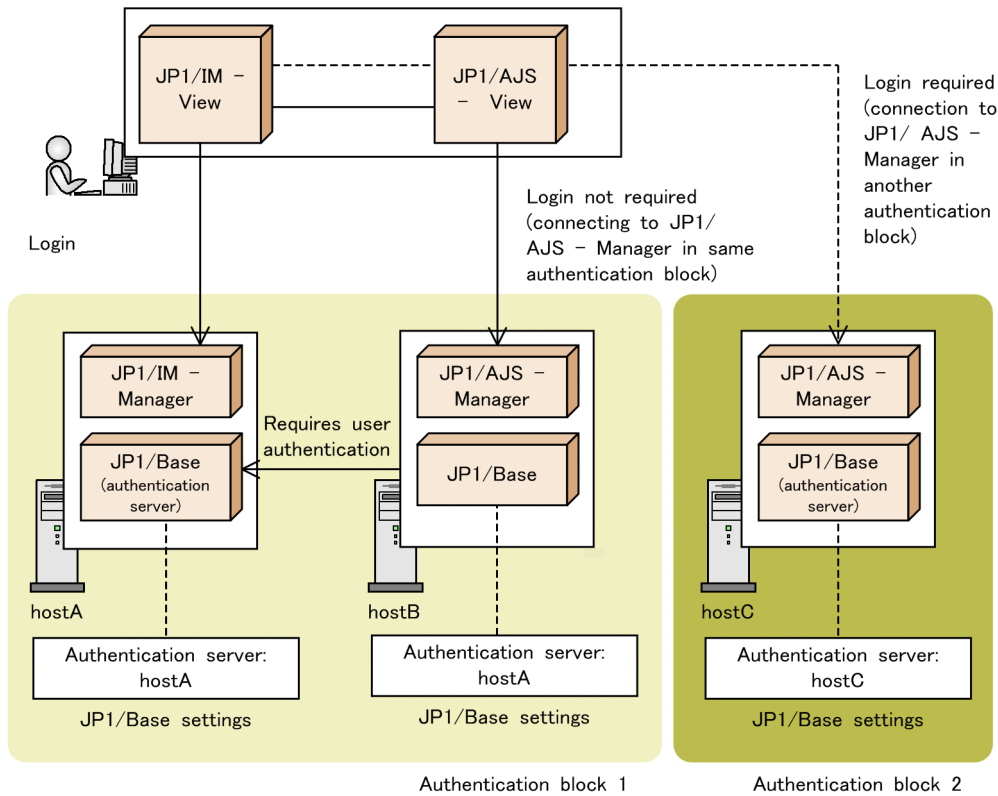
The following are examples in both JP1/IM and JP1/AJS:

Usually, user 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.

(1) Example of user authentication with two user authentication blocks

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

Figure 2–3: Example of user authentication with two user authentication blocks



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

(2) Example measures for enhancing the reliability of 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 the secondary authentication server, see [2.1.3 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 [5. 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 [4. Setup for Handling Possible Errors in JP1/Base](#).

2.1.3 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.

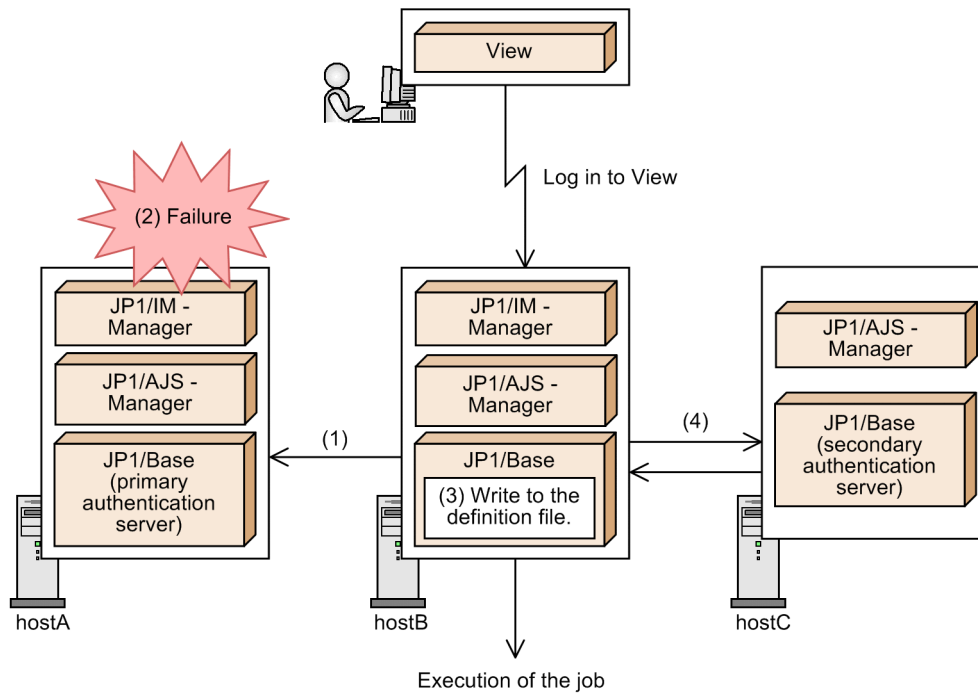
(1) Setting up a secondary authentication server

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) Flow of processing to connect the user to the secondary authentication server if connection to the primary authentication server fails

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 2–4: Connecting to the secondary authentication server if the connection with the primary authentication server fails



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 the connection is successful, you can log in to JP1/IM - View or JP1/AJS - View.

As shown in Figure 2-4, 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.

(3) Status of the authentication server and how to select the target authentication server

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. If connection to the primary authentication server fails, the host places the primary authentication server in blocked status and tries to connect to the secondary authentication server. If connection to the secondary authentication server fails, the host places the secondary authentication server in blocked status.
Primary authentication server: Blocked Secondary authentication server: Available	Host tries to connect to the secondary authentication server. If connection to the secondary authentication server fails, the host places the secondary

Authentication server status	How the target authentication server is selected
	authentication server in blocked status and does not try to connect to the primary 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 places the primary authentication server in blocked status and does not try to 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.

If a user intentionally places both authentication servers in blocked status, the system will attempt to connect to an authentication server if a login or some other task is performed from JP1/IM - View or JP1/AJS - View. If the attempt is successful, the system releases the blocked status 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, JP1/Base does not issue such an event. For details on how to issue a JP1 event, see [4.3 Detecting abnormal process termination and authentication server switching](#).

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 [8.4 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.

2.1.4 User authentication by linking with a directory server

User authentication functionality manages JP1 authentication information (JP1 user authentication information and JP1 operating permission) or JP1 authentication information's JP1 user authentication information only through linking with a directory server. This function is called *directory server linkage*. An Active Directory server is used for the directory server.

When using directory server linkage, users' passwords are managed on the directory server. In other words, they are managed not based on the JP1/Base password policy definitions but based on the directory server's policy.

The directory server linkage function has two management methods. One is to manage JP1 authentication information on a directory server and the other is to manage JP1 authentication information's JP1 user authentication information only on a directory server. The following table shows the management servers for every management method including the one not to use the directory server linkage function.

Table 2–1: JP1 authentication information management methods

User authentication method	JP1 authentication information		
	JP1 user authentication information		JP1 operating permission
	User name	Password	
Directory server linkage function unused	Managed by an authentication server	Managed by an authentication server	Managed by an authentication server
Directory server manages JP1 authentication information	Managed by a directory server	Managed by a directory server	Managed by a directory server
Directory server manages JP1 user authentication information only	Managed by both an authentication server and a directory server	Managed by a directory server	Managed by an authentication server

JP1 users can be classified into JP1 user types or JP1 user authentication information management types according to their method of user authentication. The following table shows user authentication methods and corresponding JP1 user types.

Table 2–2: JP1 user types

User authentication method	JP1 user type
Directory sever linkage unused (Authentication server performs user authentication)	<i>Standard user</i>
Directory server manages JP1 authentication information	<i>DS user</i>
Directory server manages JP1 user authentication information only	<i>Linkage user</i>

Define every user to be a standard user, DS user, or linkage user on an authentication server. Two JP1 user types can be assigned to a JP1 user at the same time for the combinations below. Account administrators shall assign a JP1 user type through recognizing where its account is defined.

- Standard user and DS user[#]
- Standard user and linkage user

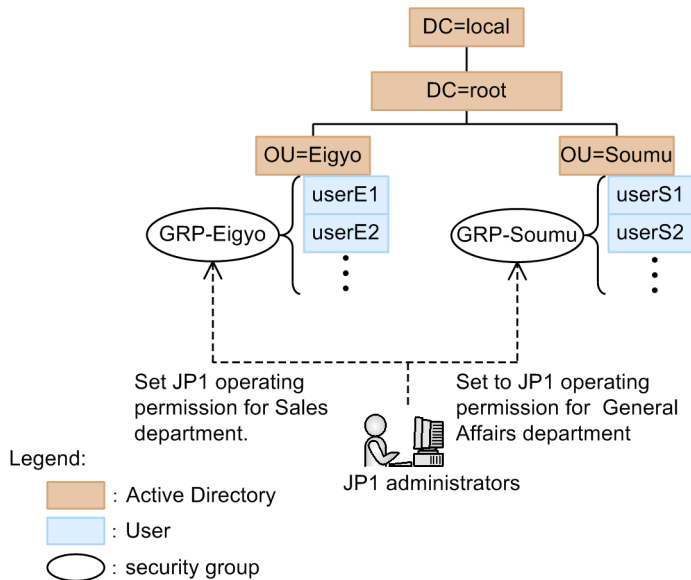
[#]:

User authentication is performed as a standard user if the name of the user for user authentication exists under both standard user and DS user.

DS users can perform the following operation:

- JP1 authentication information can be managed on a directory server.
JP1 authentication information (JP1 user authentication information and JP1 operating permission) is managed on a directory server. The account of the directory server (Active Directory) can be used as a JP1 user and can be managed together with JP1 operating permission.
- JP1 operating permission can be set in a security group of the Active Directory.
On the Active Directory, user accounts can be grouped into units for easy management by using a security group. By setting JP1 operating permission to a security group, JP1 operating permission can be also given to accounts to belong to the security group. Thus, JP1 operating permission can be easily set. The security group to which JP1 operating permission is given is called a *DS group*.
A security group can be organized to belong to a higher ranking security group, and JP1 operating permission given to the higher ranking security group can be also given to the security group.

Figure 2–5: JP1 operating permission setting to security groups



Linkage users can perform the following operation:

- JP1 authentication information's JP1 user authentication information can only be managed by a directory server. JP1 user authentication information is managed by a directory server. JP1 user name and JP1 operating permission are managed by an authentication server.

(1) Setting up linkage with a directory server

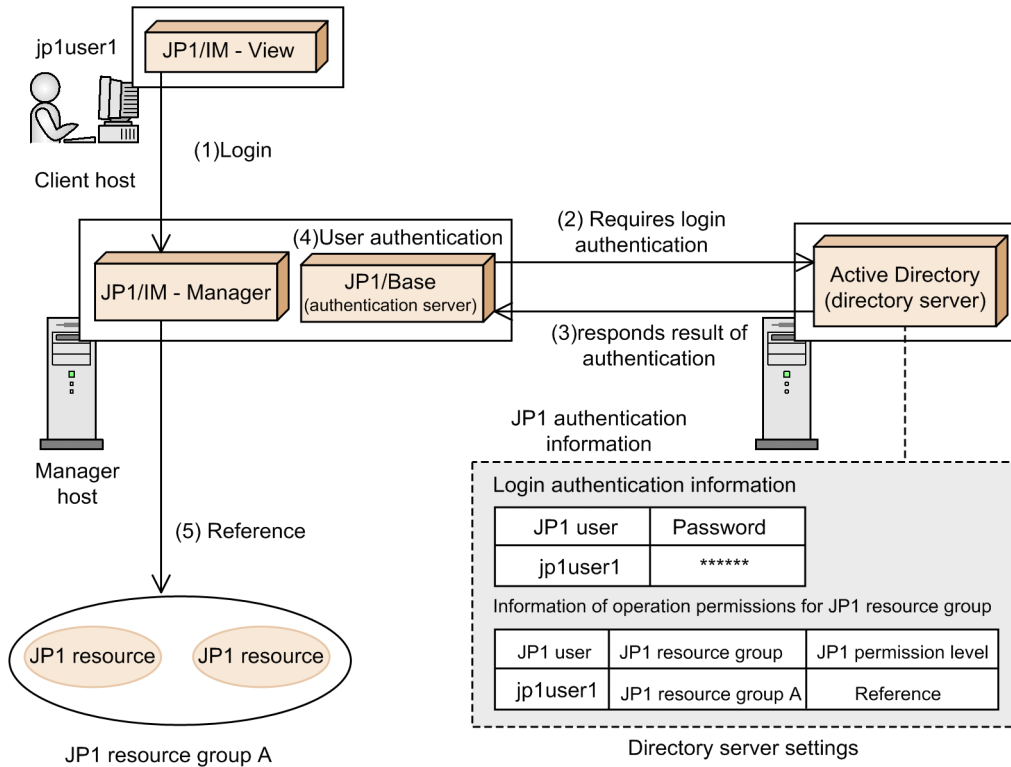
Directory server linkage is disabled by default. To link with a directory server, you will need to modify the default common definitions. For details on the settings, see [8.2 Setup for user authentication linking with the directory server \(Windows only\)](#).

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) Example of user authentication by linking with a directory server

The following figure shows an example of user authentication where JP1 authentication information is managed by a directory server.

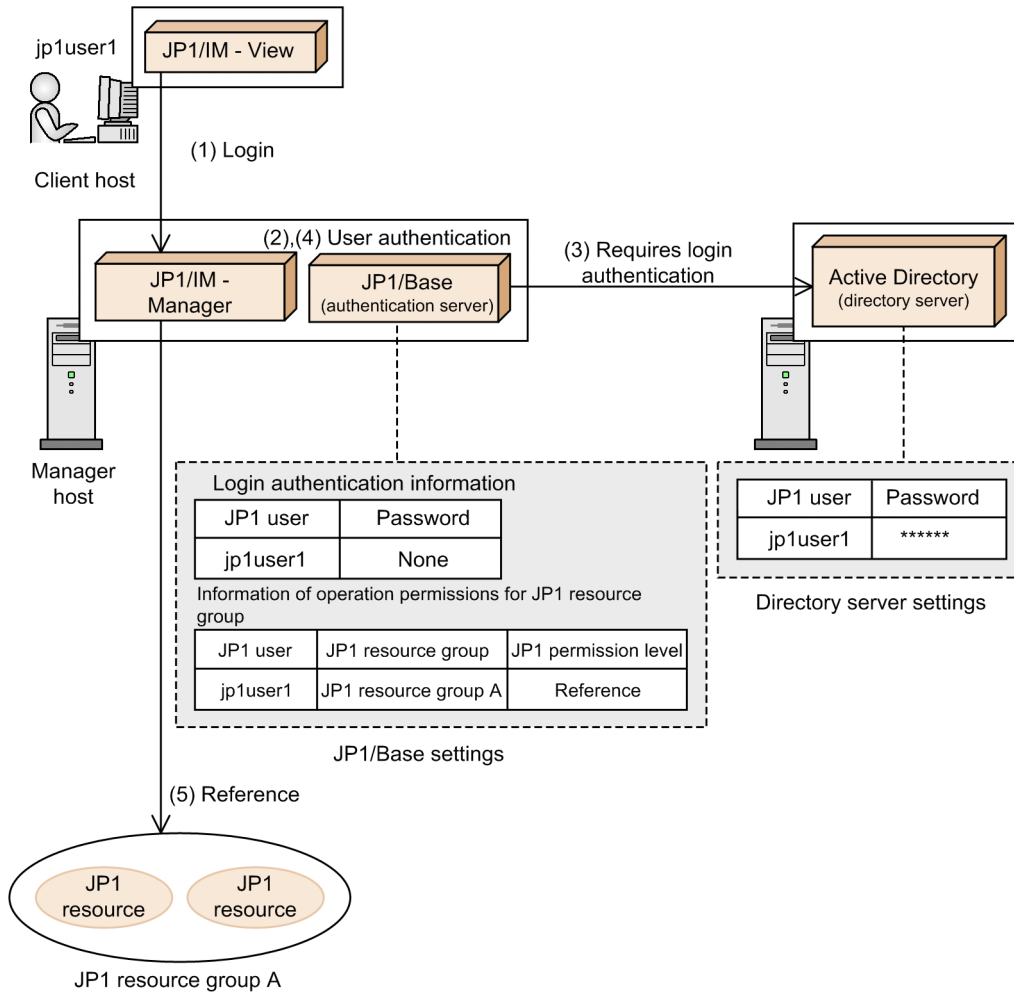
Figure 2–6: JP1Example of user authentication where JP1 authentication information is managed by a directory server



- (1) "jp1user1" logs in to JP1/IM - Manager from JP1/IM - View.
- (2) The authentication server requests the Active Directory to perform user authentication.
- (3) The Active Directory checks whether the "jp1user1" is registered based on the registered JP1 authentication information (JP1 user authentication information and JP1 operating permission), and then returns the authentication result to the authentication server.
- (4) If "jp1user1" is authenticated at login, the operation permission of "jp1user1" is returned to JP1/IM - Manager.
- (5) "jp1user1" can reference JP1 resources within "JP1 resource group A".

The following figure shows an example of user authentication where only JP1 user authentication information is managed by a directory server.

Figure 2–7: JP1Example of user authentication where only JP1 user authentication information is managed by a directory server



- (1) "jp1user1" logs in to JP1/IM - Manager from JP1/IM - View.
- (2) The authentication server performs user authentication for the logged-in "jp1user1". Based on the registered information, the authentication server checks if "jp1user1" is registered and determines the type of the user.
- (3) If "jp1user1" is a linkage user, the authentication server links with the directory server to perform user Authentication. The directory server compares the JP1 user authentication information of "jp1user1" with that on the directory server, and then returns the result to the authentication server.
- (4) If "jp1user1" is authenticated at login, the operation permission of "jp1user1" is returned to JP1/IM - Manager.
- (5) "jp1user1" can reference JP1 resources within "JP1 resource group A".

(3) Notes on user authentication by linking with a directory server

Sometimes user 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 users on a directory server

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

2.1.5 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

Note

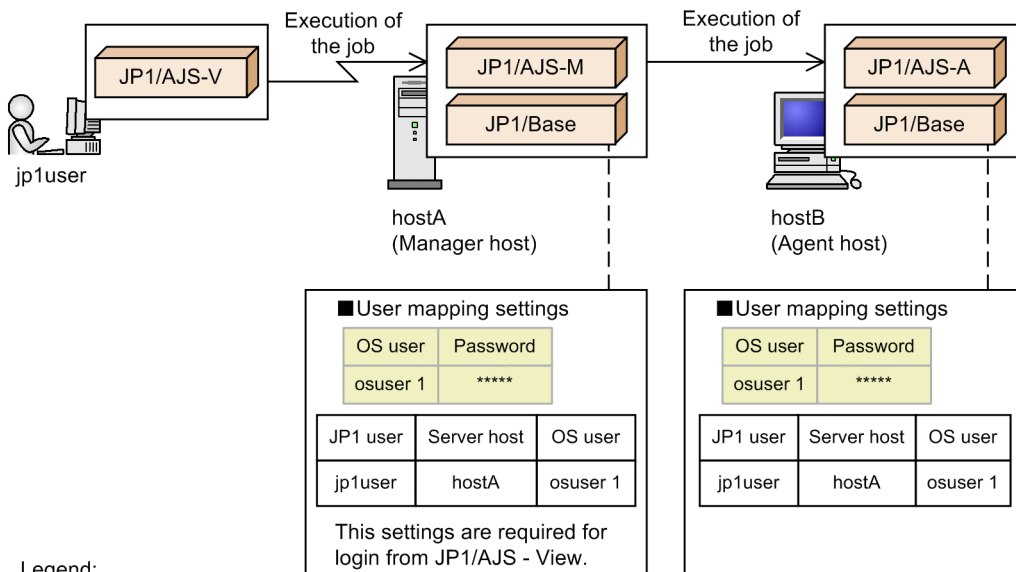
- In UNIX, only the OS user name is required for execution by an OS user. In Windows, however, since both an OS user name and a password are required, JP1/Base also manages OS passwords. Therefore, if you need to change the password of an OS user in Windows, you must also change the JP1/Base password information.

(1) Example of user mapping (in JP1/AJS)

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

Figure 2–8: Example of user mapping (in JP1/AJS)

● For JP1/AJS



Legend:

JP1/AJS-V : JP1/AJS - View

JP1/AJS-M : JP1/AJS - Manager

JP1/AJS-A : JP1/AJS - Agent

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

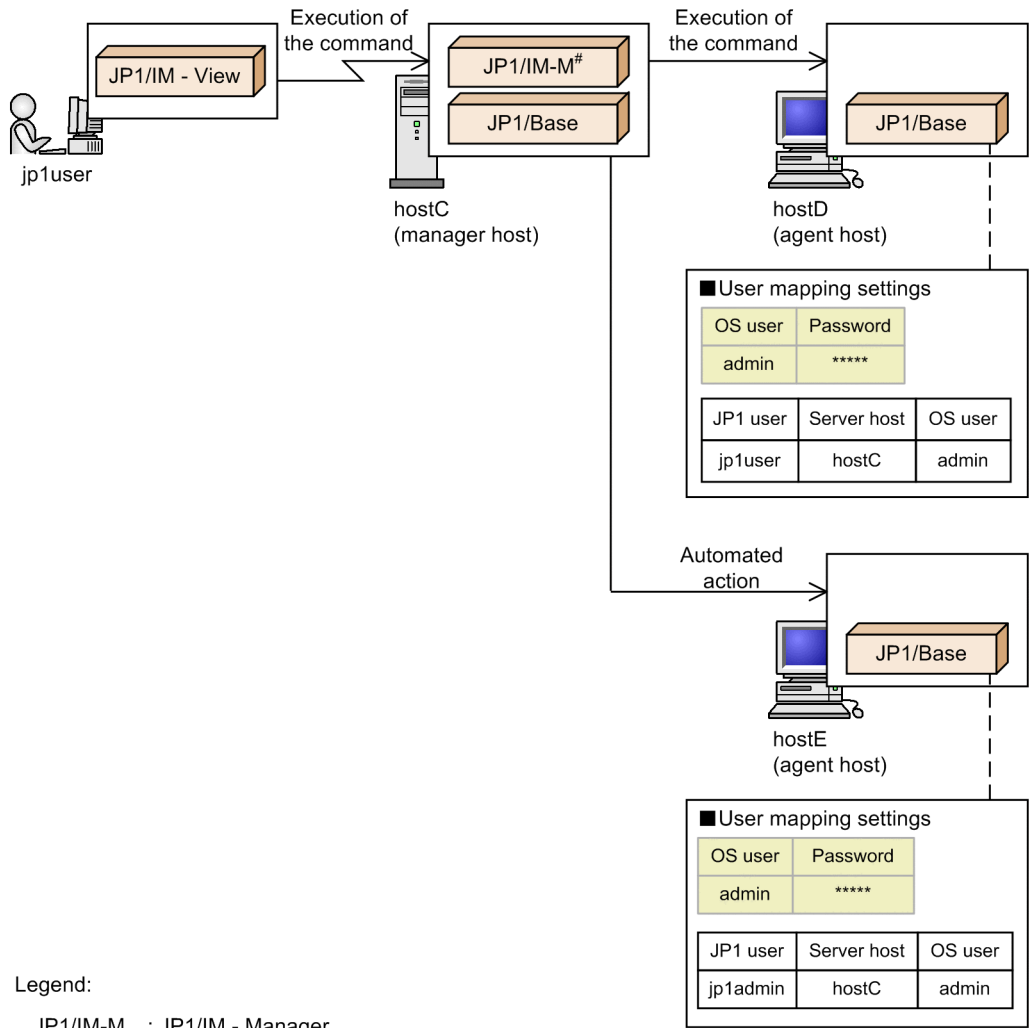
If you log in from JP1/AJS - View to JP1/AJS - Manager, mapping of JP1 users to OS users is also required on the host running JP1/AJS - Manager. Therefore, you must set up user mapping on HostA (the manager host) and HostB (an agent host that executes jobs). For details, see the manuals *JP1/Automatic Job Management System 3 Configuration Guide*.

(2) Example of user mapping (in JP1/IM)

The following diagram shows an example of user mapping in JP1/IM.

Figure 2–9: Example of user mapping (in JP1/IM)

● For JP1/IM



Legend:

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`.

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.

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

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

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.

To stop services, JP1/Power Monitor must be installed on the same machine.

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`).

2.3 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*.

2.3.1 Event service

An event service is functionality that registers and manages an event that occurs in the system as a JP1 event.

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.

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

2.3.2 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:

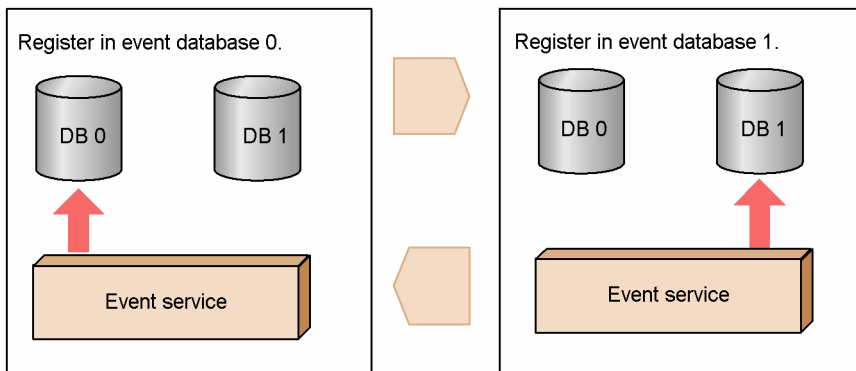
- Data (`IMEvent0.dat` and `IMEvent1.dat`)
- Indexes (`IMEvent0.idx` and `IMEvent1.idx`)
- Transfer information (`IMEvent0.fwd` and `IMEvent1.fwd`)
- Duplication prevention table (`IMEvent.rep`)

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.

(1) Swapping of event databases


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

Figure 2–10: Swapping of event databases



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 check the contents of the event database from the Event Console window of JP1/IM - View, or by using a command to output the database contents to a CSV file. For information on JP1/IM - View, see the manual *JP1/Integrated Management 3 - Manager Administration Guide*. For details on how to output the contents of the event database to a CSV file, see [10.3 Outputting the event database to a CSV file](#).

(2) 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 [11. Setting Up the Event Converters](#).

(3) Checking duplicate JP1 event 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.

(4) 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. The transfer records of JP1 events contain information required for searching the event database when checking for duplicate JP1 event registrations, such as the maximum value for the source event database serial number.

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.

If the event database is lost from the target host due to, for example, server replacement or disk failure, and the event database serial number is reset to 0 on the source host, during operation you can clear from the duplication prevention table the maximum value for the source event database serial number on the source host by issuing a JP1 event for clearing the duplication prevention table (user event) on the source host or the target host.

- JP1 event for clearing the duplication prevention table (user event)

Event ID: 7FFF8001

Message: DPT CLEAR EVENT

OBJECT_NAME: Source event server name (required only if the JP1 event is issued on the target host)

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.

2.3.3 JP1 events acquired by JP1/Base

Table 2–3: JP1 events acquired by JP1/Base

Event type	Description
JP1 events issued by JP1 programs	JP1/Base can acquire JP1 events issued by any JP1 program. It can also recognize JP1 events with the extended event attributes recognized by JP1/SES, a pre-version 5 program. JP1/Base can also acquire any events that can be acquired by JP1/IM (also a pre-version 5 program). For details on these events, see the manual for the relevant product.
JP1 events submitted to an event server by the <code>jevsend</code> or <code>jevsendd</code> commands	You can register JP1 events on an event server by executing the <code>jevsend</code> or <code>jevsendd</code> command. Unlike the <code>jevsend</code> command, the <code>jevsendd</code> command allows you to check whether the JP1 event has been registered on the event server. If you want JP1 events registered with the event server by the <code>jevsend</code> or <code>jevsendd</code> commands to appear in the Event Console window of JP1/IM - View, you must give the events a <i>severity</i> extended attribute. For details on these commands, see <i>jevsend</i> and <i>jevsendd</i> in <i>15. Commands</i> . By using the JP1 event issuing function, you can issue JP1 events directly from a user application. A user application can also acquire events directly by using the JP1 event acquisition function. For details, see the manual <i>JP1/Base Function Reference</i> .
Log files for application programs	JP1/Base can acquire JP1 events converted from information output to the log file of an application program. For details on the conversion process, see <i>11.1 Converting application program log files</i> .
Windows event logs	JP1/Base can acquire JP1 events converted from information output to Windows event logs. For details on the conversion process, see <i>11.2 Converting Windows event logs</i> .

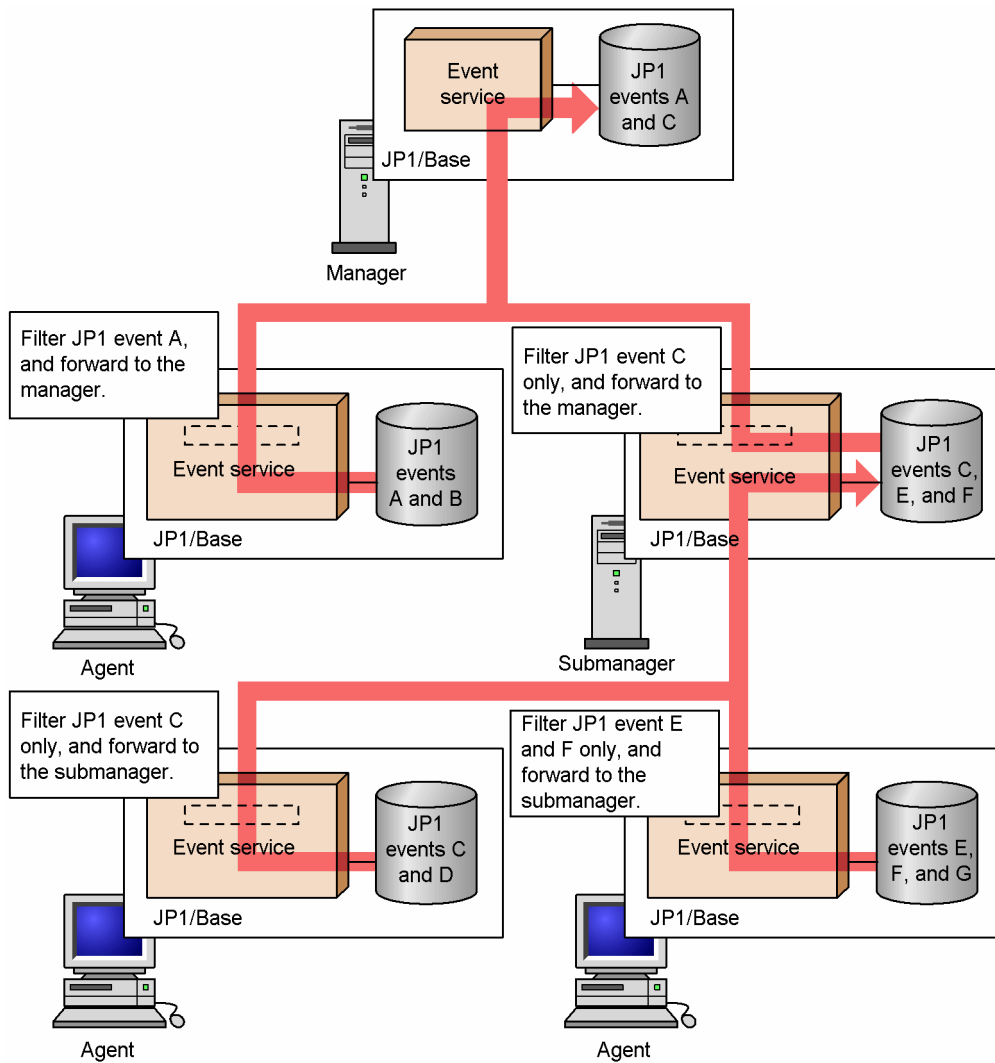
2.3.4 Forwarding JP1 events

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. The default forwarding settings file transfers important JP1 events to higher management servers 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 2–11: Example of forwarding JP1 events using an event filter



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 events transferred to a manager host can be viewed in JP1/IM - View. You can monitor the overall status of the system by logging in to the manager host from JP1/IM - View and viewing the JP1 events that have been forwarded. You can also perform an automated action for recovery in response to a JP1 event indicating a failure.

Resending JP1 events

If an attempt to forward a JP1 event fails due to an issue such as a temporary network fault or a shutdown of the event service at the destination, JP1/Base will try again by default. You can specify the retry interval and time limit in the event server settings file (`conf`).

2.4 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.

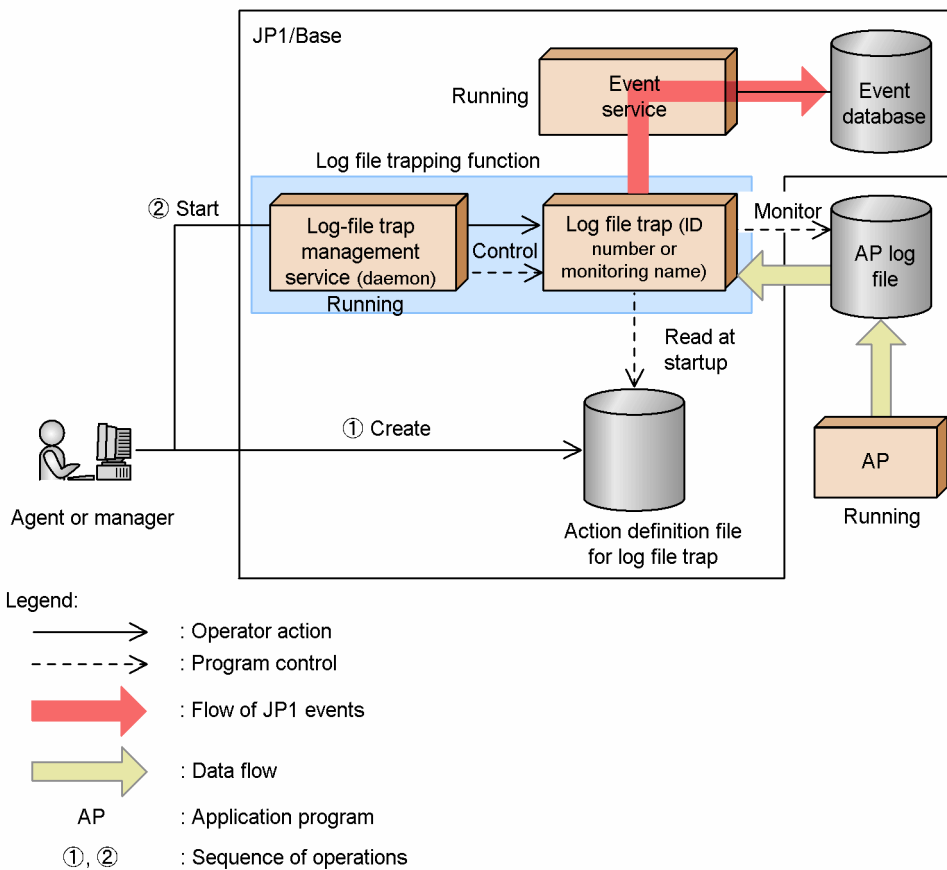
Event log trapping (Windows only)

Converts information output to Windows event logs into JP1 events.

2.4.1 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 2–12: 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. When you execute the command, the log-file trap management service (or daemon) generates log file traps which are then used 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.

If you execute the `jevlogstart` command without the `-m` option, messages containing a maximum of 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.

2.4.2 Prerequisites for a log file trap

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

- The character codes of the files or locale information (such as LANG) listed below used when executing the following command must be unified. However, if a file (hereafter called a *Unicode file*) formatted in Unicode (UTF-8 or UTF-16) is monitored in Windows, you must start a log file trap by executing the `jevlogstart` command with the `-g` option specified. At this time, create an action definition file for log file trapping in the language of the OS rather than Unicode.
 - 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.

- The event service and the log-file trap management service (or daemon) are both running.

In Windows, by default the event service and the log-file trap management service are configured to start automatically when Windows starts.

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 [7.2 Starting and stopping JP1/Base \(in UNIX\)](#).

2.4.3 Start and end of monitoring with a log file trap

Log file monitoring begins when you activate the log file trapping function via the `jevlogstart` command, and monitors the log files at set intervals. You can change the monitoring interval by specifying the `-t` option in the `jevlogstart` command. If you execute the `jevlogstart` command without the `-t` option, the monitoring interval is 10 seconds. The time at which log file monitoring stops depends on the options specified for the `jevlogstop` command.

For details on the commands, see [15. 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.

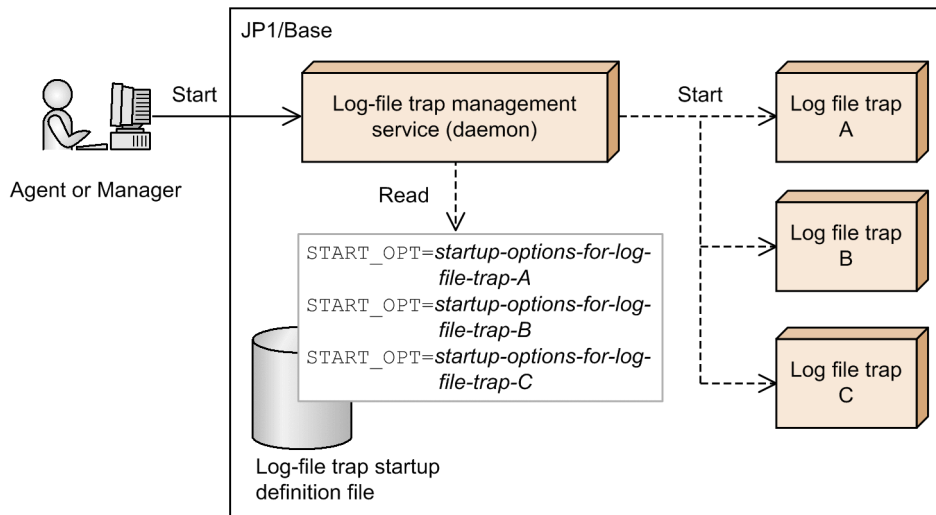
Starting and stopping log file traps

Use the `jevlogstart` and `jevlogstop` commands. 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 to be created.

By using a log-file trap startup definition file, you can configure log file trapping to start automatically when the log-file trap management service (or daemon) starts.

The following figure shows the process flow for starting log file trapping when using a log-file trap startup definition file.

Figure 2–13: Process flow for starting log file trapping by using a log-file trap startup definition file



Legend:

- >: Operator action
- - - ->: Program control

A log-file trap startup definition file specifies the log file traps to be started, and the startup options (for the `jevlogstart` command). When the log-file trap management service (or daemon) starts, it reads the contents of the log-file trap startup definition file and automatically starts the log file traps defined in the file.

You can also stop log file traps individually, or reload a specific action definition file. To do so, execute the command specifying the ID number output to standard output when the log file trap was activated, or the monitor name assigned to the log file trap when the log file trap was activated.

For details about the attributes of JP1 events converted by log file trapping, see [17.3.1\(27\) Details about event IDs specified in the ACTDEF parameter in the action definition file for log file trapping](#).

2.4.4 Types of log files that can be monitored

Log files in a variety of formats can be monitored by log file trapping. Check which file formats are supported, and specify the appropriate log file format in the action definition file for log file trapping.

The log file formats supported for monitoring are described below. For the general procedure for checking the log file format, see [11.1.1 Checking the format of application program log files](#).

Log files in the following format can be monitored:

- Sequential file (SEQ)
- Sequential file (SEQ2)
- Sequential file (SEQ3)
- Wrap-around file (WRAP1)
- Wrap-around file (WRAP2)
- Multi-process trace file (HTRACE)
- UPD type log files (UPD)

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

(1) Type of log files that can be monitored (SEQ)

Sequential file (SEQ)

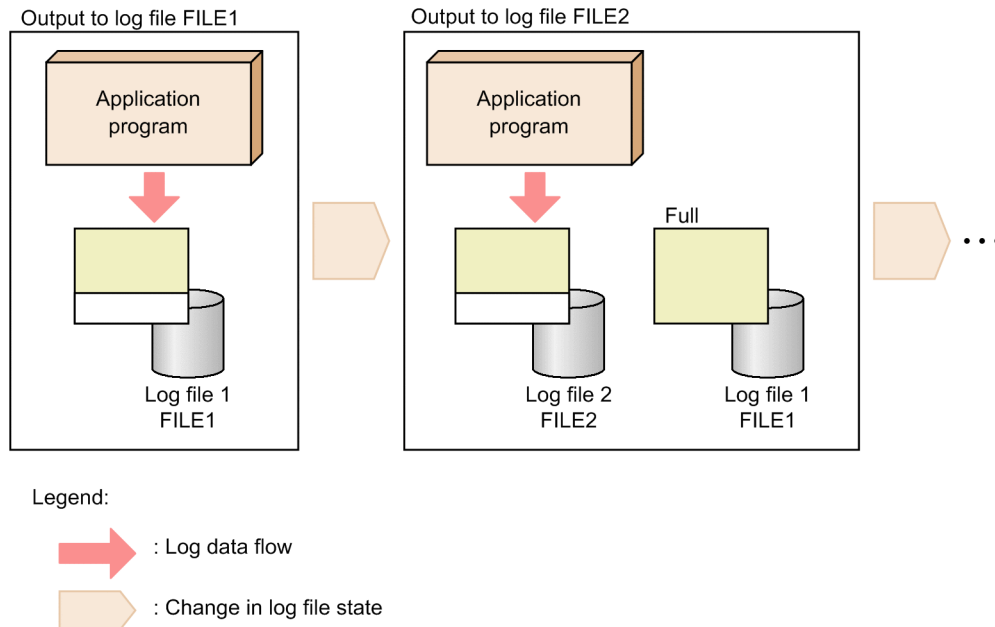
A log file that is written to continuously or, when it reaches a certain size, is replaced with a new log file with a different file name.

In the action definition file for log file trapping, specify SEQ.

Log files of any size can be monitored.

The following figure illustrates the behavior of a sequential file (SEQ).

Figure 2–14: Behavior of a sequential file (SEQ)



(2) Type of log files that can be monitored (SEQ2)

Sequential file (SEQ2)

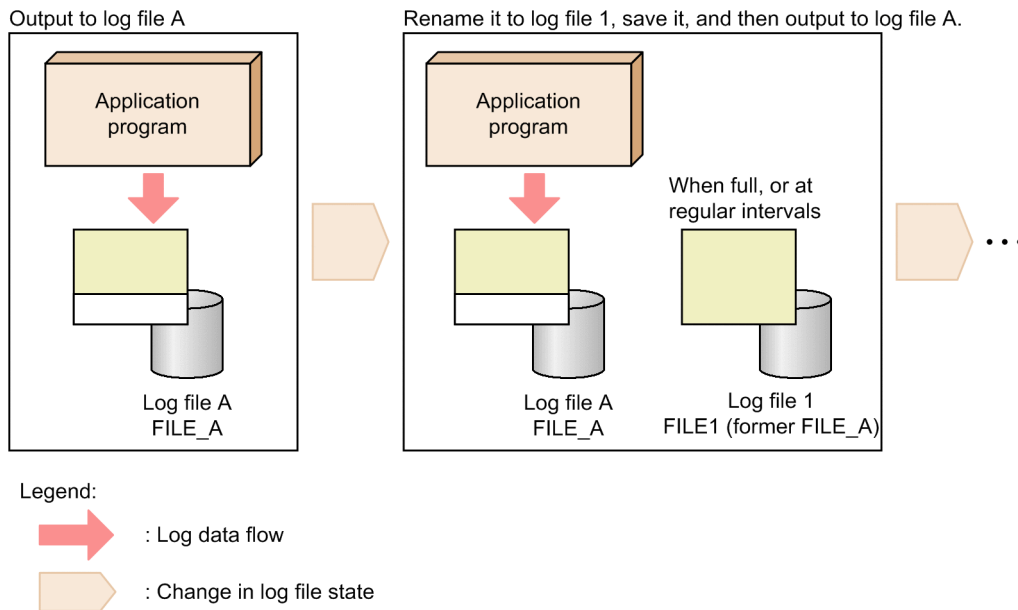
- In Windows:
A log file that is renamed, and then replaced by a new log file created with the same name as the original file.
- In UNIX:
A log file that is renamed or deleted, and then replaced by a new log file created with the same name as the original file.

In the action definition file for log file trapping, specify SEQ2.

Log files of any size can be monitored.

The following figure illustrates the behavior of a sequential file (SEQ2).

Figure 2–15: Behavior of a sequential file (SEQ2)



(3) Type of log files that can be monitored (SEQ3)

Sequential file (SEQ3)

- Windows only

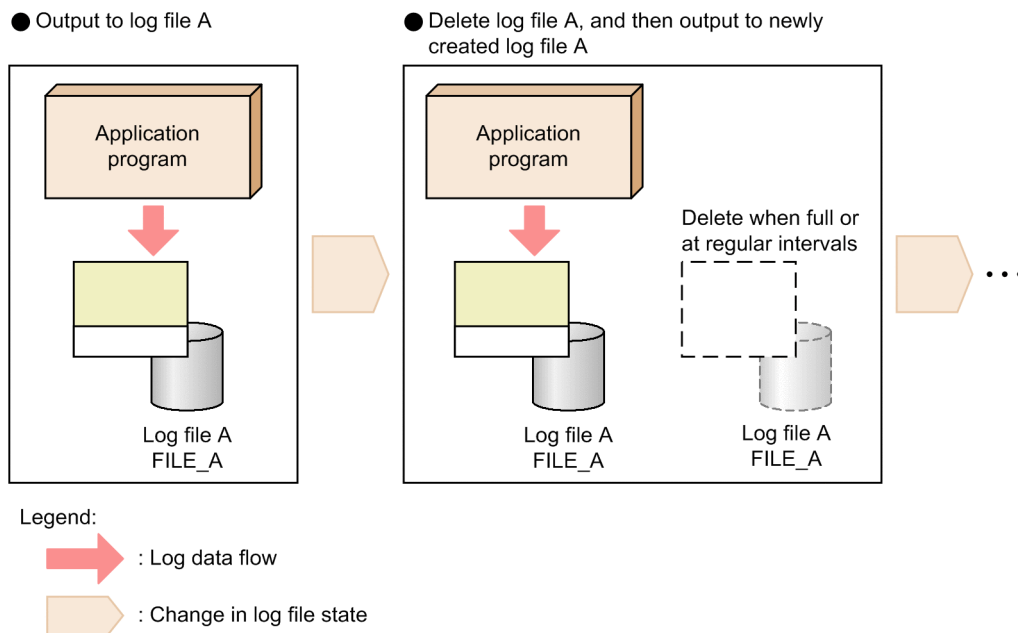
Upon reaching a certain size, the file is deleted and log data is written to a new file with the same name as the deleted file.

To monitor this type of log file in Windows, specify SEQ3 in the action definition file for log file trapping. You cannot monitor this type of sequential file by specifying SEQ2 in the action definition file for log file trapping in Windows.

Log files of any size can be monitored.

The following figure illustrates the behavior of a sequential file (SEQ3).

Figure 2–16: Behavior of a sequential file (SEQ3)



(4) Type of log files that can be monitored (WRAP1)

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.

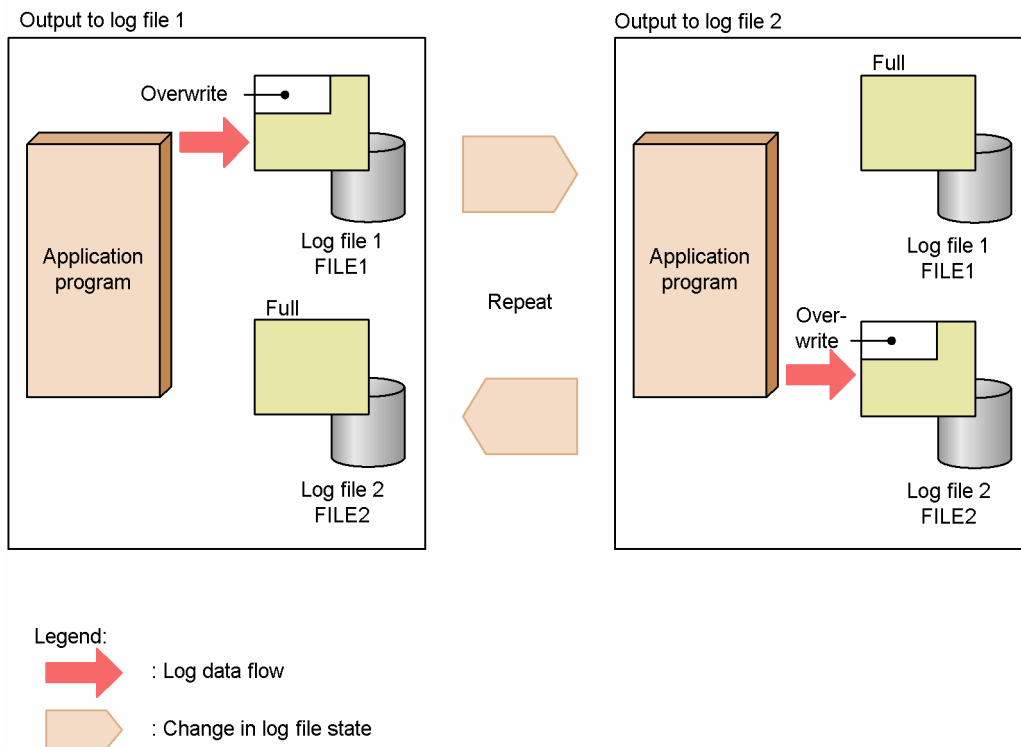
In the action definition file for log file trapping, specify WRAP1.

Log files that are smaller than 2 gigabytes can be monitored.

Free disk space that is at least as large as the file to be monitored is required.

The following figure illustrates the behavior of a wrap-around file (WRAP1).

Figure 2–17: Behavior of a wrap-around file (WRAP1)



(5) Type of log files that can be monitored (WRAP2)

Wrap-around file (WRAP2)

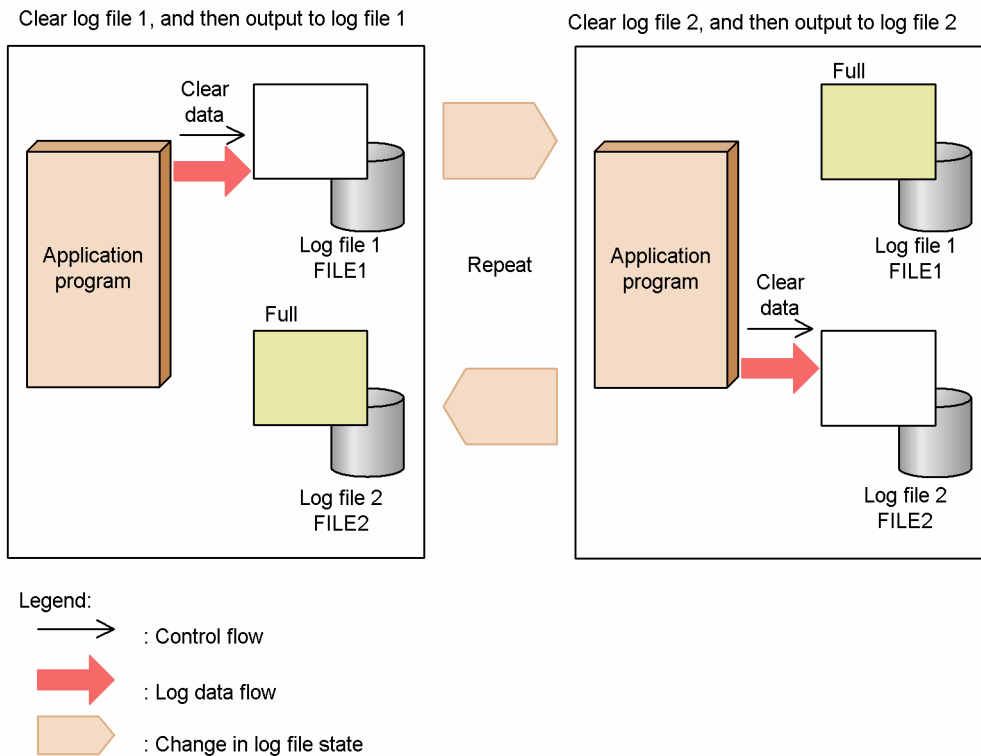
When the file reaches a certain size, data is wrapped around from the end, all the data is deleted and the new log data is again written from the top of the file.

In the action definition file for log file trapping, specify WRAP2.

Log files of any size can be monitored.

The following figure illustrates the behavior of a wrap-around file (WRAP2).

Figure 2–18: Behavior of a wrap-around file (WRAP2)



(6) Type of log files that can be monitored (HTRACE)

Multi-process trace file (HTRACE)

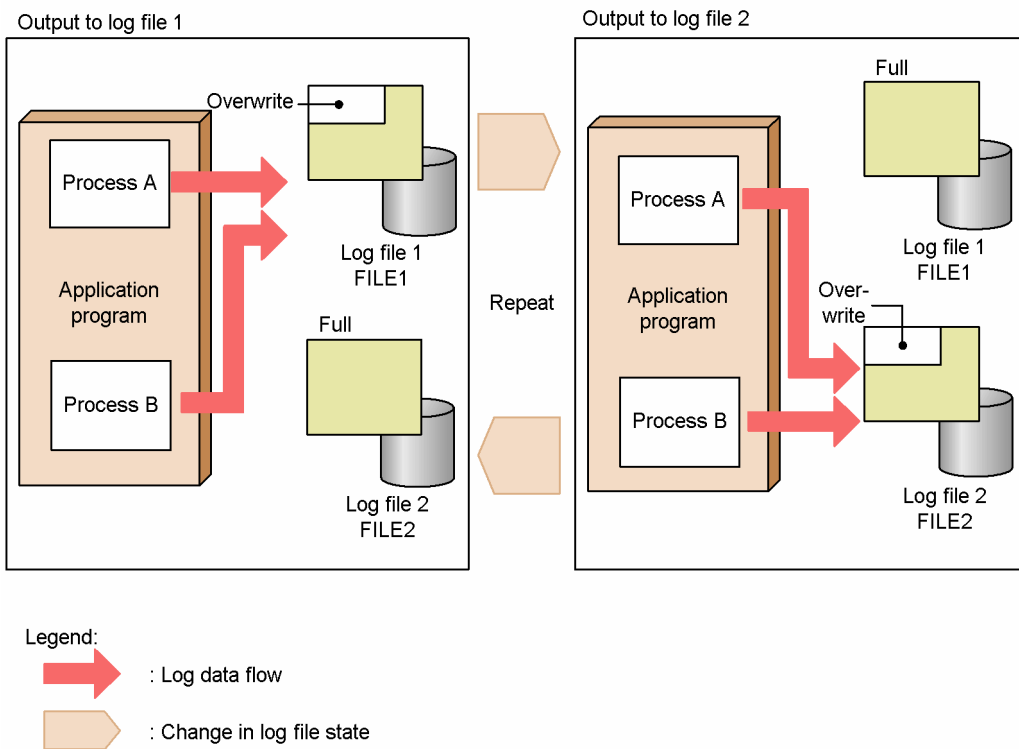
Hitachi middleware-products, such as Cosminexus, use this log file format. The log file format is a group of fixed-size trace files that are shared by multiple processes as memory-mapped files.

In the action definition file for log file trapping, specify `HTRACE`.

Log data is written to a multi-process trace file in the same way as for a wrap-around file (WRAP1). For a multi-process trace file (HTRACE), when the file size reaches a certain upper limit (the maximum limit is 16 megabytes), data is wrapped around and written from the beginning 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 2–19: Behavior of a multi-process trace file (HTRACE)



(7) Type of log files that can be monitored (UPD)

UPD type log files (UPD)

Use this approach to monitor log files whose file name contains values (such as dates) that change from time to time. You can account for the unknown value by using wildcards.

When the log file trap starts, the log-file trap management service (or daemon) monitors the most recently updated log file of those that match the wildcard pattern. While the trap is active, the service (or daemon) keeps switching its monitoring target to the file matching the wildcard pattern that has the most recent update time of those created during the monitoring process. For this process to work, the update time must be updated each time data is written to the file.

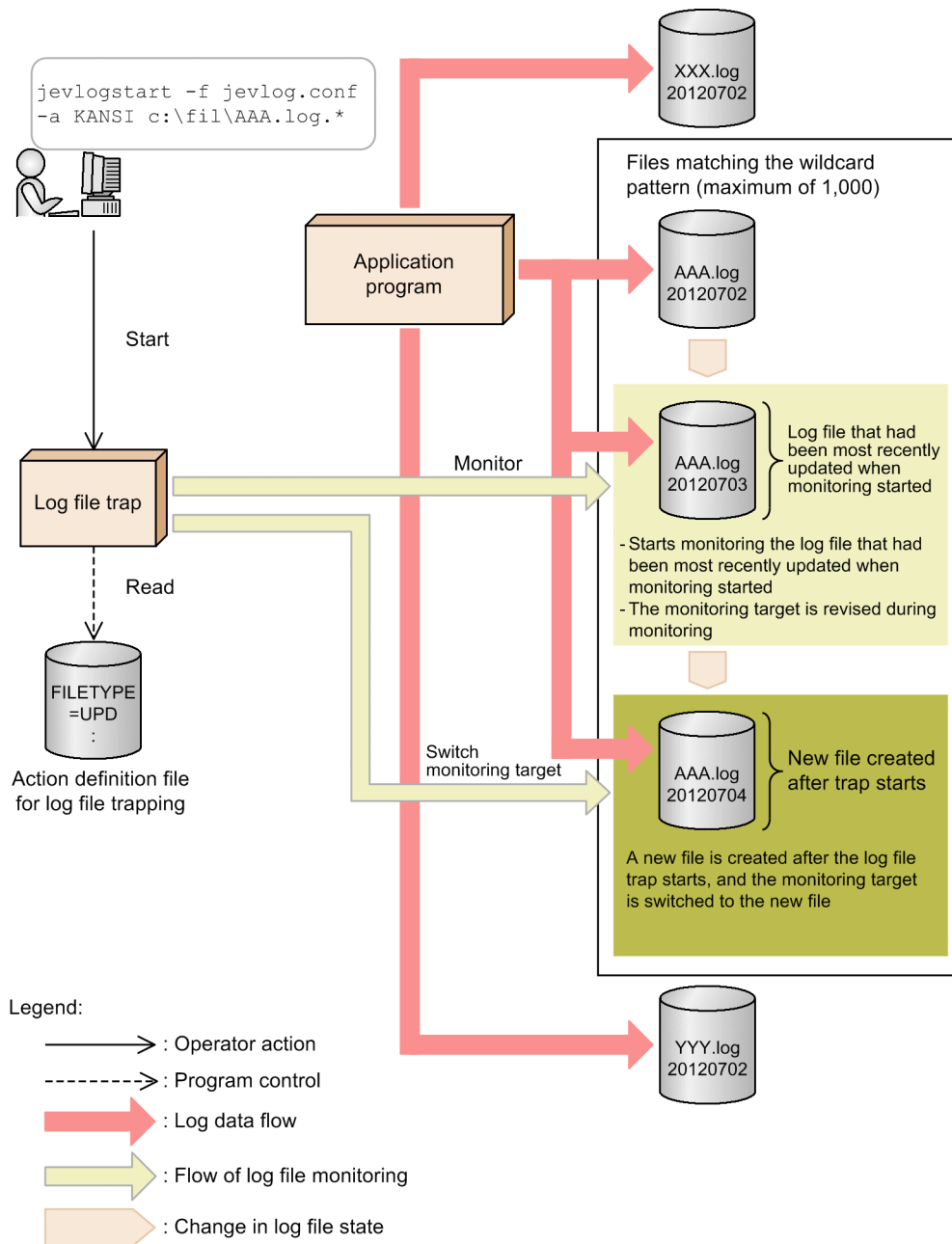
The log-file trap management service (or daemon) can monitor files that are written to continuously, and files that are replaced with a new log file with a different name when they reach a certain size (sequential files).

In the action definition file for log file trapping, specify UPD.

Log files of any size can be monitored.

The following figure illustrates the behavior of a UPD type log file.

Figure 2–20: Behavior of a UPD type log file



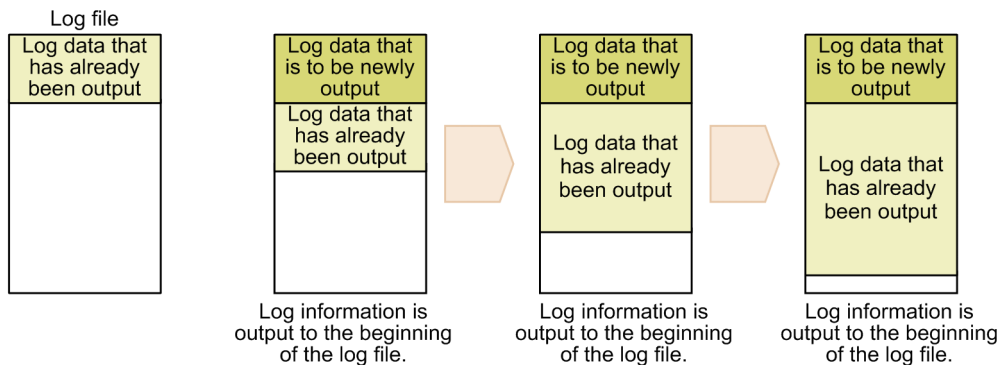
1. When executing the start command (`jevlogstart`), include wildcards in the name of the monitoring target file.
2. Files whose file name matches the wildcard pattern become potential monitoring targets for the log-file trap management service (or daemon), to a maximum of 1,000 files.
If more than 1,000 files match the wildcard pattern, the log file trap fails to start. If the number of files surpasses this limit while monitoring is in progress, JP1/Base outputs an error message and stops the log file trap.
3. At startup, the log file trap identifies the log file with the most recent update time from among the potential monitoring targets, and starts monitoring the file.
4. The log file trap reviews the monitoring target file in each monitoring interval (1 second), checking whether a new file has been created.
5. If a new file has been created, the service (or daemon) finishes processing any backlog before switching its monitoring target to the new log file.

The monitoring target will only switch if a new log file is created, not if an existing file is updated. If there are several new files, the service (or daemon) determines which file was updated most recently and designates that file as the monitoring target.


2.4.5 Types of log files that cannot be monitored

The following types of log files cannot be monitored by the log file trapping function:

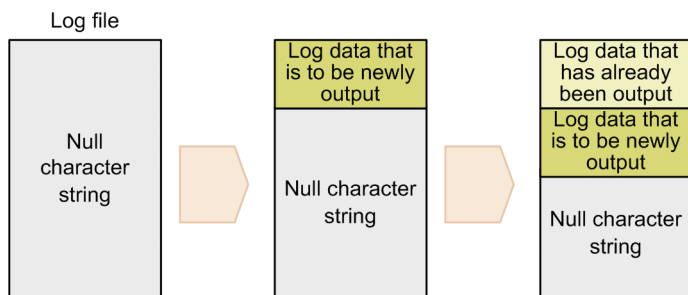
- Files in which log information is recorded to the top of the file each time




Legend:

 : Flow of status changes of the log file

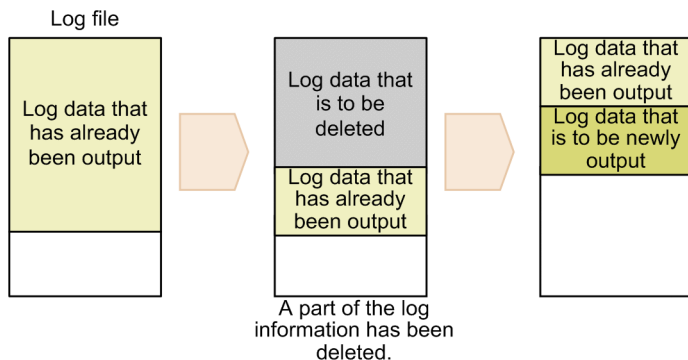
- Files that are filled with null characters that were output during creation of the files, and in which null characters are overwritten with log information each time the log information is output (except for monitoring of a multi-process trace file (HTRACE))




Legend:

 : Flow of status changes of the log file

- Files in which only a part of the log information that has already been output is deleted when data is wrapped around



Legend:

 : Flow of status changes of the log file

- 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`) or a UPD type log file, it references the date and time when the file was last modified. Monitoring this type of file might cause the log file traps to operate incorrectly.
- Files that contain binary data
A log file that contains records with binary data other than the end-of-line character.
- Files with unpredictable names (excluding UPD type log files)
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. A log file cannot be monitored if it is not accessible in read mode. In Windows, some logging programs write log data to files in lock mode. In such a case, the logging programs might fail to write log data because they cannot lock files.
- File output in a language not supported in JP1/Base
In Windows, JP1/Base supports the following languages: MS932, Unicode (UTF-8 and UTF-16), and C. For details about the languages supported by JP1/Base in UNIX, see [3.4.2 Setting the language \(for UNIX\)](#).

When monitoring sequential files (`SEQ3`):

A log file trap might be unable to monitor log entries correctly if the program that outputs the log information does not meet the following criteria:

- After outputting log data, the program does not delete the log file for a certain period of time (at least one second longer than the monitoring interval).

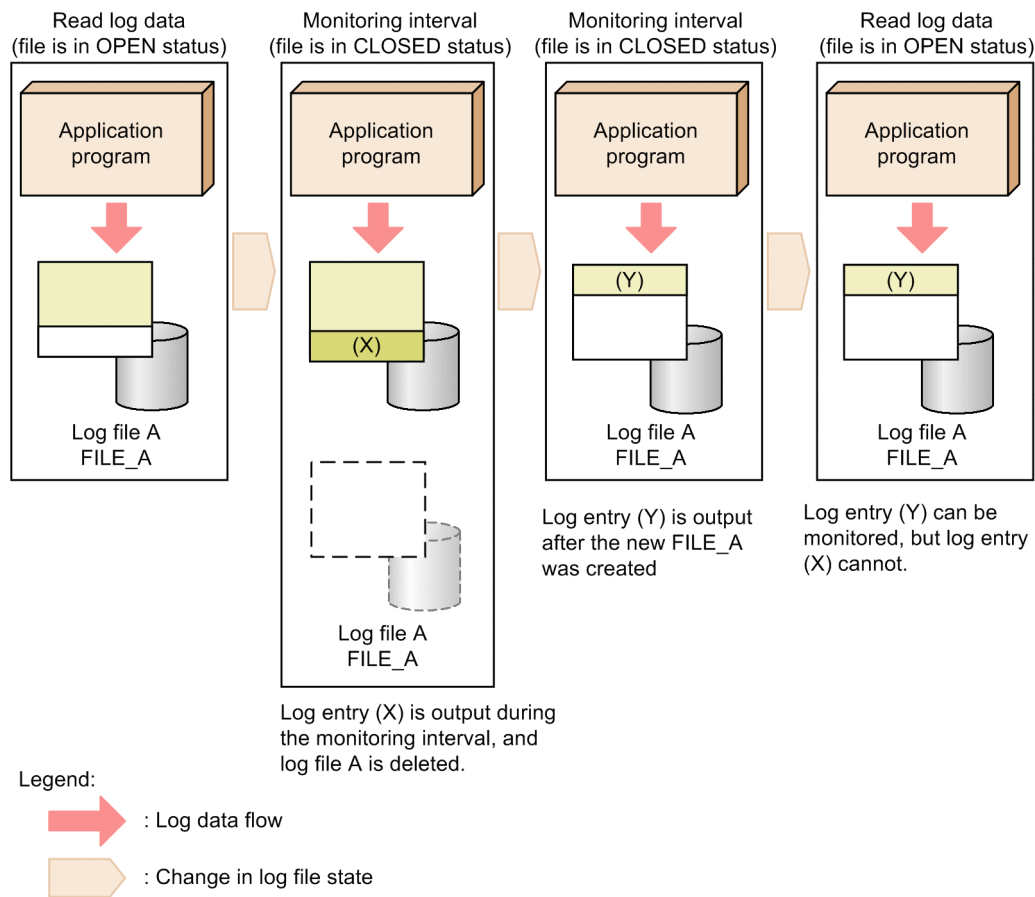
As shown in Figure 2-22, if the program deletes the log file immediately, the log file trap might not have time to read the logs that were output before the file was deleted.

- If an error occurs when the program switches the output log file (by deleting or re-creating the file), the program tries again.

In Windows, an attempt by a program to switch log files might fail while a log file trap is reading the current log file (that is, while the file is *open*).

During the monitoring interval, the log file trap leaves the log file *closed*. This gives the outputting program time to retry the operation if log file switching fails. Thus, log output might fail if the application program does not have the ability to retry log switching.

Figure 2–21: Scenarios in which log output to sequential files (SEQ3) cannot be monitored



2.4.6 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:

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

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).

2.4.7 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.

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

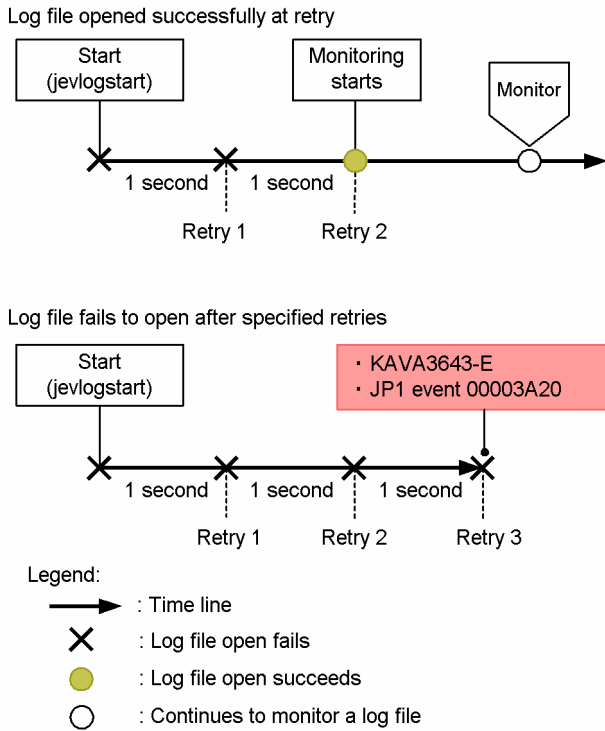
The log file that will be monitored opens when you start a log file trap using the `jevlogstart` command. If the file has been locked by the updating program, it cannot be opened and monitoring will not start. In this case, the log file trapping function will try to open the log file again. You can reconfigure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

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 [17.3.1\(14\) 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 2–22: Example of the retry process when a log file cannot be opened for monitoring



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

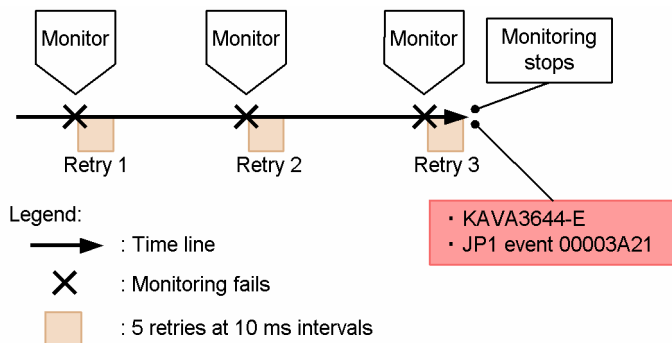
The log file trapping function retries five times at 10-millisecond intervals when it fails to read a log file during monitoring. If monitoring has not recovered after five retries, the trap is suspended until the next monitoring time. If the trap is still unable to open the file the next time it attempts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

A group of 5 retry attempts performed at 10 millisecond intervals is counted as one set, and retry attempts are considered in terms of sets. You can specify a threshold value for how many retry sets to perform in the action definition file for log file trapping. If you do not specify a threshold value in the definition file, log file trapping function retries the operation until 100 sets have been completed.

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 [17.3.1\(15\) 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 2–23: Example of the retry process when a log file cannot be read during monitoring



2.4.8 Reattempting to connect to the event service (log file trap)

If a log file trap cannot establish a connection to the event service, whether the log file trapping function tries again depends on the contents of the action definition file for log file trapping. 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. If you do not specify a retry count for a particular log file trap in the action definition file for log file trapping, attempts to establish a connection will be made three times at 10-second intervals.

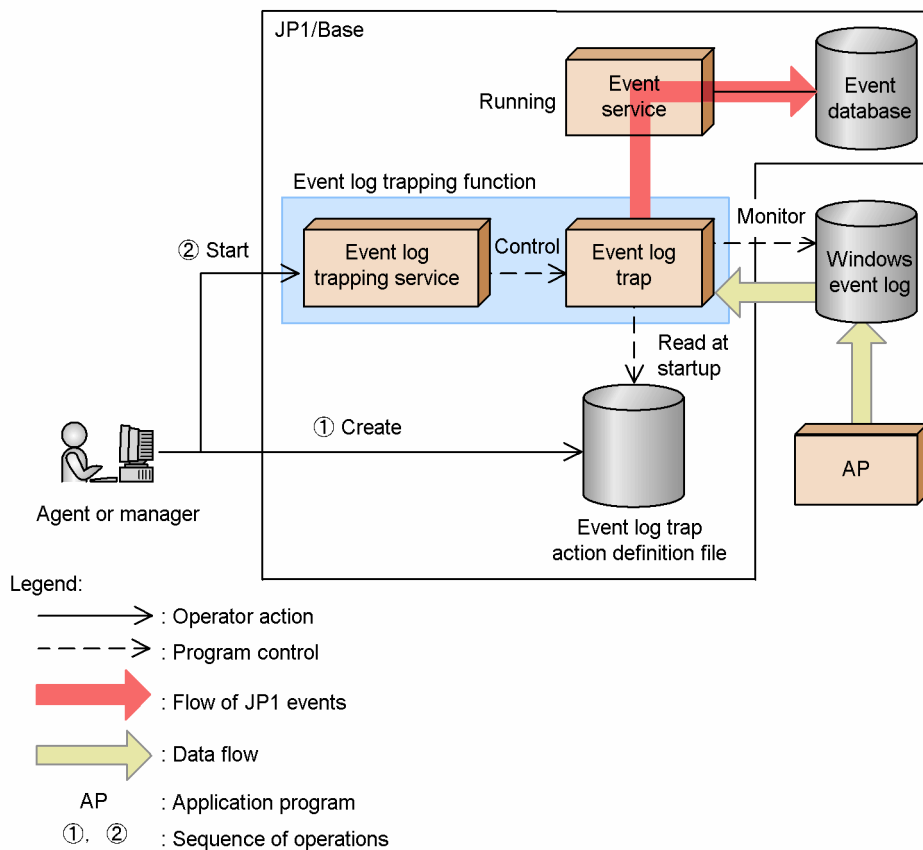
The JP1 events converted during a retry are saved in the system up to a specified maximum number. When this maximum is reached, all subsequent JP1 events are deleted.

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 [17.3.1\(13\) Details about event ID 00003A10](#).

2.4.9 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.

Figure 2–24: 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.

An event ID and/or trap name can be assigned to each monitoring condition that event log trapping uses to convert log data into JP1 events. The event ID or trap name allows you to determine the monitoring condition that was used for conversion to a JP1 event.

The severity level of a JP1 event converted from an event log entry corresponds to the type of the event log entry.

Although the event service is set to start automatically when the system starts by default, the event log trap service does not start 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.

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 about JP1 event attributes, see *17.3.1(26) Details about event ID 00003A71 or the event ID specified in the filter of the action definition file for event log trapping*.

2.4.10 Start and end of monitoring in event log trap

Event log trapping monitors the event log in real time. 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.

2.4.11 Reattempting to connect to an event service (event log trap)

By preconfiguring the action definition file for event log trapping (`ntevent.conf`), you can reattempt to connect an event service if connection to the event service fails when event log trapping starts or event log data is trapped.

2.5 Suppressing forwarding of large numbers of events

If a large number of JP1 events occur on a monitored agent in an integrated management system using JP1/IM, you can suppress event forwarding from the agent to the manager (JP1/IM - Manager). Suppressing the forwarding of large numbers of events can reduce the load on the manager.

2.5.1 Large numbers of events

A *large number of events* refers to many unexpected JP1 events that occur over a short period. Such a large number of JP1 events might occur after failure on an agent host, or when a log file trap outputs a large amount of monitored log data.

2.5.2 Precautions against large numbers of events

If a large number of JP1 events occur on a monitored agent in an integrated management system using JP1/IM, the events are forwarded to the manager, which might become overloaded. As a precaution, you can use the manager to suppress such large numbers of events or set a threshold to automatically suppress forwarding of large numbers of events.

- Using the manager to suppress large numbers of events
You can use the event-forwarding suppression command (`jevagt fw` command) to suppress event forwarding from a specific agent.
- Setting a threshold to automatically suppress forwarding of large numbers of events
You can set a threshold to detect large numbers of events, and automatically suppress event forwarding.



Note

If a log file trap is issuing large numbers of JP1 events, you can stop the corresponding log file trap from the manager. To selectively stop a log file trap on an agent from the manager, you can use the IM configuration management functionality. If you use the IM configuration management functionality, you can stop the process of the log file trap to be suppressed from the Display/Edit Profiles window in the IM configuration management viewer. For details, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

2.5.3 Using a manager to suppress event forwarding from an agent with large numbers of JP1 events

You can use the manager to suppress event forwarding from an agent on which large numbers of JP1 events are occurring. To do so, use the JP1/Base event-forwarding suppression command (`jevagt fw` command) from the manager. For details on the `jevagt fw` command, see [jevagt fw](#) in *15. Commands*.

The following describes the main functionality of the event-forwarding suppression command (`jevagt fw` command).

- Setting up event forwarding suppression
 - Suppressing event forwarding
Changes the event forwarding setting for a suppressed agent so that forwarding from the agent is suppressed.
 - Discarding received events

Discards JP1 events that are forwarded from a suppressed agent, without storing them in the event database of the manager.

- Stopping event forwarding suppression

Reverts the event forwarding setting for an agent whose event forwarding is currently suppressed back to its original setting.

- Checking event forwarding suppression status

Outputs the status for each agent whose event forwarding is currently suppressed.

By using the above functionality, you can promptly react to large numbers of events by using the manager to control event forwarding from an agent.

To use this functionality, the JP1/Base version of the manager host (host on which JP1/IM - Manager is installed) must be 10-50 or later. In addition, JP1/Base version of the agent host to be suppressed must be 08-00 or later.

A maximum of 10,000 agents can be subject to this event-forwarding suppression functionality. Note that event forwarding on an agent other than those managed by the configuration definition can also be suppressed.

(1) JP1 events that are subject to suppression (event forwarding suppression by using the `jevagtfw` command)

When the `jevagtfw` command is used to suppress event forwarding, JP1 events that are subject to the suppression are forwarded according to the settings in the forwarding setting file (`forward`).

The following JP1 events are not subject to suppression:

- Address-specified forwarding events:

Address-specified forwarding events include the following JP1 events:

- JP1 events that are forwarded to a destination event server specified by the `jevsend` or `jevsendd` commands
- JP1 events that are forwarded to a specific host by a program linking with an event service (for example, a JP1/AJS event-sending job) without using the forwarding setting file (`forward`).

- Automatic forwarding events:

These are events that are forwarded even when they do not match the filtering conditions of the forwarding setting block specified in the forwarding setting file (`forward`).

Automatically forwarded events include the following JP1 events:

- Event reporting of JP1/Base startup (00004724)
- Event reporting of JP1/Base shutdown (00004725)
- Event reporting of a threshold-based suppression (00003D0B)
- Event reporting of a stop of a threshold-based suppression (00003D0C)
- Event reporting of a stop of all threshold-based suppressions (00003D0D)
- Event reporting of the continuation of threshold-based suppressions (00003D0E)

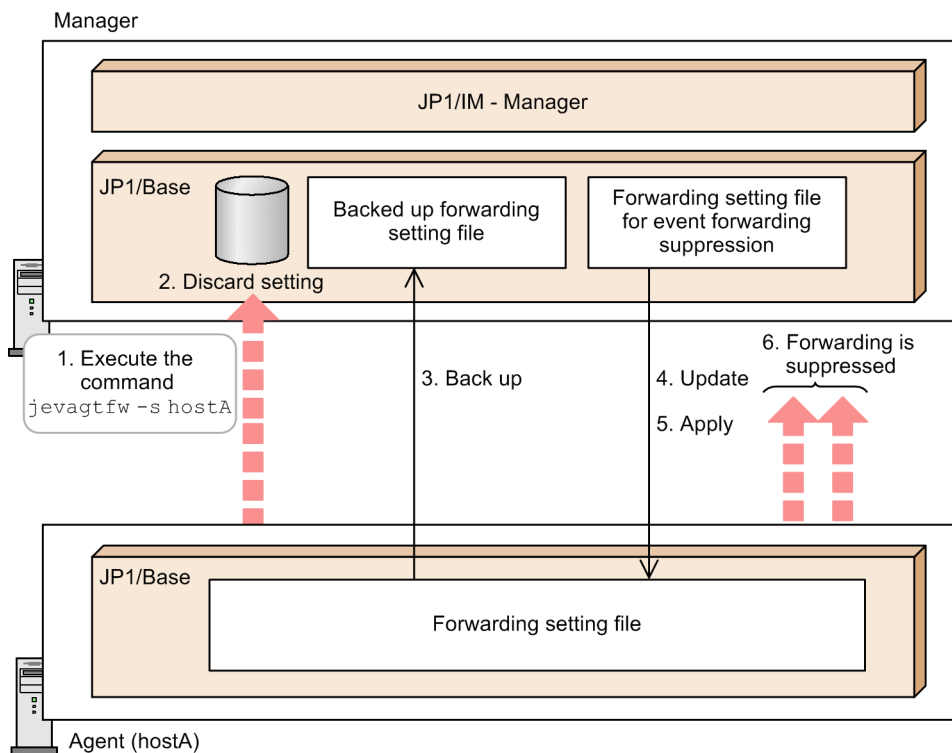
Note that if `auto-forward-off` flag is specified in the `options` parameter in the event server settings file (`conf`), the automatic forwarding events become subject to suppression in the same way as normal events.

(2) Setting up event forwarding suppression


Use the `jevagt fw` command with the `-s` option specified to set up event forwarding suppression in the event forwarding settings for a suppressed agent. Also specify settings to discard JP1 events forwarded from the suppressed agent, without storing the events in the event database of the manager.

The following diagram shows the process flow for setting up event forwarding suppression by using the `jevagt fw` command.

Figure 2–25: Process flow for setting up event forwarding suppression by using the `jevagt fw` command



Legend:

 : Large numbers of JP1 events subject to suppression

1. Execute the `jevagt fw` command with the `-s` option specified.
2. Specify settings to discard events received from a suppressed agent.
3. Back up the information in the forwarding setting file (`forward`) on the agent.
4. Send the forwarding setting file for event forwarding suppression (`forward_suppress` file or other forwarding suppression definition file) to the agent, and update the forwarding setting file (`forward`).^{#1}
5. Reload the updated forwarding setting file (`forward`) and apply it.^{#2}
6. Event forwarding is suppressed according to the forwarding setting file (`forward`).

#1: If sending the forwarding setting file for event forwarding suppression file (`forward_suppress` file or other forwarding suppression definition file) fails due to a communication error, the event forwarding suppression process is canceled. The status of the forwarding setting file (`forward`) on the agent remains unchanged from before the command is executed.

#2: If applying the updated forwarding setting file (`forward`) fails, send the backed up forwarding setting file (`forward_backup`) to the agent and apply (`restore`) it. If the restoration fails, the following message is output:

```
KAJP1434-E: Failed to restore the file forward to host-name. (file = file-name)
```

- Suppressing event forwarding

Set up event forwarding suppression on an agent. This corresponds to steps 3 to 6 in Figure 2-26.

- Discarding received events

Discards the JP1 events forwarded from a suppressed agent without storing the events in the event database of the manager. This corresponds to step 2 in Figure 2-26.

JP1 events that are subject to discard

JP1 events that are subject to discard are those that are forwarded according to the settings in the forwarding setting file (`forward`). Address-specified forwarding events and automatic forwarding events are not subject to discard. For details on address-specified forwarding events and automatic forwarding events, see *(1) JP1 events that are subject to suppression (event forwarding suppression by using the `jevagtfw` command)*.

A JP1 event forwarded via a submanager from an agent to the manager is also subject to discard, if the JP1 event is issued by a suppressed agent.

Excluding a specific JP1 event from discarded events

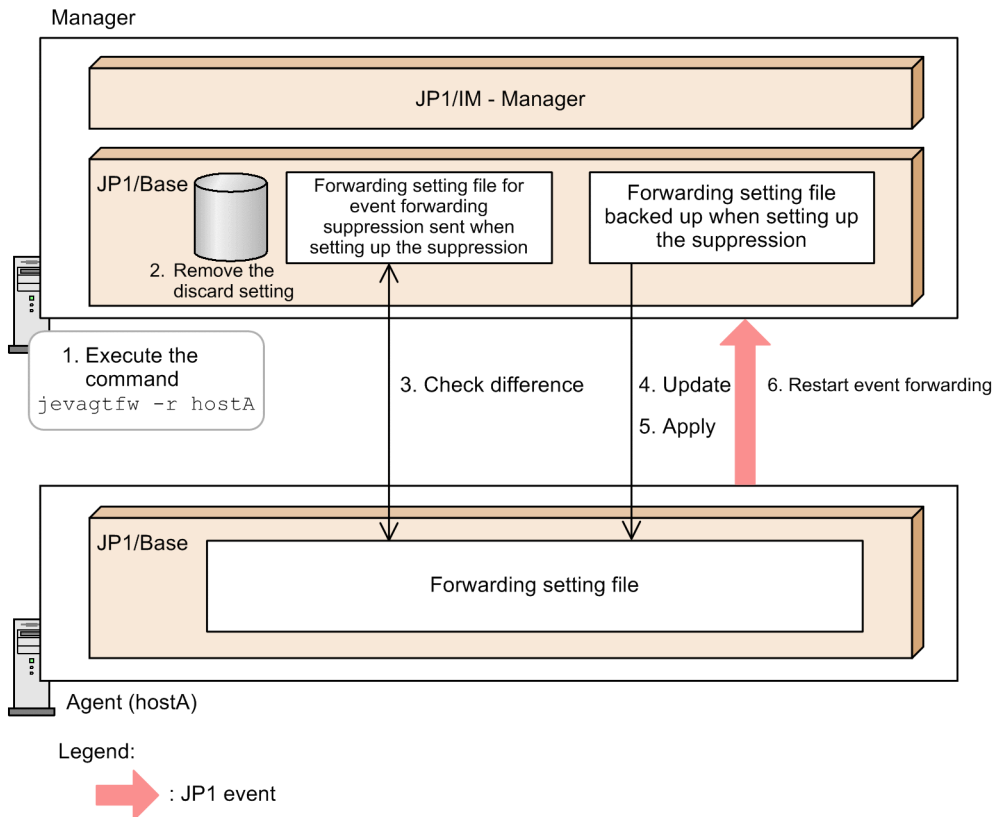
If you want to exclude a JP1 event from discarded events, define the `undisposedids` parameter in the event server settings file (`conf`) to exclude a specific JP1 event from being discarded.

Note that even when a received event is discarded, the sender event server perceives the forwarding as successful.

(3) Stopping event forwarding suppression

You can execute the `jevagtfw` command with the `-r` option specified to stop event forwarding suppression on an agent. The following diagram shows the process flow for stopping event forwarding suppression by using the `jevagtfw` command.

Figure 2–26: Process flow for stopping event forwarding suppression by using the `jevagtfw` command



1. Execute the `jevagtfw` command with the `-r` option specified.
2. Remove the setting to discard received events.
3. Compare the forwarding setting file (`forward`) on the agent and the forwarding setting file for event forwarding suppression (`forward_suppress` file or other forwarding suppression definition file) that was sent when the suppression was set up.
If the result has a difference, cancel the stop process of event forwarding suppression.
4. Send the forwarding setting file (`forward_backup`) backed up when the suppression was set up to the agent, and update the forwarding setting file (`forward`).
5. Reload the updated forwarding setting file (`forward`) and apply it.
6. Event forwarding is restarted according to the forwarding setting file (`forward`).

If the settings in the forwarding setting file (`forward`) are changed while event forwarding is suppressed:

When event forwarding suppression is stopped, the system checks whether the settings in the forwarding setting file (`forward`) have been changed. If the settings in the forwarding setting file (`forward`) have been changed, the following error messages are output, and the stop process of event forwarding suppression is cancelled:

```
KAJP1415-E: The contents of the forward file for suppressing event-forwarding of host-name are different from those set at the time of suppression.
KAJP1432-E: An attempt to stop the suppression of event-forwarding from host-name failed.
```

In this case, either of the following measures is required:

- Forcibly stop event forwarding suppression (execute the `jevagtfw` command with the `-r` and `-f` options specified).

If you can revert settings in the forwarding setting file (`forward`) to the settings before event forwarding suppression without problems, forcibly stop suppression.

- Stop event forwarding suppression only on the manager (execute the `jevagt fw` command with the `-r` and `-m` options specified).

To continue using the settings that have been changed during the event forwarding suppression, stop event forwarding suppression only on the manager. The forwarding setting file (`forward`) on the agent will not revert back to the settings before the event forwarding suppression. In this case, to confirm that no necessary definitions are omitted, compare the settings with those in the forwarding setting file (`forward_backup`) backed up when the suppression was set up and kept in the manager.

(4) Checking event forwarding suppression status

You can execute the `jevagt fw` command with the `-l` option specified to check the suppressed status for each agent whose event forwarding is currently suppressed. The following information can be checked:

- Name of the agent host whose event forwarding is currently suppressed
- Time when the event forwarding suppression was started
- Status of discarding received events (whether the received events are set to be discarded)
- Status of event forwarding suppression (whether event forwarding is set to be suppressed)

(5) Reporting the continuation of event forwarding suppression

You can use the `jevagt fw` command to issue a JP1 event reporting that event forwarding is suppressed. If an event forwarding suppression state lasts for a specified amount of time, the system issues the JP1 event (00003D05) and the following message:

```
KAJP1087-W: Suppression of event-forwarding by the jevagt fw command has continued for total-suppression-time seconds. (server = host-name)
```

The report can be enabled or disabled and the report interval can be specified in the event server settings file (`conf`). For details, see *Event server settings file* in *16. Definition Files*.

Effect of changing the system date and time

If you change the system date and time, reporting of the continuation of event forwarding suppression is affected as follows:

- If you move the system date and time ahead, reporting of the continuation of event forwarding suppression occurs at an interval shorter than the original setting.
- If you move the system date and time back, reporting of the continuation of event forwarding suppression delays.

(6) Files and directories used by event forwarding suppression using the `jevagt fw` command

In the case of the event forwarding suppression using the `jevagt fw` command, you use the manager to manage the forwarding setting file for event forwarding suppression (`forward_suppress`) and suppression information for each agent. This section describes files and directories used during the event forwarding suppression using the `jevagt fw` command.

Location:

The files and directories described above are stored under the directory specified by the event server index file (`index`) as with the event server settings file (`conf`) and the forwarding setting file (`forward`). The following describes the default locations:

In Windows:

```
installation-folder\conf\event\servers\default
```

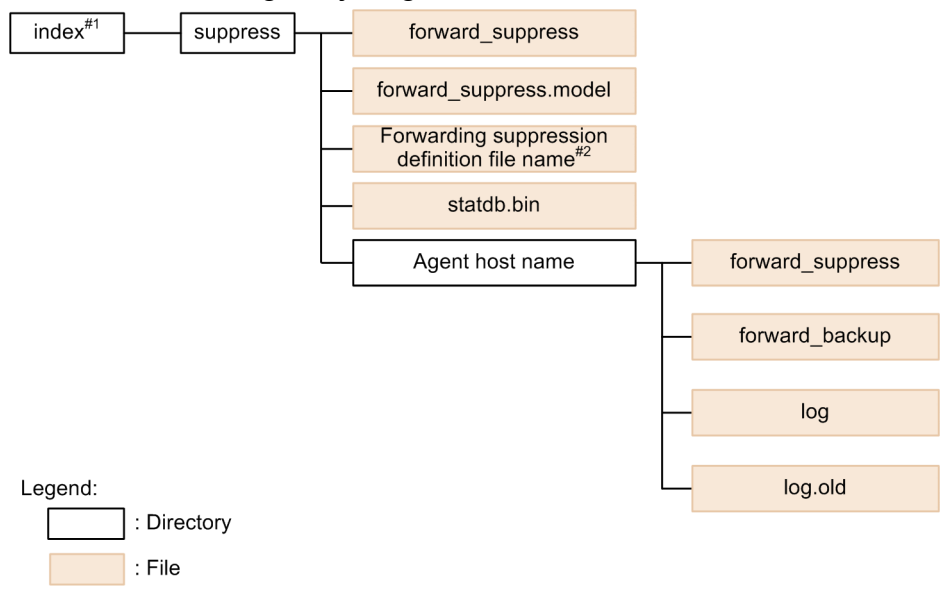
In UNIX:

```
/etc/opt/jp1base/conf/event/servers/default
```

Structure of files and directories:

The following diagram shows the structure of files and directories used during the event forwarding suppression using the `jevagt fw` command.

Figure 2–27: Structure of files and directories used during the event forwarding suppression using the `jevagt fw` command



#1: Directory specified in the event server index file (`index`)
 #2: User-specified file name

Description on files and directories

The following table lists the files and directories used during the event forwarding suppression using the `jevagt fw` command.

Table 2–4: List of files and directories used during the event forwarding suppression using the `jevagt fw` command

File or directory	Description
<code>/suppress/forward_suppress</code>	<p>The forwarding setting file for event forwarding suppression.</p> <p>This file is sent to the agent when event forwarding suppression is set up. The following contents (comments) are set by default:</p> <pre># The manager has suppressed forwarding of events by this agent. # Check with the administrator</pre>

File or directory	Description
	<p>r of the manager before editing this file.</p> <p>The format is the same as the forwarding setting file (<code>forward</code>). For the format of the forwarding setting file (<code>forward</code>), see <i>Forwarding settings file</i> in 16. <i>Definition Files</i>.</p>
<code>/suppress/forward_suppress.model</code>	The model file for the forwarding setting file for event forwarding suppression (<code>forward_suppress</code>).
<code>/suppress/forwarding-suppression-definition-file-name</code>	<p>The forwarding suppression definition file optionally specified by a user.</p> <p>To specify a separate forwarding suppression setting for each agent, prepare a forwarding suppression definition file with a desired file name, and specify the file name using the <code>-s</code> option of the <code>jevagtfw</code> command.</p>
<code>/suppress/statdb.bin</code>	A binary file that controls the suppression status.
<code>/suppress/agent-host-name</code>	<p>A directory in which suppression status for each agent host is stored.</p> <p>This directory is created when event forwarding suppression is succeeded by using the <code>jevagtfw</code> command. This directory remains unless the user deleted it.</p>
<code>/suppress/agent-host-name/forward_suppress</code>	<p>This file contains the settings in the forwarding setting file for event forwarding suppression that was sent to the agent when the event forwarding suppression was set up.</p> <p>When you attempt to stop the event forwarding suppression, the system compares the contents of this file with the contents in the forwarding setting file on the agent.</p>
<code>/suppress/agent-host-name/forward_backup</code>	<p>This file contains backup information of the forwarding setting file obtained from the agent when the event forwarding suppression was set up.</p> <p>When you attempt to stop the event forwarding suppression, the contents of this file is set to the forwarding setting file on the agent again[#].</p>
<code>/suppress/agent-host-name/log</code>	The log file in which suppression of event forwarding and stopping of the suppression are recorded. If the <code>log</code> file exceeds 64 KB, the file name is changed to <code>log.old</code> , and a new <code>log</code> file is created.
<code>/suppress/agent-host-name/log.old</code>	

[#]: If event forwarding suppression is set up, when the forwarding setting file on the agent is backed up, information beyond the 1,024th byte per line in the definition of the file is deleted as invalid. When the event forwarding suppression is stopped, the forwarding setting of which information beyond the 1,024th byte per line has been deleted is set in place. Therefore, definition information which was invalid because it exceeded 1,023 bytes per line might become valid because it is now within 1,023 bytes.

Use of machine-dependent characters

Do not use machine-dependent characters in the following files, including the comment lines:

- `suppress/forward_suppress`
- `suppress/any-file-name`

These files are sent to the agent when event forwarding suppression is set up. Use of machine-dependent characters might cause garbling or missing of characters. If garbling or missing of characters occurs, an attempt to stop event forwarding suppression might fail with an error (KAJP1415-E).

```
KAJP1415-E: The contents of the forward file for suppressing event-forwarding of host-name are different from those set at the time of suppression.
```

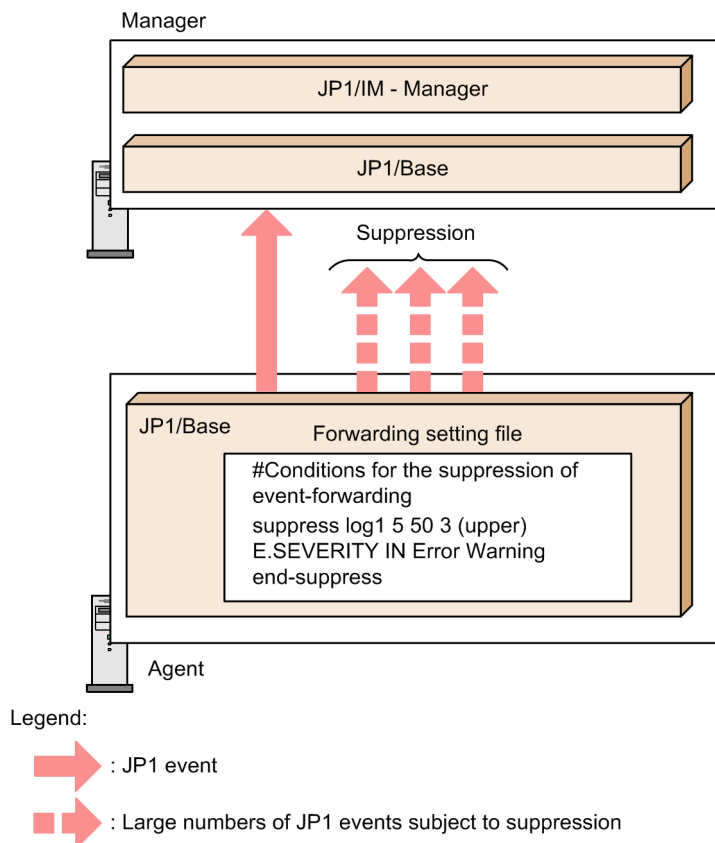
2.5.4 Setting a threshold to automatically suppress forwarding of large numbers of events

You can set a threshold to automatically suppress forwarding of large numbers of events. If a condition below the threshold persists, the system can also determine that the large numbers of events have converged and automatically stop the event forwarding suppression. The conditions that correspond to a threshold to detect large numbers of events is called *conditions for the suppression of event-forwarding*.

The conditions for the suppression of event-forwarding are specified in the forwarding-suppression setting block (from `suppress` to `end-suppress`) in the forwarding setting file (`forward`) on a suppressed agent. For example, you can specify so that event forwarding is to be suppressed if the following condition is satisfied three times in succession: 50 or more JP1 events occur within 5 seconds.

By specifying an expected large numbers of events as the conditions for the suppression of event-forwarding, you can prevent large numbers of events from being forwarded from an agent.

Figure 2–28: Overview of the threshold-based suppression of event-forwarding



Note that use of this functionality requires that the JP1/Base version of a suppressed agent host is 10-50 or later.

(1) JP1 events that are subject to suppression (threshold-based suppression of event-forwarding)

In threshold-based suppression of event-forwarding, JP1 events that are subject to the suppression are the ones forwarded according to the settings in the forwarding setting file (`forward`). Among the JP1 events filtered by the forward setting (`to`) in the forwarding setting file (`forward`), the system checks the number of JP1 events that match the destination of conditions for the suppression of event-forwarding and the event filter. If the number of matching JP1 events exceeds the threshold, event forwarding based on the forwarding setting file (`forward`) is suppressed.

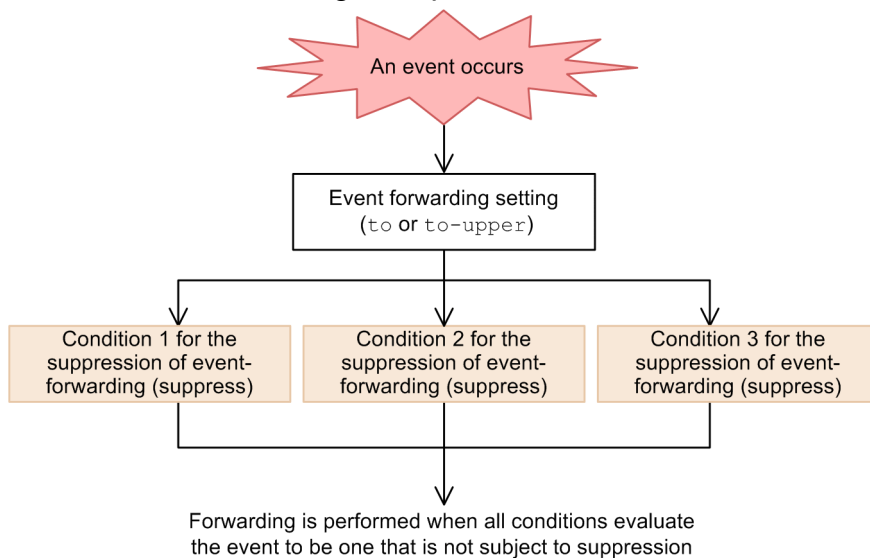
Note that address-specified events and automatic forwarding events are not subject to suppression. For details on address-specified forwarding events and automatic forwarding events, see [2.5.3\(1\) JP1 events that are subject to suppression \(event forwarding suppression by using the `jevagtfw` command\)](#).

(2) Event forwarding when multiple conditions for the suppression of event-forwarding are specified

You can specify two or more conditions for the suppression of event-forwarding in the forwarding setting file (`forward`). If you specify two or more conditions for the suppression of event-forwarding, the number of JP1 events is checked for each suppression condition. JP1 events that are judged not to be suppressed for all the suppression conditions are forwarded.

The following diagram shows the JP1 event forwarding when two or more conditions for the suppression of event-forwarding are specified.

Figure 2–29: JP1 event forwarding when two or more conditions for the suppression of event-forwarding are specified



(3) Detection and convergence of large numbers of events

The conditions for the suppression of event-forwarding have following setting items that represent JP1 event occurrence status to define large numbers of events: unit time, threshold, and check count. This section describes detection and convergence of large numbers of events based on the unit time, threshold, and check count.

The following table describes the setting items.

Table 2–5: The setting items that represent JP1 event occurrence status to define large numbers of events

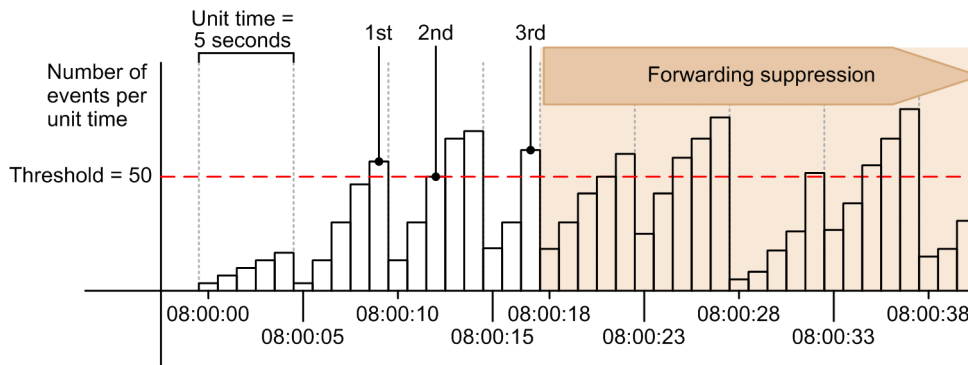
Setting item	Description
Unit time	Time duration in which the threshold is evaluated. A unit time starts when a JP1 event that matches a condition for the suppression of event-forwarding is detected or when the event forwarding suppression is stopped.
Threshold	The number of JP1 events per unit time.
Check count	The number of unit times used to determine occurrence or convergence of large numbers of events. You can set a different number for starting and stopping the event forwarding suppression.

Detecting large numbers of events

If the number of JP1 events for a unit time exceeds the threshold successively for the number of times specified in the check count, the system determines that large numbers of events are detected, and suppress the event forwarding. For example, suppose that you set 5 seconds for the unit time, 50 for the threshold, and 3 for check count. Event forwarding suppression starts when a condition in which 50 or more JP1 events occur within 5 seconds appears three times consecutively.

The following diagram shows the timing at when it is determined that an occurrence of large numbers of events is detected so that the event forwarding suppression is started, in relationship to the JP1 event occurrence status.

Figure 2–30: Timing when event forwarding is suppressed



As shown in this diagram, if the check count is set to 3, the forwarding suppression starts at the time when the number of events exceeds the threshold for the first time during the third unit time.

Convergence of large numbers of events

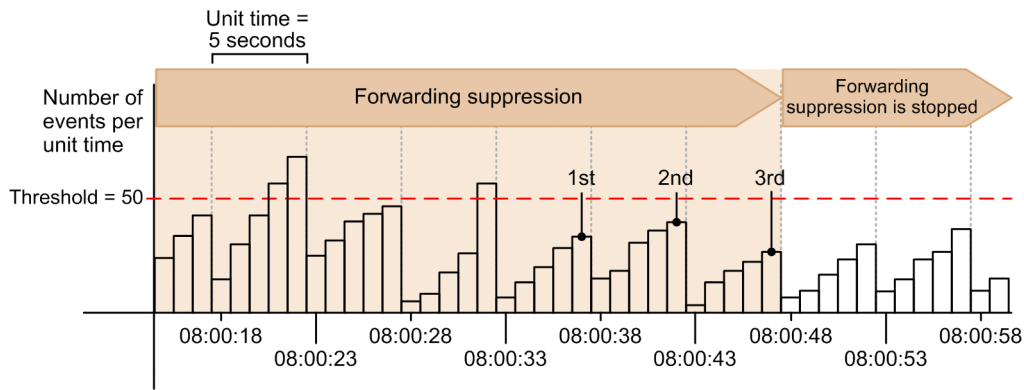
While the event forwarding is suppressed, the system determines that large numbers of events have reached convergence, and then stops event forwarding suppression if the following condition exists:

- In the conditions for the suppression of event-forwarding, the number of JP1 events per unit time consecutively falls below the threshold the number of times specified as the check count.

For example, suppose that you set 5 seconds for the unit time, 50 for the threshold, and 3 for check count. Event forwarding suppression is stopped if the following condition is satisfied three times in succession: 49 or fewer JP1 events occur within 5 seconds.

The following diagram shows the timing at when it is determined that the large numbers of events has reached convergence so that the event forwarding suppression is stopped, in relationship to the JP1 event occurrence status.

Figure 2–31: Timing when event forwarding suppression is stopped

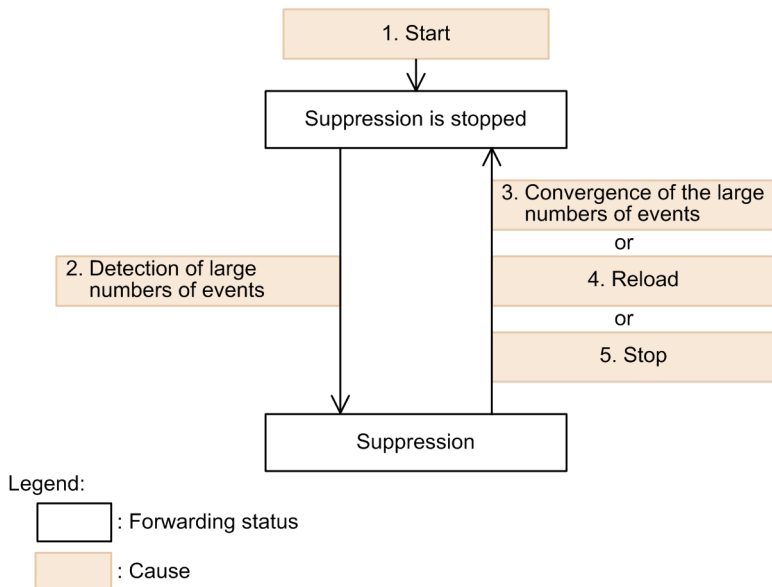


(4) Transitions of forwarding status

The threshold-based suppression of event-forwarding has a forwarding status (either suppression stopped or suppressed) for each condition for the suppression of event-forwarding. The forwarding status transitions due to some causes.

The following diagram shows the relationship between the forwarding status transitions and their causes.

Figure 2–32: Forwarding status transitions and the causes



Forwarding status

- **Suppression stopped**
This status does not suppress event forwarding.
- **Suppressed**
This status suppresses event forwarding.

Causes

1. **Startup**
Start up an event service (i.e. execute the `jevstart` command).
2. **Detection of large numbers of events**
In the conditions for the suppression of event-forwarding, the number of JP1 events per unit time consecutively exceeds the threshold the number of times specified as the check count.

3. Convergence of large numbers of events

In the conditions for the suppression of event-forwarding, the number of JP1 events per unit time consecutively falls below the threshold the number of times specified as the check count.

4. Reloading

Reload the forwarding setting file (`forward`) (execute the `jevreload` command).

5. Stop

Stop the event service (execute the `jevstop` command).

When the forwarding status transitions, a message and a JP1 event is output. The following table lists the messages and JP1 events output when the forwarding status transitions.

Table 2–6: Messages and JP1 events output when the forwarding status transitions

No.	Cause	Forwarding status		Message	JP1 event
		Before	After		
1	Startup	--	Suppression stopped	--	--
2	Detection of large numbers of events	Suppression stopped	Suppressed	KAJP1083-W: <i>host-name</i> will start the threshold-based suppression of event-forwarding. (suppression ID = <i>identifier</i>)	00003D0B
3	Convergence of large numbers of events	Suppressed	Suppression stopped	KAJP1084-I: <i>host-name</i> stopped the threshold-based suppression of event-forwarding. (suppression ID = <i>identifier</i>)	00003D0C
4	Reloading			KAJP1085-I: <i>host-name</i> stopped all threshold-based suppressions of event-forwarding.	00003D0D
5	Stop			--	--

Legend:

--: Not applicable.

(5) Checking the forwarding suppression status

You can check the forwarding suppression status of JP1 events for each condition for the suppression of event-forwarding. To check the forwarding suppression status, use the `jevfwstat` command. For details, see [jevfwstat](#) in *15. Commands*.

(6) Reporting the continuation of event forwarding suppression

You can periodically report that the event forwarding is suppressed by threshold-based suppression of event-forwarding to the manager. If an event forwarding suppression state lasts for a specified amount of time, the system issues the JP1 event (00003D0E) and the following message:

```
KAJP1086-W: Suppression of event-forwarding by host-name has continued for t
otal-suppression-time seconds. (suppression ID = identifier)
```

The report can be enabled or disabled and the report interval can be specified in the event server settings file (`conf`). For details, see *Event server settings file* in *16. Definition Files*.

(7) Notes on threshold-based suppression of event-forwarding

If you change the system date and time on the machine while the event server is running on the agent with threshold-based suppression of event-forwarding is set up, the forwarding status might incorrectly change. Alternatively, the continuation of event forwarding suppression might be erroneously reported.

The following describes the effect of changing the system date and time:

Effect when you move the system date and time ahead:

- Large numbers of events might be mistakenly evaluated as converged even when they are not, and event forwarding suppression might be stopped.
- The continuation of event forwarding suppression might be reported even when the suppression status does not last for a specified time.

Effect when you move the system date and time back:

- Large numbers of events might be mistakenly evaluated as occurred even when they are not, and event forwarding might be suppressed.
- The continuation of event forwarding suppression might not be reported even when the suppression status lasts for a specified time.

2.6 Collecting and distributing definitions (JP1/IM only)

A system configured with JP1/Base and JP1/IM can manage definition information. Such a system can also check information about service activity, and collect and distribute definitions for the event service.

2.6.1 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 *16. Definition Files*.

For details on managing definitions by using IM configuration management, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

2.6.2 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 *JP1/Integrated Management 3 - 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 *15. Commands*.

2.6.3 Managing the system's hierarchical configuration by using commands

There are two ways of managing the hierarchical configuration of a system that includes JP1/Base and JP1/IM. One way is by using the IM configuration management functionality, and the other way is by using the configuration management functionality provided by JP1/Base (commands related to configuration definition). This subsection explains how to manage a system's hierarchical configuration by using the configuration management functionality provided by JP1/Base.

The configuration management functionality provided by JP1/Base uses commands related to configuration definition in order to set, on managers and agents, the configuration definition information that defines the system's hierarchical configuration.

The commands related to configuration definition are as follows:

- `jbsrt_distrib` (distributes configuration definition information to lower-level hosts)
- `jbsrt_sync` (collects and updates configuration definition information from lower-level hosts)
- `jbsrt_del` (deletes configuration definition information)
- `jbsrt_get` (displays configuration definition information)

These commands are used to perform operations such as distributing configuration definition information from a manager to agents and updating a manager's configuration definition information with the configuration definition information collected from agents.

For details about the commands, see *jbsrt_distrib*, *jbsrt_sync*, *jbsrt_del*, and *jbsrt_get* in *15. Commands*.

To set configuration definition information, on the manager, define the system's hierarchical configuration in the JP1/IM configuration definition file (`jbs_route.conf`), and then distribute the definition information to lower-level hosts by executing the `jbsrt_distrib` command. For details about how to set configuration definition information, see the description about how to set the system's hierarchical configuration without using the IM configuration management functionality in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(1) Distributing the configuration definition information

If hosts to be managed are added or managed hosts are deleted, you need to update the agent configuration definition information (distribute new configuration definition information by executing the `jbsrt_distrib` command). There are two ways to distribute configuration definition information, as follows.

Batch distribution method

Configuration definition information is deleted from or distributed to all hosts included the configuration definition.

Differential distribution method

Configuration definition information is deleted from or distributed to only those hosts to which changes were made in the configuration definition. This method was added in JP1/Base version 11-10.

This section explains the differential distribution method.

(2) Prerequisites for using the differential distribution method

To use the differential distribution method, the following conditions must be met for manager hosts and submanager hosts:

- The version of JP1/IM - Manager is 11-00 or later.
- The version of JP1/Base is 11-10 or later.

(3) Setting the distribution method

For `JBSRT_DISTRIB_VERSION` in the common definition information, specify which distribution method is to be used when the `jbsrt_distrib` command is executed.

If 1 is set for `JBSRT_DISTRIB_VERSION`

Differential distribution method

If 0 is set for `JBSRT_DISTRIB_VERSION`

Batch distribution method

You can also specify the distribution method as an option of the `jbsrt_distrib` command. The distribution method specified as a command option will be used regardless of the value set for `JBSRT_DISTRIB_VERSION` in the common definition information.

If the `-D` option is specified for the `jbsrt_distrib` command

Differential distribution method

If the `-L` option is specified for the `jbsrt_distrib` command

Batch distribution method

If neither the `-D` option nor the `-L` option is specified, the distribution method set for `JBSRT_DISTRIB_VERSION` in the common definition information will be used.

Note that, when JP1/Base is newly installed, `JBSRT_DISTRIB_VERSION` is set to 1 (differential distribution method). If you installed JP1/Base by overwriting a JP1/Base version earlier than 11-10, `JBSRT_DISTRIB_VERSION` is not defined (in which case, the batch distribution method will be used).

For details about how to specify the distribution method by using `JBSRT_DISTRIB_VERSION` in the common definition information, see [12.2.1 Specifying the method for distributing configuration definition information](#).

For details about the `jbsrt_distrib` command, see [jbsrt_distrib](#) in [15. Commands](#).

(4) Notes about using the differential distribution method

If configuration definition information is deleted from an individual agent or submanager as in the cases described below, the hosts from which the information was deleted can no longer be detected as differential information by the manager. For this reason, use the batch distribution method to distribute configuration definition information.

- The configuration definition information was deleted by using the `jbsrt_del` command, not the `jbsrt_distrib` command.
- The machine was replaced.

(5) Reviewing the communication timeout value

During operation under a system hierarchical configuration with three or more levels, the distribution or synchronization of configuration definition by submanagers or hosts below submanagers may take too much time and fail to return a response to the integrated manager within a certain period of time. Hence, the application or synchronization of system hierarchical configuration by using a configuration management command (`jbsrt_distrib` or `jbsrt_sync`) or IM configuration management may result in timeout.

Such timeout occurs mainly in cases where there are many agents under a submanager or the network circuit speed between a submanager and an agent is low.

If timeout occurs in spite that there are no abnormalities with lower-level hosts, adjust the integrated manager's communication timeout value to be the larger one because the timeout may be caused due to either of the above mentioned cases. For details about how to set the communication timeout value, see [Common definition settings file \(configuration management functionality\)](#) in [16. Definition Files](#).

Actual elapsed time spent for the distribution or synchronization process on a manager host in the system hierarchical configuration can be confirmed in the message KAVB3185-I. Use it as a reference for adjusting the timeout value.

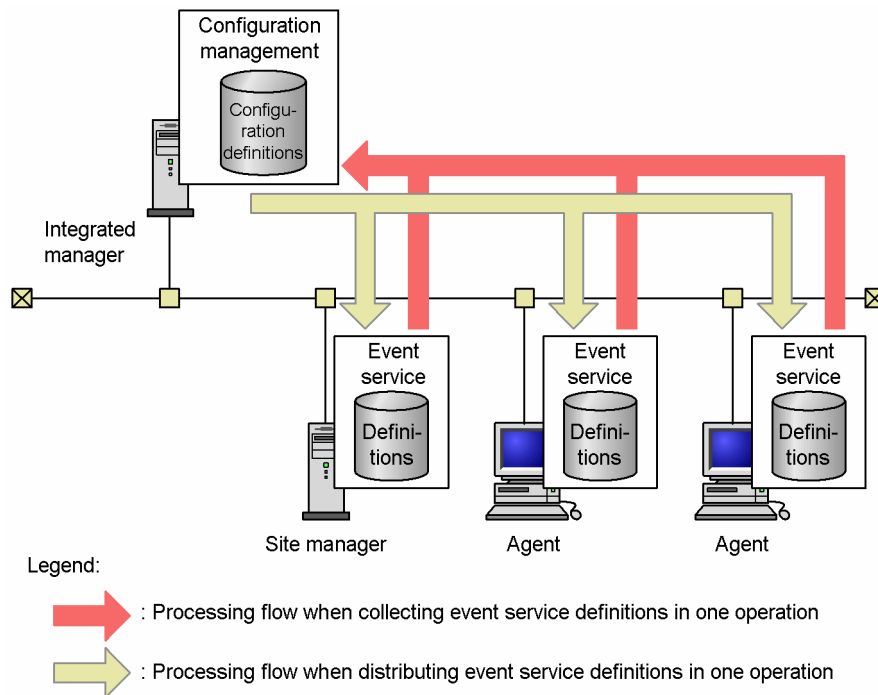
2.6.4 Collecting and distributing definitions for the event service by using commands

This section describes how to collect and distribute event service definitions by using commands. 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 2–33: Processing flow when collecting and distributing event service definitions



(1) Requirements for collecting and distributing event service 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 or later)
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 *JP1/Integrated Management 3 - Manager Configuration Guide*.

Important

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:

Table 2–7: Collectable and distributable definitions (in Windows)

Definition files	File names
Forwarding settings file	<i>installation-folder</i> \conf\event\servers\default\forward
	<i>shared-folder</i> \jplbase\event\forward
Action definition file for log file trapping	<i>installation-folder</i> \conf\any-file
Action definition file for event log trapping	<i>installation-folder</i> \conf\event\ntevent.conf
Log-file trap startup definition file [#]	<i>installation-folder</i> \conf\event\jevlog_start.conf

[#]: To distribute and collect log-file trap startup definition files, JP1/Base version 10-00 or later must be installed on the source and destination hosts.

Table 2–8: Collectable and distributable definitions (in UNIX)

Definition files	File names
Forwarding settings file	/etc/opt/jplbase/conf/event/servers/default/forward
	<i>shared-directory</i> /event/forward
Action definition file for log file trapping	/etc/opt/jplbase/conf/ <i>any-file</i>
Log-file trap startup definition file [#]	/etc/opt/jplbase/conf/event/jevlog_start.conf

[#]: To distribute and collect log-file trap startup definition files, JP1/Base version 10-00 or later must be installed on the source and destination hosts.

2.6.5 Collecting definitions of JP1 programs

By using the central scope feature of JP1/IM - Manager, you can view the definitions managed by JP1 programs, such as work tasks (jobnets) defined in JP1/AJS and information monitored by JP1/SSO, 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/SSO
- Performance data being monitored by JP1/PFM

For details, see the manual *JP1/Integrated Management 3 - Manager Administration Guide*.

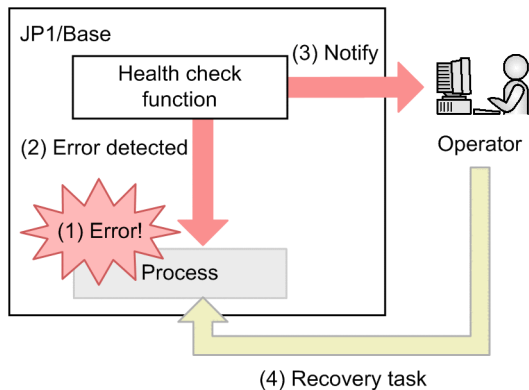
2.7 Detecting a process hangup and abnormal termination

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.



2.7.1 Flow of using the health check function to troubleshoot problems

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

Figure 2–34: Troubleshooting by using the health check function



Legend:

-  : Health check processing when an error occurs in a process
-  : Operator's action

- (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 *18. 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 on how to do so, see *4.2.1 Enabling the health check function*.

The process management service is activated and process monitoring begins.

2.7.2 Problems that can be detected by the health check function

The health check function can detect the following problems:

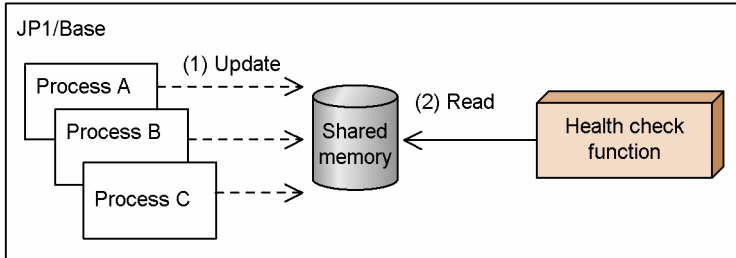
- **Process hangups**
If a process hangs, the health check function detects the error and notifies the operator. Hangups are caused by an infinite loop or deadlock, and mean that the process can no longer accept processing requests.
- **Abnormal termination of a process**
If a process terminates abnormally 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.

2.7.3 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 2–35: 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.

2.7.4 Processes monitored by the health check function

(1) List of processes monitored by the health check function

The table below lists the processes monitored by the health check function. Note that, in Windows, the process names in the table are displayed in the Task Manager window, or in UNIX, the process names are displayed by using the `ps` command.

Table 2–9: Processes monitored by the health check function

No.	Function	Process name	
		Windows	UNIX
1	Process management	jbs_spmd.exe	jbs_spmd
2	Authentication server	jbsessionmgr.exe	jbsessionmgr
3	Configuration management	jbsroute.exe	jbsroute
4	Command execution	jcocmdapi.exe jcocmdcom.exe jcocmdexe.exe jcocmd.exe	jcocmdapi jcocmdcom jcocmdexe jcocmd
5	Plugin service	jbspluginind.exe jbsplugincom.exe	jbsplugin jbsplugincom

No.	Function	Process name	
		Windows	UNIX
6	Event service	jevservice.exe	jevservice
7	Log file trapping	jevtraplog.exe	jevlogd jelparentim jelchildim
8	Event log trapping (Windows only)	jevtrapevt.exe	--
9	Health check	jbshcd.exe jbshchostd.exe	jbshcd jbshchostd
10	Service management control	jbssrvmgr.exe	jbssrvmgr
11	Local action	jbslact.exe	jbslact
12	Inter-process communication	jbscomd.exe jbscomd_ses.exe jbscomd_rcv.exe jbscomd_snd.exe jbscomd_api.exe	jbscomd jbscomd_ses jbscomd_rcv jbscomd_snd jbscomd_api

Legend:

--: Not applicable.

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.

(2) List of process names and function names in messages output by the health check function

The following table lists the process names and function names in messages output by the health check function.

Table 2–10: Process names and function names in messages output by the health check function

No.	Function	Process name	Function name
1	Process management	jbs_spmd	jbsspmd
2	Authentication server	jbssessionmgr	jbssessionmgr
3	Configuration management	jbstroute	jbstroute
4	Command execution	JCOCMDAPI JCOCMDCOM JCOCMDEXE JCOCMDROUTER	jcocmd
5	Plugin service	jbspluginind jbsplugincom	jbsplugin
6	Event service	In Windows: jevservice In UNIX: jevservice	jevservice

No.	Function	Process name	Function name
7	Log file trapping	In Windows: jevtraplog In UNIX: jelchildim jelparentim jevlogd	jevtraplog
8	Event log trapping (Windows only)	jevtrapevt	jevtrapevt
9	Health check	jbshcd jbshchostd	jbshcd jbshchostd
10	Service management control	jbssrvmgr	jbssrvmgr
11	Local action	jbslcact	jbslcact
12	Inter-process communication	jbscomd jbscomd_ses jbscomd_rcv jbscomd_snd jbscomd_api	JBSCOM

2.7.5 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 2,500 remote hosts can be monitored from one host.

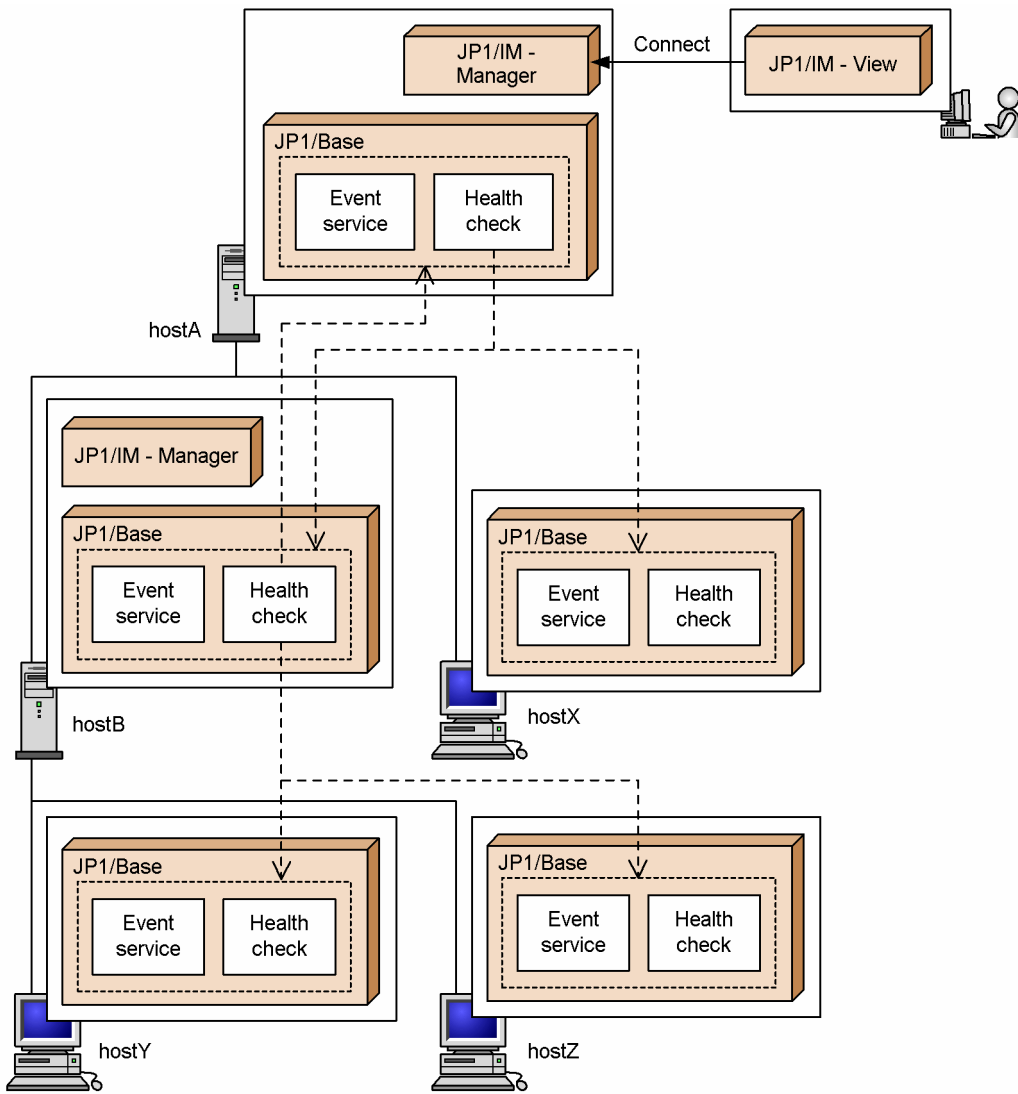
The following describes how to monitor a remote host in a system that uses JP1/IM - Manager, and how the system operates when monitoring a remote host.

(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 2–36: Example of remote host monitoring in a system that uses JP1/IM - Manager



Legend:

-----> : Remote host monitoring

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

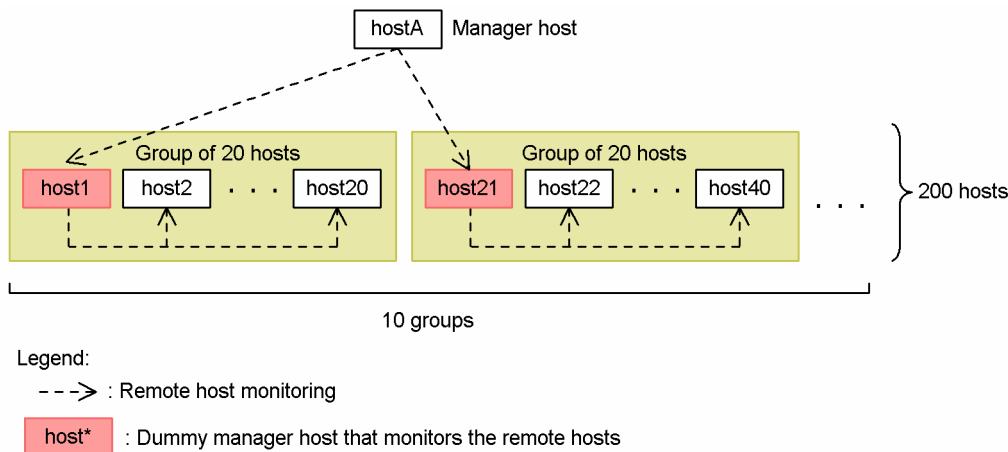
If the health check function is enabled at JP1/IM - Manager on hostA, the health check function at JP1/IM - Manager detects the error in the event service on the local host and a message appears in JP1/IM - View.

(2) 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, for one host to check 200 hosts might take about 600 seconds from start to finish. You can reduce the monitoring time by splitting the target hosts into groups, and setting a dummy manager host for each group.

Figure 2–37: 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.

(3) Checking the time spent on each monitoring operation

To check the time spent on each monitoring (polling) operation, check the polling completion message (KAVA7239-I). Each time monitoring finishes, the following polling completion message (KAVA7239-I) is output:

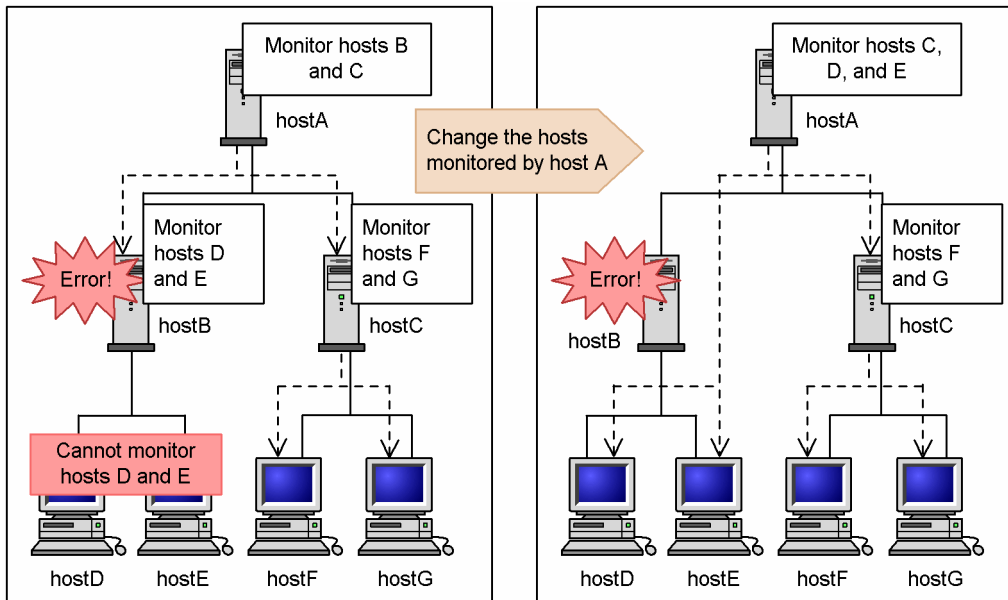
```
KAVA7239-I Monitoring by the health check function is complete. (host name = manager-host-name, monitoring time = monitoring-time-in-seconds, monitoring interval = monitoring-interval-in-seconds)
```

The polling completion message (KAVA7239-I) is output if YES is specified for the POLLENDMSG parameter in the health check definition file. When JP1/Base is installed, the default setting is that the polling completion message is not output. For details about the health check definition file, see *Health check definition file in 16. Definition Files*.

(4) 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 2–38: Example of error handling in a hierarchical configuration



Legend:

-----> : Remote host monitoring

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.

(5) Operation when a monitoring error occurs due to a temporary failure

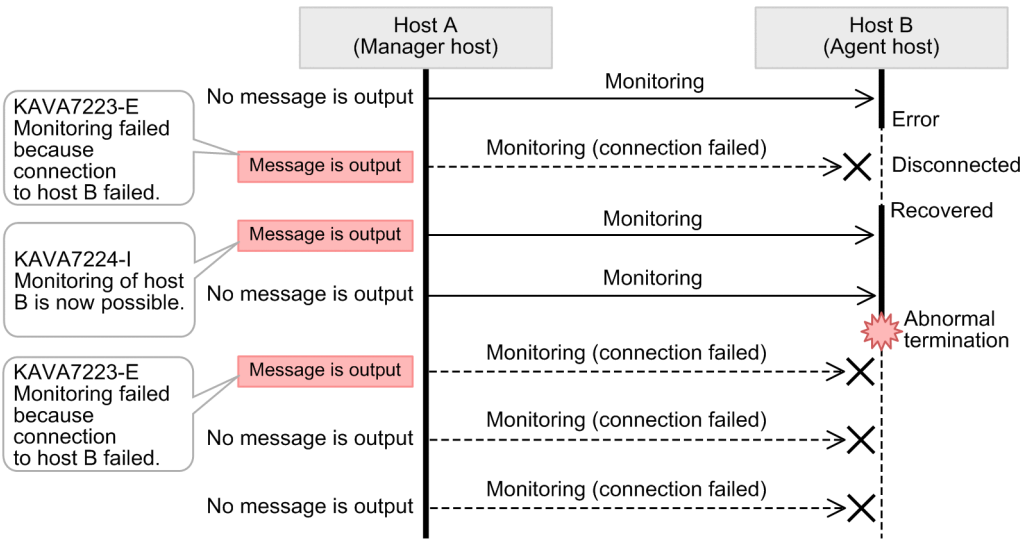
If remote host monitoring of the health check function fails to monitor a monitored host due to, for example, a system overload or network problem, the function reports an error to the monitoring host (manager).

However, if the cause of the error is temporary, the error might be corrected spontaneously after a while. Therefore, you might not want all errors to be reported to the monitoring host. In such a case, you can set a threshold (*monitoring threshold*) to distinguish real errors from temporary errors. Specify how many times monitoring can fail in succession as the monitoring threshold. When the specified threshold is reached, the function judges that an error has occurred on the monitored host and reports an error to the monitoring host.

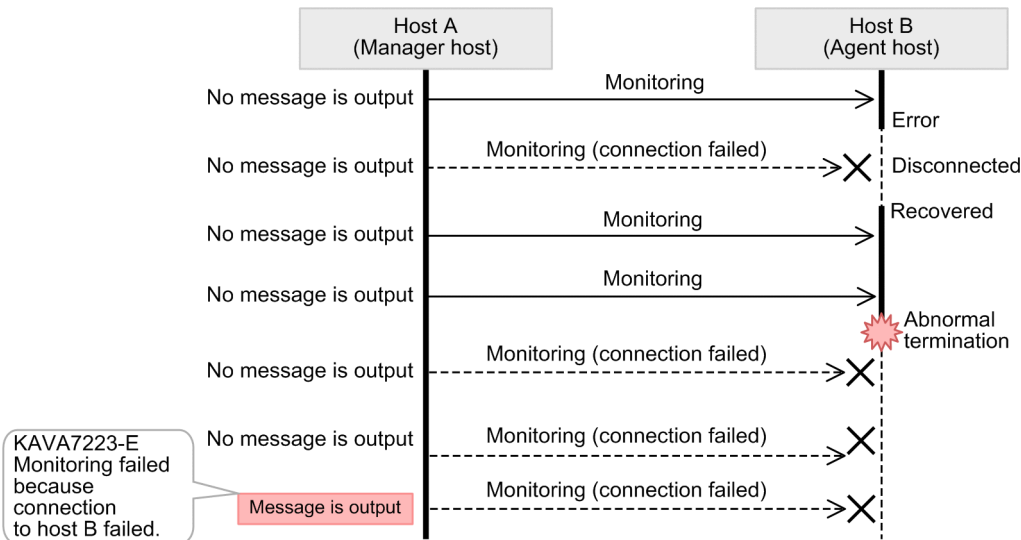
The following figure compares the behavior in cases where no monitoring threshold is set and where the monitoring threshold is set to 3.

Figure 2–39: Behavior of the health check function in cases where a monitoring threshold is set and not set

Case 1: No monitoring threshold is set



Case 2: Monitoring threshold is set to 3



Legend:
 — : Operating - - - - - : Not operating

As shown in the figure above, if no monitoring threshold is set, an error message is output at the first failure in monitoring. On the other hand, if the monitoring threshold is set to 3, an error message is output at the third successive failure in monitoring. Note that setting the monitoring threshold to 1 is equivalent to setting no monitoring threshold.

You can specify the monitoring threshold in the health check definition file (`jbshc.conf`). Note that setting the monitoring threshold causes a delay in detection of an error on the monitored host. The delay (in seconds) can be approximated as follows: $monitoring-interval \times (monitoring-threshold - 1)$. In normal operation, do not change the monitoring threshold from the initial value of 1. If you change the monitoring threshold from the initial value, determine the new value through careful consideration of the conditions in which failures and errors occur.

Determine whether the cause of failure in monitoring is temporary from messages that are output. The following shows the guidelines for determination.

1. If monitoring fails, message KAVA7223-E or KAVA7229-W is output.
2. If recovery of connection is confirmed by a subsequent connectivity check, message KAVA7224-I is output.

If messages are output in the above order, this indicates that a temporary failure occurred and was then corrected in a short time. In this case, monitoring failed because, for example, connection to the monitored host failed, a session with the monitored host was closed, or connection (or communication) timed out. For the cause of failure, see the detailed information that is output in message KAVA7223-E or KAVA7229-W. Note that detailed information is output to messages if the `ERROR_DETAIL` parameter is enabled (ON) in the health check definition file (`jbshc.conf`). If the cause of failure in monitoring is a connection or communication timeout, you also have to review the timeout value.

(6) 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 *16. Definition Files*.

(7) Reviewing the communication timeout value

If the system load on a monitored host is high, a delay in response from the monitored host to the monitoring host (manager) might cause a failure in monitoring. In such a case, the possibility of failure due to a delay in response can be reduced by adjusting the communication timeout value on the manager side.

You can specify the communication timeout value in the health check definition file (`jbshc.conf`). When you specify the communication timeout value, do not set a time longer than the monitoring interval. If the communication timeout value is longer than the monitoring interval, monitoring might not finish within a monitoring interval. In normal operation, do not change the communication timeout value from the initial value of 60 (seconds). If a processing delay occurs in a condition such as shown below, review the communication timeout value according to the operational condition:

- The system load increases temporarily or periodically.
- The system is operating at nearly full performance.

Determine whether a communication timeout occurred from the detailed information in message KAVA7223-E or KAVA7229-W that is output when monitoring fails. If occurrence of a connection or communication timeout is indicated as the cause, this means that a communication timeout occurred. Detailed information can be output to messages if the `ERROR_DETAIL` parameter is enabled (ON) in the health check definition file (`jbshc.conf`).

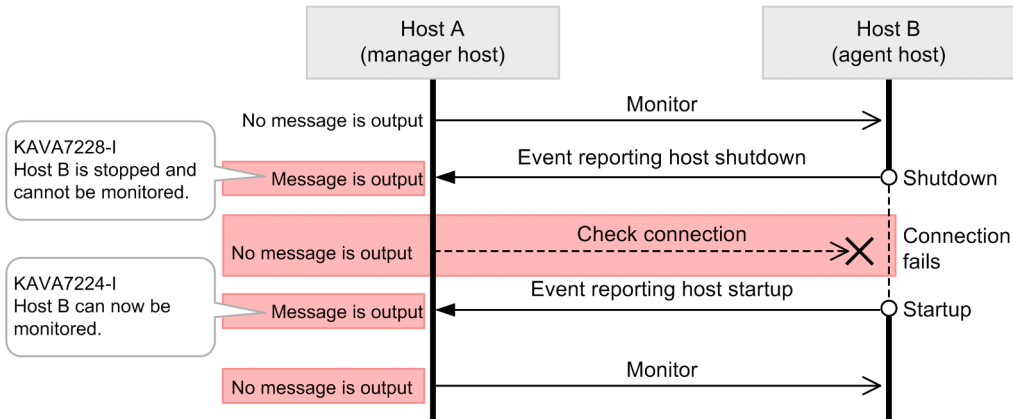
(8) Operation when a monitored host stops

If version 10-00 or later of JP1/Base is installed on both the manager host and monitored host, you can choose whether to monitor when the monitored host starts and stops. If you choose to monitor this activity, you can prevent an error from being reported if a host shuts down normally when scheduled to do so.

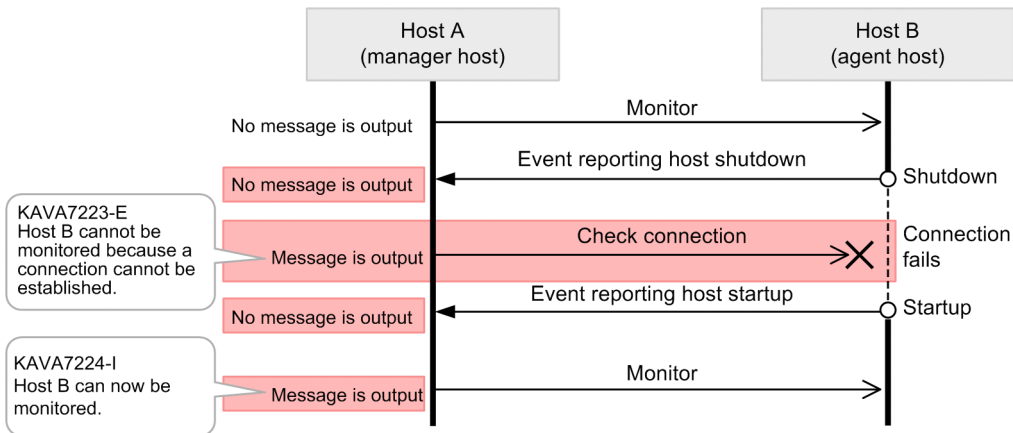
The following figure shows how the system behaves when JP1/Base monitors the startup and shutdown of monitored hosts, and when it does not.

Figure 2–40: Operation when monitoring and not monitoring monitored host startup and shutdown

● When monitoring startup and shutdown of monitored host



● When not monitoring startup and shutdown of monitored host



Legend:

- : Running - - - - - : Stopped
- : Behavior that differs when monitoring and not monitoring monitored host startup and shutdown

JP1/Base issues JP1 events when it starts and when it stops. If JP1/Base is configured to monitor when monitored hosts start and stop, and receives a JP1 event reporting that a monitored host has stopped, it outputs the message KAVA7228-I. Although JP1/Base will continue to check the connection to the monitored host at the specified monitoring interval, it will not declare an error if a connection cannot be established.

Note that, while JP1/Base on the manager host is stopped, JP1/Base cannot receive a JP1 event reporting that a monitored host has stopped. Therefore, after JP1/Base on the manager host has started, if monitoring fails for a monitored host that has not been monitored before, JP1/Base issues the message KAVA7229-W.

KAVA7229-W Monitoring cannot be performed because a connection cannot be established with Host B, which is not receiving stop notifications.

If monitoring fails for a monitored host that has been monitored before or one that sent a JP1 event reporting that a monitored host had started, JP1/Base issues the message KAVA7223-E.

KAVA7223-E Monitoring cannot be performed because a connection with Host B cannot be established.

If a monitored host that output the message KAVA7229-W or KAVA7223-E is in a state such that it is available to be monitored after the connection is confirmed, or if a JP1 event is received from the monitored host reporting that the monitored host has started, JP1/Base issues the message KAVA7224-I and restarts monitoring the host.

 **Note**

If you want to monitor the starting and stopping of monitored hosts, you must configure the monitored hosts to send JP1 events reporting that the host has started and stopped to the manager host.

In contrast, if JP1/Base is configured to not monitor the starting and stopping of monitored hosts, it does not output a message when it receives a JP1 event reporting that an agent host has stopped. In this scenario, JP1/Base continues to monitor the host in the normal way, even after it receives a JP1 event reporting that the host has stopped. If JP1/Base cannot connect with that host, it issues the message KAVA7223-E.

The message output when the health check function (for remote host monitoring) starts indicates whether JP1/Base is configured to monitor the starting and stopping of monitored hosts. The following table shows which setting is indicated by each message ID.

Setting	Message ID
Monitor starting and stopping of monitored hosts	KAVA7231-I
Do not monitor starting and stopping of monitored hosts	KAVA7230-I

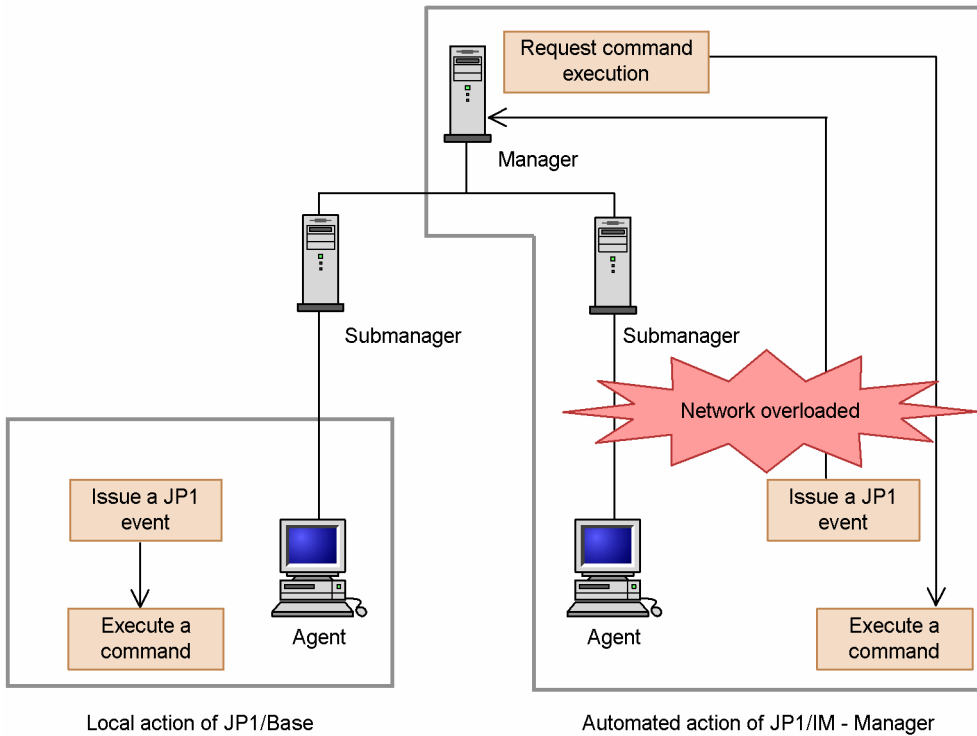
You can specify whether JP1/Base monitors the starting and stopping of monitored hosts by the setting of the `STOP_CHECK` parameter in the health check definition file (`jbshc.conf`).

2.8 Command execution triggered by a JP1 event

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 2–41: 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.

2.8.1 Conditions required for executing local actions

- JP1/Base version 09-00 or later is installed on the agent host.
- 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 all instances of JP1/IM - Manager and JP1/Base installed on the manager and submanagers are version 09-00 or later, and you are using IM configuration management, you can use the IM configuration management functionality to define a local action execution definition file on the manager host and batch distribute it to all the agent hosts. For details

on managing definitions by using IM configuration management, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Note that only the following JP1 events registered on the local event server are subject to the execution condition of the local action (event filter defined in the local action execution definition file):

- Event issued from the local event server to the local event server (JP1 event registered reason: 1)
- Event issued from the remote event server to the local event server (JP1 event registered reason: 3)
An example is an event registered by using the `jevsend` command (with the `-d` option specified) or the `jevsendd` command from another event server (of the local host) to the local event server.

JP1 events forwarded from the remote event server (JP1 event registered reason: 4) are not applicable.

2.8.2 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`)

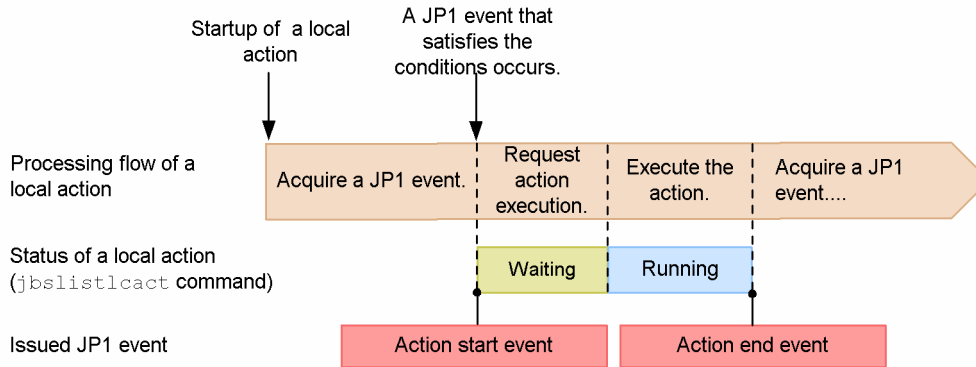
2.8.3 Execution status of local actions

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 `jbslistlact` 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 2–42: Changes to the execution status of local actions



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.

2.8.4 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.

2.9 Support for system configurations

2.9.1 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 *5. Setting Up JP1/Base for Use in a Cluster System*.

2.9.2 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 *5.9 Setting up a logical host in a non-cluster environment*.

2.10 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 [6. JP1/Base Communication Settings According to Network Configurations](#) also apply to products such as JP1/IM and JP1/AJS 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 [6. JP1/Base Communication Settings According to Network Configurations](#).



Note

- As for communication with the event service, only a dedicated communication protocol that uses an event server settings file (`conf`) was supported in JP1/Base version 9 or earlier. In JP1/Base version 10 or later, `jplhosts2` information is supported. As with other types of JP1/Base functionality, communication based on `jplhosts2` information also uses the communication settings of JP1/Base. We recommend that you use `jplhosts2` information for communication unless you have a specific reason for using `jplhosts` information. Note that communication with the event service does not support the communication settings in version 06-51 or earlier.
- When using `jplhosts2` information, the host definition that is defined for a physical host for name resolution can also be used for the logical host. This functionality is called *physical merge mechanism*. Unless there is any special reason, we recommend that you create a host definition only for the physical host.

2.10.1 Recommended communication protocol

We recommend the following binding methods for communication on JP1/Base.

(1) Recommended communication protocol when running JP1/Base on a physical host only

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.

(2) Recommended communication protocol when using a logical host (using a cluster)

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 set 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

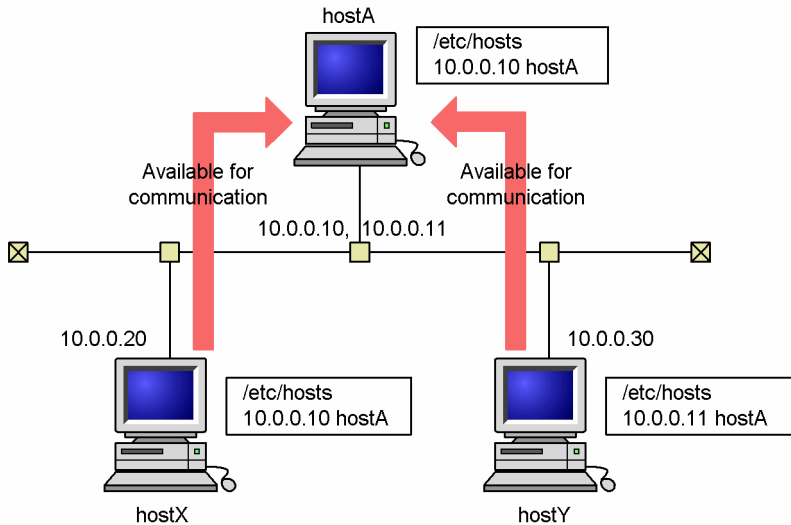
Once a host is set up for a cluster system, the communication protocol of physical hosts does not return to the ANY binding method even when all logical hosts are removed. To revert to operation using physical hosts only, change the communication protocol back to the ANY binding method by following the instructions in [6.3.2 Changing the JP1/Base communication protocol](#).

2.10.2 Changes in communication waiting process between the ANY and the IP binding methods

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.

(1) Communication waiting process when JP1/Base is activated in the ANY binding method

Figure 2–43: Communication waiting process when JP1/Base is activated in the ANY binding method on hostA



Legend:

: Host information

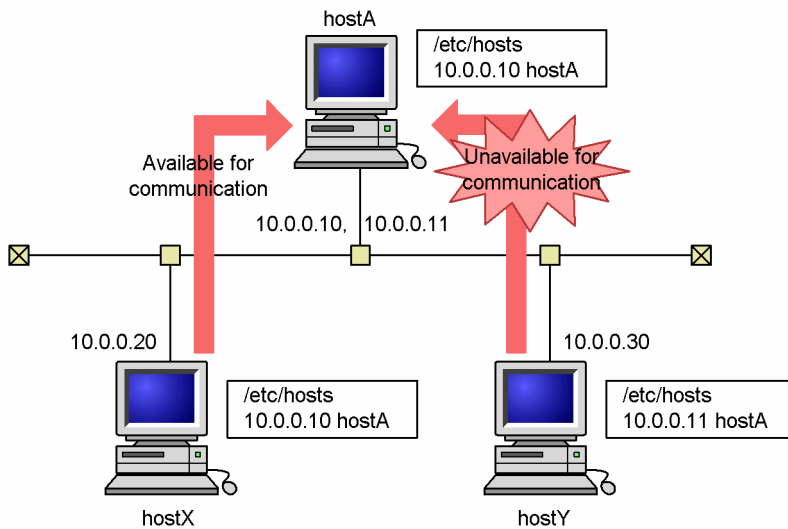
hostA has an NIC to which IP addresses 10.0.0.10 and 10.0.0.11 are assigned. This host is assumed to be able to resolve its own host name only into IP address 10.0.0.10. (In fact, depending on the OS, the host might only be able to resolve one host name into one IP address.) hostX assumes that hostA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

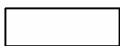
(2) Communication waiting process when JP1/Base is activated in the IP binding method

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

Figure 2–44: Communication waiting process when JP1/Base is activated in the IP binding method on hostA



Legend:

 : Host information

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.

2.10.3 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:

```
jplping host-name
```

For details on this command, see the section for *jplping* in *15. Commands*.

2.10.4 Notes on communication protocols of JP1/Base

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 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).
- In an environment with multiple LAN connections where a host name resolves to multiple IP addresses, JP1/Base uses the IP address with the highest priority for the host name.
- If JP1/Base uses the IP binding method for sending, the IP address with the highest priority for the local host name is used as the source IP address.
- A communication failure occurs when a non-loop-back address attempts to connect to a loop-back address or vice versa, even if the non loop-back address is an address within a same host. Therefore, a loop-back address cannot be used to operate JP1/Base. In addition, no host name that becomes a loop-back address as a result of address resolution can be used.
- If JP1/Base is using the IP address and host name that are defined in the `hosts` file, make sure the combination of IP address and host name is not duplicated.
- In Linux, in an environment that uses JP1/Base, do not set `net.ipv4.ip_nonlocal_bind` to 1. If `net.ipv4.ip_nonlocal_bind` is set to 1, profile collection by JP1/IM Configuration Management fails. The setting of `net.ipv4.ip_nonlocal_bind` can be checked by using the `sysctl` command.

```
# sysctl net.ipv4.ip_nonlocal_bind
```

If `net.ipv4.ip_nonlocal_bind` is set to 1, follow one of the following procedures:

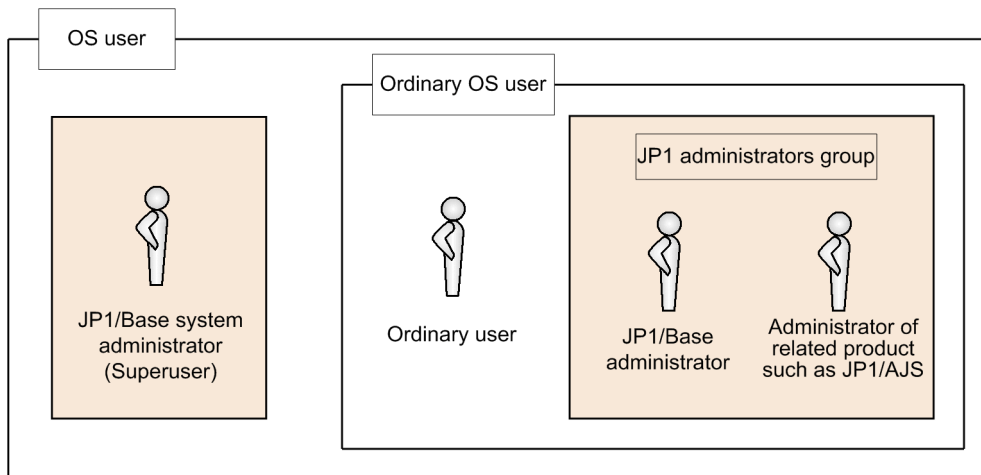
- Delete this parameter from `/etc/sysctl.conf`, and then restart the system or execute "`sysctl -w net.ipv4.ip_nonlocal_bind=0`", and then restart JP1/Base and the JP1 programs for which JP1/Base is a prerequisite.
- Change the setting in `/etc/sysctl.conf` to "`net.ipv4.ip_nonlocal_bind=0`", execute the "`sysctl -p`" command, and then restart JP1/Base and the JP1 programs for which JP1/Base is a prerequisite.
- JP1/Base cannot be used in an environment where a unique host name or IP address cannot be resolved from the host name at communication with the server. For this reason, JP1/Base does not support dynamic NAT (in which the host is assigned an address available at the time, and rules are set and changed automatically). Nor does JP1/Base support NATP containing port translations (IP Masquerade and NAT+).
- Using DHCP
If the IP addresses used by JP1/Base are managed using DHCP, set an unlimited duration for the IP address lease so that the IP address does not change.
JP1/Base will not work properly if the IP address changes during JP1/Base operation.

2.11 Managing JP1/Base as a JP1/Base administrator (UNIX only)


By setting up a JP1 administrators group and a JP1/Base administrator, you can operate JP1/Base from an OS user account that does not have system administrator (superuser) privileges for JP1/Base. The JP1 administrators group is an OS user group that any user can create. A user who belongs to the JP1 administrators group and has been given permission to operate JP1/Base is called a *JP1/Base administrator*.

The following figure shows the relationship between the JP1 administrators group and the JP1/Base administrator.

Figure 2–45: Relationship between JP1 administrators group and JP1/Base administrator



Legend:

 : Can use JP1/Base.

A JP1/Base administrator is able to operate JP1/Base on behalf of the JP1/Base system administrator, provided that the JP1/Base system administrator has enabled this feature.

For details on how to operate JP1/Base as a JP1/Base administrator, see *J. Operating JP1/Base as a JP1/Base Administrator (UNIX Only)*.

2.12 JP1/Base compatibility

This section describes the compatibility between JP1/Base and program products supported by event service functionality, and the compatibility between JP1/Base Version 10 and previous versions.

2.12.1 Compatibility and connectivity with previous versions of JP1/Base

JP1/Base Version 9 is compatible with previous version of JP1/Base. However, for connectivity with previous versions, JP1/Base follows the same restrictions that higher program products (such as JP1/IM - Manager and JP1/AJS3) have. For details about connectivity of a higher program product, see the manual for the program product. Also, note the following cases.

(1) 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 Version 7 or earlier and you want to preserve the command execution log (ISAM) files 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 15. *Commands*.

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

(2) 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.

(3) 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.

(4) 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 [15. Commands](#).

(5) Communicating with hosts that do not have a means of encrypted communication

Imagine a situation where communication takes place between an in-house environment and a cloud environment. In this situation, multiple communication modes might be used for communication between the two environments, with agent hosts in the in-house environment using non-SSL communication and those in the cloud environment using SSL communication. In this case, communication with hosts that do not have a means of encrypted communication can be established by setting the hosts that use non-SSL communication in the non-SSL communication host configuration file.

For details on the non-SSL communication host configuration file, see [Non-SSL communication host configuration file](#) in [16. Definition Files](#).

3

Installation and Setup

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

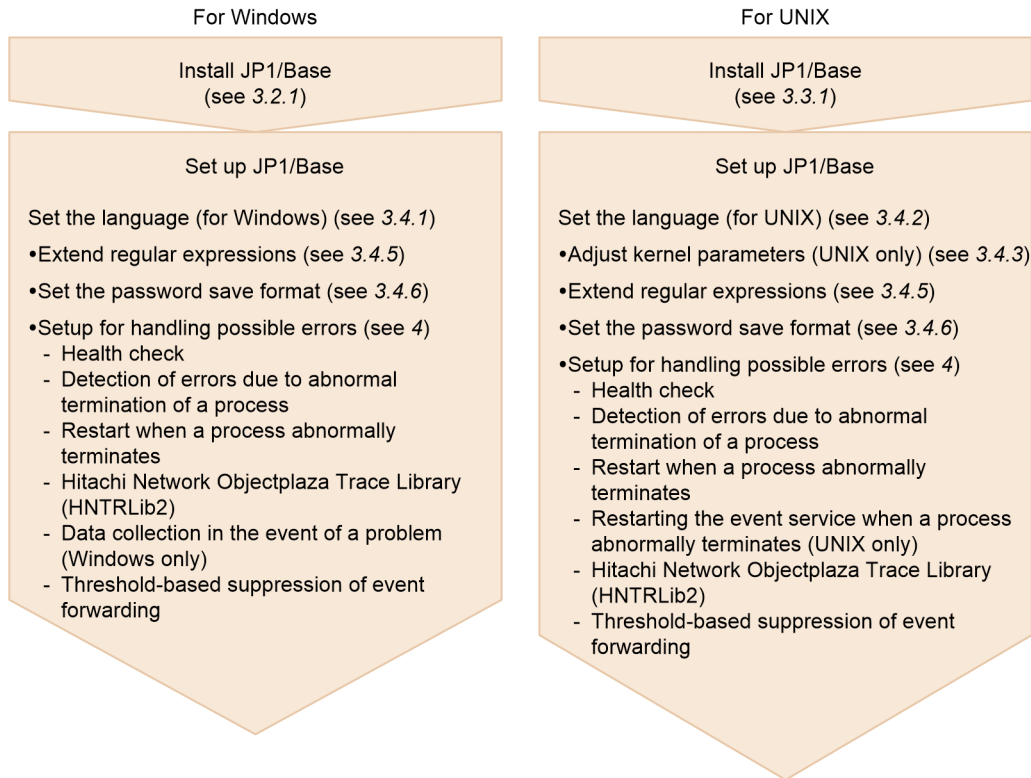
Note that before you install JP1/Base, you must apply the additional OS packages and patches that are required by JP1/Base. For details, see the *Release Notes*.

3.1 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 3–1: Installation and setup overview



3.2 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.

3.2.1 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 media into the drive.

Start the installer, select JP1/Base included with JP1/AJS or JP1/IM, and then follow the instructions provided by the installer to complete the installation.

During installation, set the following items:

- User information
- Installation folder

The default installation folder is as follows:

`system-drive\Program Files (x86)\Hitachi\JP1Base`

Note: Do not install the files under `system-drive\Program Files` in an x64 environment. Doing so might cause problems as a result of mixing with 64-bit modules.

- 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 3–1: Initial settings for user management function

Item	Contents	
Authentication server settings	Authentication server name	Local host name
JP1 user settings	JP1 user name	jpladmin
	Password	jpladmin
	JP1 resource group	*
	Granted permissions	JP1_AJS_Admin, JP1_JPQ_Admin, JP1_AJSCF_Admin, JP1_CSA_Admin, JP1_HPS_Admin, JP1_PFM_Admin, JP1_Console_Admin, JP1_CF_Admin, JP1_CM_Admin, JP1_Rule_Admin, JP1_ITSLM_Admin, JP1_Audit_Admin, JP1_DM_Admin, JP1_SSO_Admin, Cosminexus_vMNG_Admin, HCS_UserMng_Admin, HCS_HDvM_Admin, HCS_HRpM_Admin, HCS_HTSM_Admin, HCS_HSNM2_Modify, HCS_HFSM_Admin, HCS_HCSM_Admin, HCS_HGLM_Admin, HCS_HTnM_Admin, JP1_AO_Admin, JP1_IMNP_Admin, UCNP_Admin, HNP_Admin, JP1_Analytics_Admin, JP1_ITDM_Admin, ISCF_Admin, JP1_IOTDM_Admin, JP1_IOTDM_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	jpladmin
	Server host name	*
	Mapping between the JP1 user and OS user	The JP1 user (jpladmin) 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 *8.1 User management setup (in Windows)*.

At execution, the Installer automatically installs the Hitachi Network Objectplaza Trace Library (HNTRLib2). The installation folder is as follows:

HNTRLib2 for 32bit

system-drive\Program Files (x86)\Hitachi\HNTRLib2

HNTRLib2 for 64bit

system-drive\Program Files\Hitachi\HNTRLib2

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

3. Restart the system.

Restart Windows if prompted.

Remote installation of JP1/Base (software deployment) through JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/Software Distribution

JP1/Base supports remote installation through JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/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/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/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.

See JP1/NETM/DM, JP1/IT Desktop Management 2 or Job Management Partner 1/Software Distribution Manual for more information.

Be sure to use a JP1/NETM/DM 09-00 or later packager, a JP1/IT Desktop Management 2 packager or a Job Management Partner 1/Software Distribution 09-00 or later packager to package this software product.

JP1/NETM/DM is sold only in Japan.

3.2.2 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. Uninstall JP1/Base.

In the Control Panel, click **Programs and Features** and uninstall **JP1/Base**.

If a product that requires JP1/Base is installed, the KAVA1870-E message is output and uninstallation cannot be performed.

In this case, first uninstall the applicable JP1 product, and then uninstall **JP1/Base**.

3. Restart the system.

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

4. Delete user files.#

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

To return the system to its original state, use Windows Explorer to delete the folder in which JP1/Base was installed.

#: 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.

3.2.3 Notes on installing and uninstalling JP1/Base

- Before installation, terminate all resident applications, including virus check software. If you do not do so, installation might fail.
- You need administrator permissions to perform installation, setup, or uninstallation. In an environment for which UAC is enabled, an ordinary user must be granted such permissions to perform these operations. Additionally, even if UAC is not enabled for the environment, log on as a user who belongs to the Administrators group to perform these operations.
- Do not set the startup type to disabled for the services below if you perform installations, perform uninstallations, or apply corrective patches. If the type is set to disabled, then the operations stated above might fail.
 - Application Experience service
 - Windows Modules Installer service
- The following message dialog box may appear if you attempt to overwrite or uninstall this product while it is running.

The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

If this dialog appears, aborts the operation by clicking the Cancel button, close all running JP1/Base services and applications currently using JP1/Base, and then retry the operation.

- Do not install this product at a path that contains any of the 3rd or 4th level JIS characters.
- Restart the computer if the system requests a restart after any of the following:
 - When installing for the first time
 - When performing an overwrite installation
 - When performing an upgrade installation

(1) Installation

- Do not install JP1/Base in a folder in which another program product is installed.
- The highest-level folder (JP1Base), its subfolders, and files created by JP1/Base inherit the permissions the user assigns to the installation folder. We recommend that permissions are assigned to the installation folder as follows:
 - Administrators group and SYSTEM account: Full Control

- Users account: Read & Execute
- 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.

- When you install JP1/Base, the paths for the `bin` folder and the `bin\ext` folder of JP1/Base are automatically added to the `PATH` environment variable. JP1/Base cannot be installed if this would cause the length of the `PATH` environment variable to exceed the maximum permitted by the operating system. In this situation, remove unwanted paths from the `PATH` environment variable and repeat the installation process.
- If several paths are in the `PATH` environment variable, paths are prioritized according to the order in which they are specified. If the path to the `bin` folder of JP1/Base is specified later than that of the `bin` folder for JP1/AJS3 - View or JP1/IM - View in the `PATH` environment variable, products such as JP1/IM - Manager and JP1/AJS3 that have JP1/Base as a prerequisite might not operate correctly. Make sure that the path for the JP1/Base `bin` folder appears before the JP1/AJS3 - View and JP1/IM - View `bin` folder in the `PATH` environment variable.
- When you install this product for the first time and select the installation folder from the screen, a folder named "Hitachi" is created under "*system-drive*: \Program Files (x86)". The folder name starts with uppercase "H" and is followed by lowercase letters, regardless of the combination of uppercase and lowercase letters that you specify.

For example, the folder name is "Hitachi" even if you specify "HITACHI" or "hitachi".

Use of the folder name "Hitachi" does not cause any problems with operations, so you can continue to use it without any problem occurring.

- Do not include symbols (`;` `#` `'` `%` and so on) in the installation folder name; otherwise, JP1/Base will not work properly.
- The drive on which this product is to be installed must be the local drive. Do not use a network drive.
- Before installation, stop the following programs. After installation, if the OS requests that you restart the computer, do so by following the instructions.
 - All JP1/Base services
 - All services for the products based on JP1/Base
 - Applications using JP1 events
 - Service for the integrated trace function (HNTRLib2)
- When installing this product or executing the command `jp1bshasetup`, Windows Defender might output warning messages. These warning messages, however, are output due to the registration of services and may be safely ignored.
- If the path at which this product is installed meets the following conditions, profiles cannot be collected or applied properly in IM Configuration Management:

(a) The path of the installation folder includes either left or right parentheses, but does not include a space character.

Example: `C:\ProgramFiles(x86)\Hitachi\JP1Base\`

(b) The path of the installation folder includes special characters.

Example: `C:\JP1@\Program Files (x86)\Hitachi\JP1Base\`

Example: `C:\JP1&\Program Files (x86)\Hitachi\JP1Base\`

Example: `C:\JP1^\Program Files (x86)\Hitachi\JP1Base\`

When using IM Configuration Management, do not install this product in the types of paths shown above. We have confirmed that there are no problems installing JP1/Base in the following path:

Example: `C:\Program Files (x86)\Hitachi\JP1Base\`

(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 both JP1/Base and JP1/IM - Manager, and then reinstall JP1/Base and 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.
- If reinstalling JP1/Base after forcibly uninstalling it without uninstalling the product that requires JP1/Base, it is necessary to restore the common definition information other than JP1/Base that has been backed up. For the procedure to restore backed-up common definition information, see *(10) Procedure for restoring common definition information of a JP1 product that requires JP1/Base*.
- 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.

(3) Setting the Windows environment

When you install JP1/Base, the path of the Hitachi common folder is set in the `PATH` environment variable as the path of the JP1/Base `bin` folder and Hitachi Network Objectplaza Trace Library (HNTRLib2) as follows:

Path of the Hitachi common folder

HNTRLib2 for 32bit

```
system-drive\Program files (x86)\Common Files\HITACHI
```

HNTRLib2 for 64bit

```
system-drive\Program files\Common Files\HITACHI
```

In addition, the port numbers listed in *C. List of Port Numbers* are added to the `services` file.

(4) Uninstallation

- If any of the following products is installed, the KAVA1870-E message is output, and uninstallation cannot be performed.
 - JP1/AJS3 - Manager
 - JP1/AJS3 - Agent
 - JP1/AJS3 - Agent Minimal Edition
 - JP1/AJS3 - WOA
 - JP1/Power Monitor

- JP1/IM2 - Manager
- JP1/IM2 - View
- JP1/IM2 - EG
- 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\HCDINST\product-model-name[_{1|2|3|4|5}].LOG`
- When you uninstall JP1/Base, the path of the JP1/Base `bin` folder is removed from the `PATH` environment variable and the port numbers that were added to the `services` file are removed. The service `jp1imcmda` is not deleted from systems where JP1/IM - View is also installed. Manually delete any remaining settings for which you have no further need. However, take care not to delete the service `jp1imcmda` if JP1/IM - View is installed on the system. Take particular care not to delete the path for the Hitachi common folder, which is used by a number of products other than the Hitachi Network Objectplaza Trace Library (HNTRLib2).
- When you uninstall JP1/Base, the program folder may remain in the Start menu. Remove the program folder if no longer required, referring to the Windows help.
- Before uninstalling JP1/Base, confirm that no product for which JP1/Base is a prerequisite is currently installed.

(5) Overwrite installation

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

- 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 or later 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 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 15. *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 16. *Definition Files*.
2. Execute the `jevdbmkrep` command.
For details on the `jevdbmkrep` command, see *jevdbmkrep* in 15. *Commands*.
3. Start the event server.

- The log-file trap startup definition file (`jevlog_start.conf`) is new in version 10-00. If you link with version 10-00 or later of JP1/IM, you can use the IM configuration management feature with this file to control the starting and stopping of log file traps.

If you intend to use IM configuration management to control the starting and stopping of log file traps, and have defined the startup of a log file trap in the start sequence definition file (`JP1SVPRM.DAT`), use the following procedure to migrate the definition to the log-file trap startup definition file:

- From the start sequence definition file, delete the startup definition for the log file trap.
- In the log-file trap startup definition file, enter the settings for the log file trap that you want to stop and start.

For details on the log-file trap startup definition file, see *Log-file trap startup definition file* in *16. Definition Files*.

Note the following when migrating these definitions:

- You must specify the name of the log-file trap startup definition file in the `-f` option of the `jevlogstart` command.
- Do not specify a monitoring target name or log-file trap action definition file name that is already being used by another log file trap. If the name is already in use, choose another.
- In version 11-00, the menu item names displayed when you select **Programs** and then **JP1_Base** from the Windows **Start** menu have been changed. If you upgrade JP1/Base from version 10-50 or earlier as an overwrite installation, the menu item names change as follows:

Menu item names in 10-50 or earlier	Menu item names in 11-00 or later
setup	JP1_Base Setup
Administrator Console	JP1_Base Console

Note: You can change menu item names as you like.

- In versions 11-50 or later, the number of records in the command execution log file (initial setting is 20,000 records) may be insufficient in case of a large-scale system (1,024 or more agents) to use JP1/IM - Manager's remote commands or automated actions, and therefore we recommend that you expand the setting of the number of records.

If the function for automatically re-organizing the command execution log file is enabled however, the amount of time required for startup might increase in proportion to the file size. Therefore, confirm beforehand that the newly specified number of records does not hinder operation. For details, see *4.9 Function for automatically re-organizing the command execution log file*.

- An overwrite installation of JP1/Base may require a restart.
- Before overwrite-installing JP1/Base, stop the products based on JP1/Base.
- Before overwrite-installing JP1/Base, stop the products that use HNTRLlib2.

You can use the `hntr2getname` command to acquire information about which products are using HNTRLlib2. Start the command prompt, execute following commands:

```
cd system-drive\Program Files\Hitachi\HNTRLlib2\bin\  
hntr2getname
```

- 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.
- If there is only one FQDN format event server name in the Event server index file for the JP1/Base physical host and you call the JP1 event acquisition function, add the definition of * (indicating that the event server name runs on local host) as event-server-name. (This works on JP1/Base version 12-10 or later.) If you do not add the definition mentioned above, the JP1 event acquisition function fails.

For details, see *Event server settings file* of *16. Definition Files*.

- When upgrading to 13-00 or a later version of JP1/Base from 12-50 or an earlier version by performing an overwrite installation, files and folders used by functions linking products using JP1/SES events will be kept. These files and folders have no effect on the operation of JP1/Base.

(6) Language settings in Windows

1. Verify that all the language settings are uniformly set to Japanese, English, or Chinese (simplified), and then install the product.

- For Windows Server 2016:

Contents	Setting	Language setting
System locale	Control Panel - Region - Administrative - Change system locale - Region settings	Language for non-Unicode programs
Format for languages and regions	Control Panel - Region - Format	Format
	Control Panel - Region - Location	Home location

- For Windows Server 2022, Windows Server 2019:

Contents	Setting	Language setting
System locale	Control Panel - Region - Administrative - Change system locale - Region settings	Language for non-Unicode programs
Format for languages and regions	Control Panel - Region - Format	Format
	Setting - Region	Region and Regional format

Note

Selecting the **Beta: Use Unicode UTF-8 for worldwide language support** check box may cause text to appear garbled. This check box appears by opening the **Control Panel**, navigating from the Region dialog box to the **Administrative** tab, and clicking **Change system locale** in **Language for non-Unicode programs**.

2. After changing the language setting, select **Control Panel**, open the **Region** window, then click the **Administrative** tab. In the **Welcome screen and new user accounts** area, select the **Copy settings** check box to copy the settings, and then restart the operating system.

3. Install JP1/Base.

(7) Notes on upgrading JP1/Base

JP1/Base can be upgraded by an overwrite installation. Definitions are inherited from the previous version, but note the following points.

If you manually reorganized the previous version's program folder, it will not be removed when you perform an upgrade installation. Remove the old program folder if no longer required after finishing the upgrade.

(8) Notes on performing installation using disk replication

This is a Hitachi program product that supports the installation of replicated disks by JP1/ServerConductor/Deployment Manager and Hitachi Compute Systems Manager Deployment Manager Plug-in, or replication functionality that uses image files provided by virtualized platforms.

When performing disk replication installation, we recommend that you replicate the default settings of each JP1/Base definition file after installation and setup.

However, if you change the settings and then use the same settings in the target replication hosts, note the following points.

(a) Precautions for before replication

Setting the user management functionality

If Administrator privileges are specified for the OS user for user mapping, re-specify the settings after the replication.

Setting the processing environment of the event service

Do not set IP addresses or host names for each parameter in the event server index file, the event server settings file, or the API settings file.

Deleting definition information for system configurations

When defining the target replication host under the system configuration in JP1/IM, delete the previously set configuration information by using the `jbsrt_del` command.

(b) Precautions for after replication

Initializing the event database

JP1 events might remain in the event database if you restart the computer with an internally generated host name at the time of disk replication installation. Initialize the event database before operation starts.

For operational procedures, see the *JP1/ServerConductor/Deployment Manager User's Guide* and *Hitachi Compute Systems Manager Deployment Manager Plug-in User's Guide*. For details about the replication functionality of virtualized platforms, see the product manual.

(9) Notes on the silent installation functionality

This software product can be installed by using the silent installation functionality.

Execute the following command:

```
Drive-of-supplied-media:\_OWNEXE\HPPSINST.BAT /Drive-of-supplied-media:\_P  
PDIR\PCC2A2C6LDL\DISK1 /"full-path-of-installation-destination"
```

Notes on performing silent installation

- To execute the contents of supplied media directly from a hard drive, copy the contents of the supplied media to a directory on the hard drive whose path does not include any spaces. Then, compare the copied files to the original files (at the binary level, for example) to ensure that they are the same.
- Check the return value of the execution result to verify that the installation ended successfully. For details on return values, see descriptions on the silent installation in documents published on the JP1 website.

(10) Procedure for restoring common definition information of a JP1 product that requires JP1/Base

The following describes the procedure for restoring common definition information when reinstalling JP1/Base without uninstalling the JP1 product that requires JP1/Base.

Note: Do not start the JP1/Base service or other JP1 product service during the restore procedure.

And execute the following command to backup the common definition information of all JP1 products in case of performing incorrect procedure to restore the common definition information.

- Physical host:

```
jbsgetcnf > backup-file-name
```

- Logical host:

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

1. Back up JP1/Base.

For details on backups, see [3.5.2 Backup and recovery \(in Windows\)](#).

If JP1/IM - Manager is installed, backup the command execution log (ISAM) file. For details about the backup of command execution log (ISAM) file, see the manual *JP1/Integrated Management 3 - Manager Administration Guide (Database backup and recovery)*.

Collect the log data before you perform the procedure to restore the common definition information in case the integrated trace log is deleted. For details on collecting log data, see [18.4 How to collect data](#).

2. Check the output destination of the common definition information backup file.

Check whether there is sufficient free disk space ($1 + 0.4 \times \text{number-of-logical-hosts}$ [MB] or more) for the output destination of the common definition information backup file (*Windows-installation-folder*\Temp\). And check whether the common definition information backup file and output folder have not been locked by applications like editor. And also check for the access permission.

If there is insufficient free disk space, the common definition information backup file will not be output correctly. For example, the file size of the common definition information backup becomes 0 byte.

If folder or file has been locked by some application or if you do not have access permission, error message KAVA1871-E will be output during the uninstallation.

3. Set the JP1_BASE_UNINST_FORCE system environment variable to 1.

4. Uninstall JP1/Base.

In the Control Panel, click **Programs and Features** and uninstall **JP1/Base**.

Uninstallation can be performed even if the prerequisite products of JP1/Base are installed.

During the uninstallation, common definition information excluding JP1/Base is output as the common definition information backup file.

- Physical host: *Windows-installation-folder*\Temp\JP1_COMDEF\comdef_JP1_DEFAULT.conf
- Logical host: *Windows-installation-folder*\Temp\JP1_COMDEF\comdef_logical-host-name.conf

5. Clear the setting of the JP1_BASE_UNINST_FORCE environment variable.

6. Restart the system.

Restart the system to disable the JP1/Base operating environment.

7. Delete user files.

Use Windows Explorer to delete the JP1/Base files and folders.

8. Reinstall JP1/Base.

For details on install, see [3.2.1 Installing JP1/Base](#).

You cannot change the installation folder.

9. Re-set up JP1/Base.

If you are operating in a cluster, create a logical host.

The logical host name (Uppercase/Lowercase) and shared folder name cannot be changed.

Recover the adapter command configuration file (*installation-folder\plugin\conf*.conf*) from the backup in step 1.

If JP1/IM - Manager is installed, recover the command execution log (ISAM) file from the backup in step 1.

Recover the event database from the backup in step 1. For details on recovering the event database, see [3.5.2\(4\)\(a\) When the forwarding settings file is not configured to forward JP1 events to other hosts](#).

Build the JP1/Base environment.

- When recovering the JP1/Base environment:
Recover the JP1/Base other definition files, common definition information, and `jp1hosts2` information from the backup in step 1.
For details on recovery, see [3.5.2 \(3\) Recovering JP1/Base setup information](#).
- When rebuilding JP1/Base environment:
Perform JP1/Base setup again.
For details on setup, see [3.4 JP1/Base setup](#).
And also, perform other settings as necessary.

If you have set up JP1/Base in the setup of another product, set it up again.

10. Execute the `jbssetcnf` command using the common definition information backup file output in step 4.

Restore the common definitions for JP1 products excluding JP1/Base. Execute the command for the physical host and all logical hosts.

```
jbssetcnf common-definition-information-backup-file-name
```

11. Delete the common definition information backup file output folder that is created in step 4.

Delete the common definition information backup file output folder (*Windows-installation-folder\Temp\JP1_COMDEF*).

3.3 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.

3.3.1 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 [3.3.2 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 3–2: Initial settings for user management function

Item	Contents	
Authentication server settings	Authentication server name	Local host name
JP1 user settings	JP1 user name	jpladmin
	Password	jpladmin
	JP1 resource group	*
	Granted permissions	JP1_AJS_Admin, JP1_JPQ_Admin, JP1_AJSCF_Admin, JP1_CSA_Admin, JP1_HPS_Admin, JP1_PFM_Admin, JP1_Console_Admin, JP1_CF_Admin, JP1_CM_Admin, JP1_Rule_Admin, JP1_ITSLM_Admin, JP1_Audit_Admin, JP1_DM_Admin, JP1_SSO_Admin, Cosminexus_vmNG_Admin, HCS_UserMng_Admin, HCS_HDvM_Admin, HCS_HRpM_Admin, HCS_HTSM_Admin, HCS_HSNM2_Modify, HCS_HFSM_Admin, HCS_HCSCM_Admin, HCS_HGLM_Admin, HCS_HTnM_Admin, JP1_AO_Admin, JP1_IMNP_Admin, UCNP_Admin, HNP_Admin, JP1_Analytics_Admin, JP1_ITDM_Admin, ISCF_Admin, JP1_IOTDM_Admin
User mapping settings	JP1 user name to be mapped	jpladmin
	Name of the server host where the JP1 user issues operating instruction	*
	Mapping between the JP1 user and OS user	The JP1 user (jpladmin) is mapped to an OS user (root) registered with each host.

For details on each item, see [8.3 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/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/Software Distribution:

JP1/Base supports remote installation through JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/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.
- Upgrade to a newer version
You can upgrade an existing JP1/Base program to a newer version on the target host through remote installation.

See JP1/NETM/DM, JP1/IT Desktop Management 2 or Job Management Partner 1/Software Distribution Manual for more information.

Be sure to use a JP1/NETM/DM 09-00 or later packager, a JP1/IT Desktop Management 2 packager or a Job Management Partner 1/Software Distribution 09-00 or later packager to package this software product.

JP1/NETM/DM is sold only in Japan.

3.3.2 Using the Hitachi Program Product Installer

The Hitachi Program Product Installer is stored on the medium supplied with JP1/Base.

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 drive.

Execute the command as follows:

The mounting method differs depending on the OS, hardware, and environment. For details on how to mount the drive, see the documentation for your OS.

Command for AIX:

```
/usr/sbin/mount -r -v cdrfs /dev/cd0 /cdrom
```

Command for Linux:

```
/bin/mount -r -o mode=0544 /dev/cdrom /mnt/cdrom
```

Note that the device special file name (in italics), and the mount directory name of the provided media file system (underlined) differs depending on the environment.

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

```
/cdrom/XXXX/setup /mnt/cdrom
```

XXXX differs depending on your operating environment.

In Linux, the drive is mounted automatically. Specify the device special file name for the automatically mounted drive in place of /mnt/cdrom.

(2) Installing JP1/Base

You can install JP1/Base using the Hitachi Program Product Installer. The initial window appears when you start the Installer. An example is shown in the following figure.

Figure 3–2: 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

You can uninstall (delete) JP1/Base using the Hitachi Program Product Installer.

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

```
/etc/hitachi_setup
```

The initial Installer window appears. [For an example, see Figure 3-2.](#)

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

You can use the Hitachi Program Product Installer to view version information for Hitachi products installed on your system.

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

```
/etc/hitachi_setup
```

The initial Installer window appears. For an example, see Figure 3-2.

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

3.3.3 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. 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.

If a product that requires JP1/Base is installed, `Deletion failed.` is displayed, and uninstallation fails. In this case, check that the KAVA1870-E message has been output to the following JP1/Base installation log (latest log file):

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

After uninstalling the applicable JP1 product, uninstall JP1/Base following the instructions of Hitachi Program Product Installer.

Note

Uninstalling JP1/Base causes HNTRLlib2 to be uninstalled automatically. If the system contains other programs that use HNTRLlib2, however, HNTRLlib2 is not uninstalled until all of those programs are uninstalled.

3.3.4 Notes on installing and uninstalling JP1/Base

(1) Installation

- If you see a message stating that installation failed while using the Hitachi Program Product Installer, the installation log is output to 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 `/tmp/HITACHI_JP1_INST_LOG` directory.

- Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

(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 *15. 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 reinstalling JP1/Base after forcibly uninstalling it without uninstalling the product that requires JP1/Base, it is necessary to restore the common definition information other than JP1/Base that has been backed up. For the procedure to restore backed-up common definition information, see *(8) Procedure for restoring common definition information of a JP1 product that requires JP1/Base*.

(3) Setting the OS environment

At JP1/Base installation, the port numbers listed in *C. List of Port Numbers* are added to the `/etc/services` file. This information is removed when JP1/Base is uninstalled.

(4) 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`
- 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.

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

- The port numbers for the `jesrd` service are not removed from the `services` file. Delete them if they are no longer needed.
- If any of the following products is installed, the KAVA1870-E message is output, and uninstallation cannot be performed.
 - JP1/AJS3 - Manager
 - JP1/AJS3 - Agent
 - JP1/AJS3 - Agent Minimal Edition
 - JP1/AJS3 - WOA
 - JP1/Power Monitor
 - JP1/IM2 - Manager
 - JP1/IM2 - View
 - JP1/IM2 - EG

(5) Overwrite installation

Note the following if you are performing an overwrite installation of JP1/Base in an environment running an earlier version of a JP1 program:

- 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 or later 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 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 15. *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 16. *Definition Files*.
 2. Execute the `jevdbmkrep` command.
 - For details on the `jevdbmkrep` command, see *jevdbmkrep* in 15. *Commands*.
 3. Start the event server.
- The log-file trap startup definition file (`jevlog_start.conf`) is new in version 10-00. If you link with version 10-00 or later of JP1/IM, you can use the IM configuration management feature in conjunction with this file to control the starting and stopping of log file traps.

If you intend to use IM configuration management to control the starting and stopping of log file traps, and have defined the startup of a log file trap in `jbs_start`, use the following procedure to migrate the definition to the log-file trap startup definition file.

- Delete the startup definition for the log file trap from `jbs_start`.
- In the log-file trap startup definition file, enter the settings for the log file trap that you want to stop and start.

For details on the log-file trap startup definition file, see *Log-file trap startup definition file* in *16. Definition Files*.

Note the following when migrating these definitions:

- You must specify the name of the log-file trap startup definition file in the `-f` option of the `jevlogstart` command.
- Do not specify a monitoring target name or log-file trap action definition file name that is already being used by another log file trap. If the name is already in use, choose another.
- In versions 11-50 or later, the number of records in the command execution log file (initial setting is 20,000 records) may be insufficient in case of a large-scale system (1,024 or more agents) to use JP1/IM - Manager's remote commands or automated actions, and therefore we recommend that you expand the setting of the number of records. If the function for automatically re-organizing the command execution log file is enabled however, the amount of time required for startup might increase in proportion to the file size. Therefore, confirm beforehand that the newly specified number of records does not hinder operation. For details see *4.9 Function for automatically re-organizing the command execution log file*.
- 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.
- If there is only one FQDN format event server name in the Event server index file for the JP1/Base physical host and you call the JP1 event acquisition function, add the definition of `*` (indicating that the event server name runs on local host) as event-server-name. (This works on JP1/Base version 12-10 or later.) If you do not add the definition mentioned above, the JP1 event acquisition function fails.
For details, see *Event server settings file* of *16. Definition Files*.
- When upgrading to 13-00 or a later version of JP1/Base from 12-50 or an earlier version by performing an overwrite installation, files and folders used by functions linking products using JP1/SES events will be kept. These files and directories have no effect on the operation of JP1/Base.

(6) Notes on performing installation using disk replication (Linux only)

This is a Hitachi program product that supports the installation of replicated disks by JP1/ServerConductor/Deployment Manager and Hitachi Compute Systems Manager Deployment Manager Plug-in, or replication functionality that uses image files provided by virtualized platforms.

When performing disk replication installation, we recommend that you replicate the default settings of each JP1/Base definition file after installation and setup.

However, if you change the settings and then use the same settings in the target replication hosts, note the following points.

(a) Precautions for before replication

Setting the processing environment of the event service

Do not set IP addresses or host names for each parameter in the event server index file, the event server settings file, or the API settings file.

Deleting definition information for system configurations

When defining the target replication host under the system configuration in JP1/IM, delete the previously set configuration information by using the `jbsrt_del` command.

(b) Precautions for after replication

Initializing the event database

JP1 events might remain in the event database if you restart the computer with an internally generated host name at the time of disk replication installation. Initialize the event database before operation starts.

For operational procedures, see the *JP1/ServerConductor/Deployment Manager User's Guide* and *Hitachi Compute Systems Manager Deployment Manager Plug-in User's Guide*. For details about the replication functionality of virtualized platforms, see the product manual.

(7) Notes on the silent installation functionality

This software product can be installed by using the silent installation functionality.

Execute the following command:

In AIX:

```
Supplied-media/AIX/setup -f -k Product-type-No Path-of-supplied-media
```

In Linux:

```
Supplied-media/X64LIN/setup -f -k Product-type-No Path-of-supplied-media
```

Notes on performing silent installation

- To execute the contents of supplied media directly from a hard drive, copy the contents of the supplied media to a directory on the hard drive whose path does not include any spaces. Then, compare the copied files to the original files (at the binary level, for example) to ensure that they are the same.
- Check the return value of the execution result to verify that the installation ended successfully. For details on return values, see descriptions on the silent installation in documents published on the JP1 website.

(8) Procedure for restoring common definition information of a JP1 product that requires JP1/Base

The following describes the procedure for restoring common definition information when reinstalling JP1/Base without uninstalling the JP1 product that requires JP1/Base.

Note: Do not start the JP1/Base service or other JP1 product service during the restore procedure.

And execute the following command to backup the common definition information of all JP1 products in case of performing incorrect procedure to restore the common definition information.

- Physical host:

```
jbsgetcnf > backup-file-name
```

- Logical host:

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

1. Back up JP1/Base.

For details on backups, see [3.5.3 Backup and recovery \(in UNIX\)](#).

If JP1/IM - Manager is installed, backup the command execution log (ISAM) file. For details about the backup of command execution log (ISAM) file, see the manual *JP1/Integrated Management 3 - Manager Administration Guide (Database backup and recovery)*.

Collect the log data before you perform the procedure to restore the common definition information in case the integrated trace log is deleted. For details on collecting log data, see [18.4 How to collect data](#).

2. Check the output destination of the common definition information backup file.

Check whether there is sufficient free disk space ($1 + 0.4 \times \text{number-of-logical-hosts}$ [MB] or more) for the output destination of the common definition information backup file (`\tmp\`). And check whether the common definition information backup file and output directory have not been locked by applications like editor. And also check for the access permission.

If there is insufficient free disk space, the common definition information backup file will not be output correctly. For example, the file size of the common definition information backup becomes 0 byte.

If directory or file has been locked by some application or if you do not have access permission, error message KAVA1871-E will be output during the uninstallation.

3. Set the following environment variables:

- # JP1_BASE_UNINST_FORCE=1
- # export JP1_BASE_UNINST_FORCE

4. Uninstall JP1/Base.

Uninstall JP1/Base as prompted by the Hitachi Program Product Installer by referring [3.3.3 Uninstalling JP1/Base](#).

Uninstallation can be performed even if the prerequisite products of JP1/Base are installed.

During the uninstallation, common definition information excluding JP1/Base is output as the common definition information backup file.

- Physical host: `/tmp/JP1_COMDEF/comdef_JP1_DEFAULT.conf`
- Logical host: `/tmp/JP1_COMDEF/comdef_logical-host-name.conf`

5. Clear the setting of the JP1_BASE_UNINST_FORCE environment variable.

6. Reinstall JP1/Base.

For details on install, see [3.3.1 Installing JP1/Base](#).

7. Re-set up JP1/Base.

If you are operating in a cluster, create a logical host.

The logical host name (Uppercase/Lowercase) and shared directory name cannot be changed.

Recover the adapter command configuration file (`/opt/jp1base/plugin/conf/*.conf`) from the backup in step 1.

If JP1/IM - Manager is installed, recover the command execution log (ISAM) file from the backup in step 1.

Recover the event database from the backup in step 1. For details on recovering the event database, see [3.5.3\(4\)\(a\) When the forwarding settings file is not configured to forward JP1 events to other hosts](#).

Build the JP1/Base environment.

- When recovering the JP1/Base environment:
Recover the JP1/Base other definition files, common definition information, and `jp1hosts2` information from the backup in step 1.
For details on recovery, see [3.5.3 \(3\) Recovering JP1/Base setup information](#).
- When rebuilding JP1/Base environment:

Perform JP1/Base setup again.

For details on setup, see [3.4 JP1/Base setup](#).

And also, perform other settings as necessary.

If you have set up JP1/Base in the setup of another product, set it up again.

8. Execute the `jbssetcnf` command using the common definition information backup file output in step 4.

Restore the common definitions for JP1 products excluding JP1/Base. Execute the command for the physical host and all logical hosts.

```
jbssetcnf common-definition-information-backup-file-name
```

9. Delete the common definition information backup file output directory in step 4.

Delete the common definition information backup file output directory (`\tmp\JP1_COMDEF\`).

(9) Enabling big timestamps when running Linux

You can continue using the Linux xfs file system in 2038 and beyond by enabling big timestamps[#]. This feature is disabled by default. See the manual for the OS in use to enable big timestamps by 03:14:07 (UTC) January 19, 2038 when running Linux.

#

This setting increases the data size of inode timestamps and quota expiration timestamps.

3.4 JP1/Base setup

3.4.1 Setting the language (for Windows)

If you install JP1/Base as a new installation, the language used in JP1/Base is set according to the locale set during installation (system locale). The following table lists the language that is set for each locale (system locale).

Table 3–3: Language set in JP1/Base for each locale (system locale)

Locale (system locale)	Language
Japanese	Japanese
Chinese	Chinese
Other than Japanese or Chinese	English

To change the locale (system locale) after installation, you must set the appropriate encoding. The following table lists languages and the corresponding encoding.

Table 3–4: Encodings in Windows

OS	Language	Encoding
Windows	Japanese	SJIS
	Chinese	GB18030
	English	C

(1) Procedure for setting the encoding

1. Edit `jp1bs_param.conf`.

Open the `installation-folder\conf\jp1bs_param.conf` file with a text editor. Then, for the *encoding* part of the `"LANG"="encoding"` entry, set the appropriate encoding as shown in Table 3-4.

2. Save the file, and then execute the following command by using a user account with administrator permissions:

```
installation-folder\bin\jbssetcnf installation-folder\conf\jp1bs_param.conf
```

3. Start or restart JP1/Base.

The new settings are applied when JP1/Base starts. If JP1/Base is running, restart it.

3.4.2 Setting the language (for UNIX)

The language used by JP1/Base is set in the `LANG` environment variable.

Keep the following in mind when setting the language used by JP1/Base:

- Use the same encoding as JP1/Base for products on the same host (such as JP1/IM and JP1/AJS) that use JP1/Base.
- When using JP1/Base in a UTF-8 locale, use one of the following setup scenarios system-wide:

- Upgrade all instances of JP1/Base to version 8 or later, and make sure that all products for which JP1/Base is a prerequisite are compatible with UTF-8 encoding.
- If there are computers in your system running version 7 of JP1/Base, JP1 events issued in UTF-8 locales cannot be processed correctly. Make sure that each instance of JP1/Base in a UTF-8 locale is version 8 or later, and configure JP1/Base to run in character code compatibility mode.
- Automatic startup and termination settings are specified according to the encoding that is set for the LANG environment variable during installation. However, if an encoding that is not shown in Table 3-5 is set, the LANG environment variable is set to C.
- In the following cases, you must specify Japanese as the language of the LANG environment variable in the automatic start script.
 - When Japanese is specified in the event filter of the forward settings file (`forward`)
 - When Japanese is specified in the `lpszFilter` parameter of the JP1 event acquisition function (`JevGetOpen`) in the user program
 - When Japanese is specified in various JP1/IM filters in JP1/IM[#]

[#]: For detailed conditions of servers that require language specification, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The following table shows the encodings available in each operating system, and the corresponding LANG value.

Table 3–5: Encodings and LANG environment variable values in UNIX

OS	Language	Encoding	Value of LANG
AIX	Japanese	SJIS	ja_JP.IBM-932 or Ja_JP
		EUCJIS	ja_JP.IBM-eucJP or ja_JP
		UTF-8	JA_JP.UTF-8, JA_JP, or ja_JP.UTF-8
	Chinese	GB18030	Zh_CN or Zh_CN.GB18030
		UTF-8 ^{#1}	ZH_CN or ZH_CN.UTF-8
	English	C	C
Linux	Japanese	SJIS ^{#2}	ja_JP.SJIS or ja_JP.sjis
		EUCJIS	Not used
		UTF-8	ja_JP.UTF-8 or ja_JP.utf8
	Chinese	GB18030	zh_CN.GB18030 or zh_CN.gb18030
		UTF-8	zh_CN.UTF-8 or zh_CN.utf8
	English	UTF-8 ^{#3}	en_US.UTF-8 or en_US.utf8
		C	C

^{#1}: This encoding is supported by only the log file trapping function. Log file trapping can be used to monitor UTF-8-encoded log data.

^{#2}: This encoding is valid in only SUSE Linux.

^{#3}: To apply the English UTF-8 encoding in Linux when upgrading from JP1/Base 13-00 or an earlier version, you must change the character code and language type mapping definition after the version upgrade installation is complete. For details, see (3) *Changing the character code and language type mapping definition after installing a version upgrade*.

(1) Setting the language for JP1/Base

1. Edit the `jplbs_env.conf` file.

Open the `/etc/opt/jplbase/conf/jplbs_env.conf` file in an editor, and set the value of the LANG environment variable with reference to [Table 3-5](#). The setting takes effect the next time JP1/Base starts.

2. Edit the `jplbs_param.conf` file.

For the *encoding* part of the "LANG"="*encoding*" entry, set the appropriate encoding as shown in [Table 3-5](#).

Open the `/etc/opt/jplbase/conf/jplbs_param.conf` file in an editor, and delete the line that starts with "JP1_BIND_ADDR". Then, for the character encoding to be specified "LANG"="*character encoding*", specify a character encoding listed in [Table 3-3](#).

3. Save the file, and then execute the following command as a superuser or a JP1/Base administrator:

```
/opt/jplbase/bin/jbssetcnf /etc/opt/jplbase/conf/jplbs_param.conf
```

4. Edit the automatic start script (`jbs_start`).

To use the automatic start script (`jbs_start`), set the LANG environment variable to the same language specified in `jplbs_env.conf` in step 1.

If you manually start an event service without using the automatic start script (`jbs_start`), locale information used when the event service is started (for example, the LANG environment variable) must match the language specified in `jplbs_env.conf`.

If, for example, you specify `ja_JP.UTF-8` as the language for `jplbs_env.conf`, change the LANG environment variable of the automatic startup script (`jbs_start`) as follows:

```
## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jplbase/bin
LANG=ja_JP.UTF-8
SHLIB_PATH=/opt/jplbase/lib:/opt/hitachi/common/lib
```

To run JP1/Base in a cluster system, similarly change the value of the LANG environment variable of `jbs_start.cluster` to match the language specified in `jplbs_env.conf` for the logical host.

5. Start or restart JP1/Base.

The new settings are applied when JP1/Base is started. If JP1/Base is running, restart it.

(2) Setting character code compatibility mode

1. Create the file `jbslm_setup.conf` by copying the model file (`jbslm_setup.conf.model`).

Location of `jbslm_setup.conf.model`:

```
/etc/opt/jplbase/conf/
```

Parameter:

The format of the parameter is as follows:

```
[JP1_DEFAULT\JP1BASE\  
"LANG_MODE"=dword:{00000000 | 00000001}
```

0: Do not use character code compatibility mode.

1: Use character code compatibility mode. The system converts characters from UTF-8 (Japanese) to EUC (Japanese) encoding.

On a logical host, replace `JP1_DEFAULT` with the logical host name.

2. Execute the `jbssetcnf` command.

For details on the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

3. Start or restart JP1/Base.

The new settings are applied when JP1/Base is started. If JP1/Base is running, restart it.

(3) Changing the character code and language type mapping definition after installing a version upgrade

The English UTF-8 encoding has been added to the Linux character code and language type mapping definition in JP1/Base 13-00.

When upgrading from an earlier version than JP1/Base 13-00, perform the procedure described below to apply the character code and language type mapping definition added with JP1/Base 13-00 after installing the upgrade in order to maintain the character code and language type mapping definitions set before upgrading.

1. Copy the model files (`eventenc.dat.model` and `eventlng.dat.model`) and create `eventenc.dat` and `eventlng.dat`.

Execute the following commands to change each definition file.

- Changing the character code mapping definition file

```
cp -p /opt/jplbase/lib/eventenc.dat.model /opt/jplbase/lib/eventenc.dat
```

- Changing the language type mapping definition file

```
cp -p /opt/jplbase/lib/eventlng.dat.model /opt/jplbase/lib/eventlng.dat
```

2. Start or restart the JP1/Base service, event service, and log-file trap management service.

Start each service to enable settings. If a service has already been started, restart the service.

3.4.3 Notes on running JP1 in a Chinese (Simplified) language environment

(1) Restrictions on GB18030 encoding

Chinese encoding supports GB18030-2000. The specifiable GB18030 encoding range differs according to the JP1/Base entry item.

No.	Entry item	GB18030 encoding range		
		1-byte (ASCII)	2-byte (GBK)	4-byte (Unicode)
1	Host name (physical host name, logical host name)	OK	--	--
2	Operating system account (domain name, user name)	OK	--	--
3	File pass	OK	--	..#1
4	Command line	OK	--	..#1

No.	Entry item	GB18030 encoding range		
		1-byte (ASCII)	2-byte (GBK)	4-byte (Unicode)
5	Definition name and value of common definition information	OK	--	--
6	Definition file description#2	OK	OK	OK
7	Monitoring target log content	OK	OK	OK
8	JP1 event attribute (message, extension attribute)	OK	OK	OK

Legend:

OK: The encoding is supported.

--: The encoding is not supported.

#1: If 4-byte encoding (Unicode) is specified, the characters are replaced with half-width question marks (?).

#2: The encoding range for the file path and command line described in the definition file is the same as the encoding range for entry items No.3 and No.4.

(2) Restrictions on Unicode

Only the range for the Basic Multilingual Plane is guaranteed for the encoding contained in Unicode(4-byte GB18030 and UTF-8) character strings.

If Unicode (4-byte GB18030 and UTF-8) character strings contain surrogate pairs, sometimes regular expressions might not produce the intended results.

(3) Notes on function specifications

(a) Event service

Regular expressions for the event filter

In Windows, extended regular expressions are applied. Use the syntax for the extended regular expressions.

In UNIX, the specified definitions for regular expressions are applied.

Registering JP1 events

- JP1 events are registered in UTF-8 encoding. "UTF-8" is specified for the basic attribute code set.
- There is a limit on the length of basic attribute messages (1023 bytes). If the message length exceeds the limit when it is converted to UTF-8 encoding, the excess portion is discarded. In this case, the KAJP1082-W message is output to the log.

`jevexport` command

- You can specify "GB18030" as the code set name specified for the `-l` option.
- If you specify "GB18030" for the `-l` option and then specify the `-a` option, English is output to the title line.

(b) Log file trap

Log files output in Chinese (Simplified) can be monitored in the same manner as for the existing functionality.

Regular expressions for the action definition file

In Windows, extended regular expressions are applied. Use the syntax for the extended regular expressions.

In UNIX, the specified definitions for regular expressions are applied.

Registering JP1 events

JP1 events are registered in UTF-8 encoding. "UTF-8" is specified for the basic attribute code set.

(c) Event log trap (Windows only)

Unicode-based monitoring can be performed in a Chinese (Simplified) language environment.

Regular expressions for the action definition file

Extended regular expressions are applied. Use the syntax for the extended regular expressions.

Registering JP1 events

JP1 events are registered in UTF-8 encoding. "UTF-8" is specified for the basic attribute code set.

(d) Local action

Regular expressions for the execution definition file

In Windows, extended regular expressions are applied. Use the syntax for the extended regular expressions.

In UNIX, the specified definitions for regular expressions are applied.

3.4.4 Adjusting the kernel parameters (UNIX only)

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.

3.4.5 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.

Initially, you can use the following regular expressions:

Table 3–6: Regular expressions available 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 (`nthevent.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 *JP1/Base Function Reference*.

In version 07-00 and later of JP1/Base, you can 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 3–7: Regular expressions available when extended

OS	Supported regular expressions
Windows	Complies with the syntax for XPG4 extended regular expressions.
UNIX	For AIX, 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 (<code>regexp</code> or <code>regex</code>).

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.

You can restore the default regular expressions using 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.
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 (or daemon) is started. Complies with the setting on the physical host.

3.4.6 Setting the password save format

You can improve password security by changing the format in which passwords are stored from hash level 1 to hash level 2. Note that, if you perform a new installation of JP1/Base version 12-00 or a later version, the format is set to hash level 2. However, if you perform an upgrade installation from version 11-50 or earlier to version 12-00 or later, and if the format is omitted from the common definition information, the format defaults to hash level 1. If you want to use the same password registered before the over write installation, use the same password save format. If you want to strengthen the password protection, follow the procedure to change password save format and change the password save format to hash level 2 mode. You do not need setting the password save format on any host other than the authentication server. Linked users who are authenticated by a directory server are not affected by this setting.

Note the following when changing the password save format:

- The accounts of JP1 users registered with an authentication server (except for users linked to a directory server) must be deleted and re-registered after you change the password save format. Until you do so, these users cannot undergo user authentication or change their passwords.
- The password save format must be the same on the primary authentication server and the secondary authentication server.
- If the password save format is hash level 2, any host other than an authentication server that issues a command to configure a JP1 user must be running version 10-00 or later of JP1/Base. If the `jbsadduser` command is executed from a host running version 09-00 or earlier, the message KAVA5023-E is output. If the `jbschgpasswd` command is executed, the message KAVA5223-E is output. In either case, the command terminates abnormally.

To change the format in which passwords are saved:

1. On the primary authentication server, create a definition file with the following contents.
You can choose any name for the file.

```
[JP1_DEFAULT\JP1BASE\  
"HASH_LEVEL"=dword:{00000001|00000002}
```

1: Operates in hash level 1 mode.

2: Operates in hash level 2 mode.

On a logical host, replace JP1_DEFAULT with the logical host name.

2. Execute the `jbssetcnf` command.

```
jbssetcnf definition-file-name
```

The contents of the new definition file are applied to the common definition information on the primary authentication server.

3. Start the primary authentication server.

4. Execute the `jbsrmuser` command.

Of the JP1 users registered on the authentication server, delete all JP1 users who are not linked to the directory server. You do not need to delete access permissions.

5. Re-register the JP1 users you deleted.

Re-register all the JP1 users you deleted in step 4.

6. Copy the settings from the primary authentication server to the secondary authentication server.

For details, see [8.1.4 Copying settings from the primary authentication server](#) or [8.3.4 Copying settings from the primary authentication server](#).

7. Create a definition file on the secondary authentication server.

You can choose any name for the file. Specify the parameter in the same format as step 1.

If the primary and secondary authentication servers are both physical hosts, you can simply copy the definition file you used in step 2 to the secondary authentication server. In all other scenarios, create separate definition files for the primary and secondary authentication servers.

8. Execute the `jbssetcnf` command.

```
jbssetcnf definition-file-name
```

The contents of the definition file you created in step 7 or the definition file you copied from the primary authentication server are applied to the common definition information on the secondary authentication server.

9. Start the secondary authentication server.

The password save format is changed.

3.4.7 Setting a password policy

This subsection describes how to set a password policy. When an attempt is made to register a JP1 user or to change a JP1 user's password, this password policy is used to check the set password. For details on the password policy, see [2.1.1\(3\) Password policy-based management](#).

The procedure below describes how to set a password policy.

(1) Common definition information

Setting a password policy means making changes to the common definition information. You must therefore first back up the common definition information before proceeding to set a password policy.

To back up common definition information, execute the following command to acquire only the common definition information for JP1/Base:

```
jbsgetcnf -c JP1BASE > backup-file
```

When you run JP1/Base in a cluster system, execute the following command to acquire only the common definition information for JP1/Base:

```
jbsgetcnf -h logical-host-name -c JP1BASE > backup-file
```

(2) Password policy settings

You can set a password policy on the primary authentication server as follows:

1. Edit the password policy definition file.

The `jp1bs_passwdpolc.conf` file is copied from the `jp1bs_passwdpolc.conf.model` file upon installation.

In Windows:

```
installation-folder\conf\passwdpolc\jp1bs_passwdpolc.conf
```

```
shared-folder\jp1base\conf\passwdpolc\jp1bs_passwdpolc.conf (applicable to cluster use)
```

In UNIX:

```
/etc/opt/jp1base/conf/passwdpolc/jp1bs_passwdpolc.conf
```

```
shared-directory/jp1base/conf/passwdpolc/jp1bs_passwdpolc.conf (applicable to cluster use)
```

Set values for the parameters in the password policy definition file. For details on the password policy definition file, see [Password policy definition file](#) in *16. Definition Files*.

Example of how to specify the `jp1bs_passwdpolc.conf` file

```
[JP1_DEFAULT\JP1BASE\PASSWDPOLC]
"ENABLE"=dword:0000001
"PASSWORD_LEN_MIN"=dword:00000010
"NUM_OF_CHAR_TYPE_MIN"=dword:00000003
"REQ_CHAR_TYPE"="NUM,UPPER,SYMBOL"
```

2. Execute the `jbssetcnf` command.

```
jbssetcnf Password-policy-definition-file
```

For details about the `jbssetcnf` command, see [jbssetcnf](#) in *15. Commands*.

3. Start or restart JP1/Base.

The new settings are applied when JP1/Base starts. If JP1/Base is running, restart it.

Because the secondary authentication server must have the same password policy as the primary authentication server, copy the set password policy definitions to the secondary authentication server.

Notes

- When a secondary authentication server is installed, it must have the same password policy definitions as the primary authentication server.
- If you change the password policy settings, you have to modify the originally registered passwords to make them compliant with the new password policy, as follows:
 1. Acquire a list of JP1 users (a list containing the date and time at which user data was last modified for each JP1 user (*yyyy/mm/dd HH:MM:SS* format)).
Confirm that the authentication server is up and running, and then execute the following command:

```
jbslistuser -ld
```
 2. Change the passwords of all JP1 users whose data was last modified prior to the setting of the new password policy.

3.4.8 Syslog output when SUSE Linux 15 or later is used

This manual assumes that the log information of UNIX OSs is output to syslog. However, if you are running SUSE Linux 15 or later, by default, log information is output to journals only, not to syslog (a text file).

If you want to output OS log information to syslog (as in normal cases), perform the following procedure so that the log information output to journals is transferred to syslog.

1. Install the rsyslog package.

```
rsyslog-8.33.1-x.xx.x86_64
```

2. Make sure that the setting for transferring information to syslog is enabled.

```
/etc/systemd/journald.conf
```

```
ForwardToSyslog=yes#
```

If the setting for transferring information to syslog is commented out, the default setting *yes* is applied.

3. Start rsyslog.

```
systemctl start rsyslog
```

3.5 Backup and recovery

Consider backup and recovery for JP1/Base in the context of a system-wide backup plan.

3.5.1 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.

Back up or recover JP1/Base while JP1/Base is not up and running.

When an upper-layer program backs up its data while JP1/Base is up and running, we recommend that the upper-layer program also back up the JP1/Base event database for error reporting purposes. JP1 events might be issued during the backup, and, depending on the event issuance timing, the upper-layer program might fail to reference event information, in which case the data is not correctly backed up. By backing up the event database for error reporting purposes, the upper-layer program can, after the recovery, check the status at the time when the data was backed up.

3.5.2 Backup and recovery (in Windows)

(1) Backing up JP1/Base setup information

JP1/Base setup information includes:

- Definition files
- Common definition information
- `jp1hosts2` 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 3–8: JP1/Base files to back up in Windows

File name	Contents
<i>JP1/Base-folder</i> ^{#1} \boot\JP1SVPRM.DAT	Start sequence definition file
<i>JP1/Base-folder</i> ^{#1} \boot\jp1svprm_wait.dat	Service starting delay time / timer monitoring period definition file ^{#2}
<i>JP1/Base-folder</i> ^{#1} \jp1bs_env.conf	JP1/Base environment settings file
<i>JP1/Base-folder</i> ^{#1} \jp1bs_param.conf <i>JP1/Base-folder</i> ^{#1} \jp1bs_param_v7.conf	JP1/Base parameter definition file
<i>JP1/Base-folder</i> ^{#1} \jp1bs_spmd.conf	JP1/Base process management definition file

File name	Contents
<i>JP1/Base-folder</i> ^{#1} \jplbs_service_0700.conf	Extended startup process definition file
Files in <i>JP1/Base-folder</i> ^{#1} \route\	Configuration definition file (used by JP1/IM)
<i>JP1/Base-folder</i> ^{#1} \user_acl\JP1_Passwd	JP1 user definition file
<i>JP1/Base-folder</i> ^{#1} \user_acl\JP1_Group	JP1 group definition file
<i>JP1/Base-folder</i> ^{#1} \user_acl\JP1_UserLevel	User permission level file
<i>JP1/Base-folder</i> ^{#1} \user_acl\JP1_AccessLevel	JP1 resource group definition file
<i>JP1/Base-folder</i> ^{#1} \user_acl\JP1_Accountaccess	JP1 account access information file
<i>JP1/Base-folder</i> ^{#1} \user_acl\jplBsUmap.conf	User mapping definition file
<i>JP1/Base-folder</i> ^{#1} \passwdpolc\jplbs_passwdpolc.conf	Password policy definition file
<i>JP1/Base-folder</i> ^{#1} \ds\jplbs_ds_setup.conf	Directory server linkage definition file
<i>installation-folder</i> \conf\event\index	Event server index file
<i>event-folder</i> ^{#3} \conf	Event server settings file
<i>event-folder</i> ^{#3} \forward	Forwarding settings file
<i>installation-folder</i> \suppress\forward_suppress	Forwarding settings file for event forwarding suppression
<i>event-folder</i> ^{#3} \[recv_add_extattr send_add_extattr]	Additional extended attribute settings file
<i>installation-folder</i> \conf\event\api	API settings file
<i>installation-folder</i> \conf\event\ntevent.conf	Action definition file for event log traps
<i>Any-file</i> ^{#4} or <i>installation-folder</i> \conf\jevlog.conf ^{#4}	Action definition file for log file trapping
<i>installation-folder</i> \conf\event\jevlog_start.conf	Log-file trap startup definition file
<i>JP1/Base-folder</i> ^{#1} \event\jevlogd.conf	Log information definition file
<i>event-folder</i> ^{#3} \[jev_forward.conf <i>any-file</i>] ^{#5}	Distribution definition file (for forward setting file)
<i>installation-folder</i> \conf\[jev_logtrap.conf <i>any-file</i>] ^{#5}	Distribution definition file (for action definition file for log file trapping)
<i>installation-folder</i> \conf\event\[jev_ntevent.conf <i>any-file</i>] ^{#5}	Distribution definition file (for action definition file for event log traps)
<i>installation-folder</i> \conf\event\[jev_logstart.conf. <i>any-file</i>] ^{#5}	Distribution definition file (for action definition file for log file trap startup)
<i>any-file</i>	Password definition file (Windows only)
<i>any-file</i>	Directory server modification file (Windows only)
<i>installation-folder</i> \plugin\conf*.conf	Adapter command settings file
<i>JP1/Base-folder</i> ^{#1} \jbshc\jbshc.conf	Health check definition file
<i>any-file</i>	Common definition settings file (health check function)

File name	Contents	
<i>JP1/Base-folder</i> #1\jplhosts	jplhosts definition file	
<i>JP1/Base-folder</i> #1\jplhosts2.conf	jplhosts2 definition file	
<i>JP1/Base-folder</i> #1\jbsdfts*.conf	Service management control definition file	
<i>any-file</i>	Local action environment variable file	
<i>JP1/Base-folder</i> #1\lact\jbslact.conf	Local action execution definition file	
<i>any-file</i>	Common definition settings file (local action function)	
<i>JP1/Base-folder</i> #1\physical_ipany.conf	Communication protocol settings file	
<i>JP1/Base-folder</i> #1\logical_ipany.conf		
<i>JP1/Base-folder</i> #1\physical_recovery_0651.conf		
<i>JP1/Base-folder</i> #1\logical_recovery_0651.conf		
<i>JP1/Base-folder</i> #1\physical_anyany.conf		
<i>JP1/Base-folder</i> #1\physical_ipip.conf		
<i>JP1/Base-folder</i> #1\logical_ipip.conf		
<i>JP1/Base-folder</i> #1\jplbs_base_log_setup.conf		Operation log definition file

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

- Physical host: *installation-folder*\conf
- Logical host: *shared-folder*\jplbase\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*\jplbase\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 the standard file name or a name of your choice. 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. To back up common definition information, execute the following command to acquire only the common definition information for JP1/Base:

```
jbsgetcnf -c JP1BASE > backup-file
```

When you run JP1/Base in a cluster system, execute the following command to acquire only the common definition information for JP1/Base:

```
jbsgetcnf -h logical-host-name -c JP1BASE > backup-file
```


Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

Important

When the logical host in question is used in a cluster system, execute the command on the primary node. The backed-up common definition information must be restored on both the primary server and the secondary server.

(c) Backing up jp1hosts2 information

Execute the following command to back up `jp1hosts2` information defined in your system.

```
jbshosts2export > backup-file
```

If you defined `jp1hosts2` information for a logical host, execute the command as follows:

```
jbshosts2export -h logical-host-name > backup-file
```

For a logical host in a cluster configuration, execute the command on the primary node.

(2) Backing up an event database

There are two modes of backing up event database files:

- Backup for data recovery
- Backup for error reporting purposes for later reference

(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 purposes for later reference

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 reaches the maximum size (10 megabytes 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.

If the event database is too large (1 GB or greater per file), it takes time to export all events by using the `jevexport` command. Furthermore, if the output csv file is too large, an attempt to reference it might fail.

The use of an event filter when backing up the event database on a regular basis allows you to back up only those events that occurred after the previous backup.

The following event filter backs up JP1 events that have occurred during the past two days:

```
B.TIME WITHIN D 2
```

Shown below is an example of the `jevexport` command execution result when an event filter file in which the above-mentioned event filter is specified is used. When you specify `ON` for the `-t` option, the event filter specified in `filter.txt` is applied, and the registration times and arrival times of JP1 events are output in Western calendar notation.

```
jevexport -t ON -f filter.txt -o backup-file
```

For details about the `jevexport` command, see *jevexport* in *15. Commands*.

(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.

To recover common definition information on a set-up host, execute the following command to temporarily delete the common definition information for JP1/Base.

Physical host:

```
jbsunsetcnf -i -h JP1_DEFAULT -c JP1BASE
```

Logical host:

```
jbsunsetcnf -i -h logical-host-name -c JP1BASE
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

Execute the following command:

```
jbssetcnf name-of-backup-file-backed-up-in-(1) (b)
```

Important

If the logical host in question is used in a cluster system, execute the command on both the primary node and the secondary node. The backed-up common definition information must be restored on both the primary server and the secondary server.

(c) Recovering jp1hosts2 information

If you backed up `jp1hosts2` information by following the procedure in (1)(c) *jp1hosts2 information*, execute the following command to recover the information:

```
jbshosts2import -r name-of-backup-file-backed-up-in-section-(1) (c)
```

If you backed up `jp1hosts2` information for a logical host, execute the command as follows:

```
jbshosts2import -h logical-host-name -r name-of-backup-file-backed-up-in-section-(1)-(c)
```

For a logical host in a cluster environment, execute the command on the primary node.

(4) Recovering the event database

When you recover the event database from a backup, the highest serial number recorded in the database will be the highest number at the time the backup was taken.

Event servers that receive forwarded JP1 events (typically environments where JP1/IM Manager is installed) keep a record of the highest serial number in the event database from which the event was forwarded. The event server uses this information as the basis for a duplication registration check. As long as the serial number of a new JP1 event is greater than the highest on record, the event server considers the event to be original and registers it without conducting any further checks. However, if a lower serial number is reported, the event server searches the database for the same JP1 event to rule out the possibility that the forwarded event is a duplicate. A larger event database means more information to search, which can cause delays when forwarding events and in features that use the event service.

(a) When the forwarding settings file is not configured to forward JP1 events to other hosts

1. Stop all products that use JP1/Base.

2. Stop JP1/Base.
3. Move the backed-up files.

Move the files to the following folder:

```
installation-folder\sys\event\servers\default\#
```

or

```
shared-folder\jplbase\event\#
```

#: If you specified a different location to be used by the event server in the event server index file (`index`), place the files in that location.

4. Start JP1/Base.
5. Start the products that use JP1/Base.

(b) When the forwarding settings file is configured to forward JP1 events to other hosts

If the forwarding target is JP1/Base 11-10 or later and the duplication prevention table is in the file format, recover the event database with the following procedure:

1. Stop all products that use JP1/Base.
2. Stop JP1/Base.

3. Move the backed-up files.

Move the files to the following folder:

```
installation-folder\sys\event\servers\default\#
```

or

```
shared-folder\jplbase\event\#
```

#: If you specified a different location to be used by the event server in the event server index file (`index`), place the files in that location.

4. Start JP1/Base.
5. Send a JP1 event for clearing the duplication prevention table (user event) to the forwarding target to clear the maximum value for the source event database serial number of the forwarding source from the forwarding target's duplication prevention table.

```
> jevsendd -i 7FFF8001 -m "DPT CLEAR EVENT" -d target-event-server-name
```

If the forwarding target is a sub manager of JP1/IM - Manager, also send to its higher manager a JP1 event for clearing the duplication prevention table (user event).

6. Start the products that use JP1/Base.

If the forwarding target is a JP1/Base version earlier than 11-10 or the duplication prevention table is in the memory format, recover the event database with one of the following procedures:

- Initialize the event database.

Initialize the event database as described in *10.2.2 Initializing an event database while the event service is stopped*. You can view the contents of a backed-up event database by using the `jvexport` command to output the contents to a CSV file.

- Disable duplication registration checking on the event servers specified as forwarding destinations in the forwarding settings file.

Perform the following tasks on the forwarding destination:

1. Stop all products that use JP1/Base.
2. Stop JP1/Base.
3. Add the following line to the event server settings file (`conf`):
`repetition-noncheck-server event-server-to-be-recovered`
4. Start JP1/Base.
5. Start the products that use JP1/Base.

Perform the following task on the forwarding source:

Recover the database by following the procedure in *(a) When the forwarding settings file is not configured to forward JP1 events to other hosts*.

When the forwarding target first receives a forwarded JP1 event, the event service resets the highest serial number recorded for the forwarding source. You can then re-enable duplication registration checking on the destination event server if you choose. Enable duplication registration checking on the target event server and re-create the duplication prevention table by executing the `jvdbmkrep` command before you start the event server.

3.5.3 Backup and recovery (in UNIX)

(1) Backing up JP1/Base setup information

JP1/Base setup information includes:

- Definition files
- Common definition information
- `jplhosts2` 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 `cpio` command, or a more advanced backup command to back up these files. Choose any backup method.

Table 3–9: JP1/Base files to back up in UNIX

File names	Contents
<code>JP1/Base-directory^{#1}/jplbs_env.conf</code>	JP1/Base environment settings file
<code>JP1/Base-directory^{#1}/jplbs_param.conf</code> <code>JP1/Base-directory^{#1}/jplbs_param_v7.conf</code>	JP1/Base parameter definition file
<code>JP1/Base-directory^{#1}/jplbs_spmd.conf</code>	JP1/Base process management definition file

File names	Contents
<i>JP1/Base-directory</i> ^{#1} / <i>jplbs_service_0700.conf</i>	Extended startup process definition file
Files in <i>JP1/Base-directory</i> ^{#1} / <i>route/</i>	Configuration definition file (used by JP1/IM)
<i>JP1/Base-directory</i> ^{#1} / <i>user_acl/JP1_Passwd</i>	JP1 user definition file
<i>JP1/Base-directory</i> ^{#1} / <i>user_acl/JP1_Group</i>	JP1 group definition file
<i>JP1/Base-directory</i> ^{#1} / <i>user_acl/JP1_UserLevel</i>	User permission level file
<i>JP1/Base-directory</i> ^{#1} / <i>user_acl/JP1_AccessLevel</i>	JP1 resource group definition file
<i>JP1/Base-directory</i> ^{#1} / <i>user_acl/JP1_Accountaccess</i>	JP1 account access information file
<i>JP1/Base-directory</i> ^{#1} / <i>user_acl/jplBsUmap.conf</i>	User mapping definition file
<i>JP1/Base-directory</i> ^{#1} / <i>passwdpolc/jplbs_passwdpolc.conf</i>	Password policy definition file
<i>JP1/Base-directory</i> ^{#1} / <i>event/index</i>	Event server index file
<i>event-directory</i> ^{#4} / <i>conf</i>	Event server settings file
<i>event-directory</i> ^{#4} / <i>forward</i>	Forwarding settings file
<i>/etc/opt/jplbase/conf/event/servers/default/suppress/forward_suppress</i>	Forwarding settings file for event forwarding suppression
<i>event-directory</i> ^{#4} / <i>[recv_add_extattr send_add_extattr]</i>	Additional extended attribute settings file
<i>/etc/opt/jplbase/conf/event/api</i>	API settings file
<i>Any-file</i> ^{#2} or <i>/etc/opt/jplbase/conf/jevlog.conf</i> ^{#2}	Action definition file for log file trapping
<i>/etc/opt/jplbase/conf/event/jevlog_start.conf</i>	Log-file trap startup definition file
<i>JP1/Base-directory</i> ^{#1} / <i>event/jevlogd.conf</i>	Log information definition file
<i>event-directory</i> ^{#4} / <i>[jev_forward.conf any-file]</i> ^{#3}	Distribution definition file (for forward setting file)
<i>/etc/opt/jplbase/conf/[jev_logtrap.conf any-file]</i> ^{#3}	Distribution definition file (for action definition file for log file trapping)
<i>/etc/opt/jplbase/conf/event/[jev_ntevent.conf any-file]</i> ^{#3}	Distribution definition file (for action definition file for event log traps)
<i>/etc/opt/jplbase/conf/event/[jev_logstart.conf any-file]</i> ^{#3}	Distribution definition file (for action definition file for log file trap startup)
<i>/opt/jplbase/plugin/conf/*.conf</i>	Adapter command settings file
<i>JP1/Base-directory</i> ^{#1} / <i>jbshc/jbshc.conf</i>	Health check definition file
<i>any-file</i>	Common definition settings file (health check function)
<i>JP1/Base-directory</i> ^{#1} / <i>jplhosts</i>	<i>jplhosts</i> definition file
<i>JP1/Base-directory</i> ^{#1} / <i>jplhosts2.conf</i>	<i>jplhosts2</i> definition file
<i>JP1/Base-directory</i> ^{#1} / <i>jbsdfts/*.conf</i>	Service management control definition file

File names	Contents	
<i>any-file</i>	Local action environment variable file	
<i>JP1/Base-directory</i> ^{#1} / <i>lcact/jbslcact.conf</i>	Local action execution definition file	
<i>any-file</i>	Common definition settings file (local action function)	
<i>JP1/Base-directory</i> ^{#1} / <i>physical_ipany.conf</i>	Communication protocol settings file	
<i>JP1/Base-directory</i> ^{#1} / <i>logical_ipany.conf</i>		
<i>JP1/Base-directory</i> ^{#1} / <i>physical_recovery_0651.conf</i>		
<i>JP1/Base-directory</i> ^{#1} / <i>logical_recovery_0651.conf</i>		
<i>JP1/Base-directory</i> ^{#1} / <i>physical_anyany.conf</i>		
<i>JP1/Base-directory</i> ^{#1} / <i>physical_ipip.conf</i>		
<i>JP1/Base-directory</i> ^{#1} / <i>logical_ipip.conf</i>		
<i>JP1/Base-directory</i> ^{#1} / <i>jplbs_base_log_setup.conf</i>		Operation log definition file

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

- Physical host: */etc/opt/jplbase/conf*
- Logical host: *shared-directory/jplbase/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 the standard file name or a name of your choice. 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/jplbase/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.

To back up common definition information, execute the following command to acquire only the common definition information for JP1/Base:

```
jbsgetcnf -c JP1BASE > backup-file
```

When you run JP1/Base in a cluster system, execute the following command to acquire only the common definition information for JP1/Base:

```
jbsgetcnf -h logical-host-name -c JP1BASE > backup-file
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

Important

When the logical host in question is used in a cluster system, execute the command on the primary node. The backed-up common definition information must be restored on both the primary server and the secondary server.

(c) Backing up jp1hosts2 information

Execute the following command to back up `jp1hosts2` information defined in your system.

```
jbshosts2export > backup-file
```

If you defined `jp1hosts2` information for a logical host, execute the command as follows:

```
jbshosts2export -h logical-host-name > backup-file
```

For a logical host in a cluster configuration, execute the command on the primary node.

(2) Backing up an event database

There are two modes of backing up event database files:

- Backup for data recovery
- Backup for error reporting purposes for later reference

(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 purposes for later reference

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 reaches the maximum size (10 megabytes 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.

If the event database is too large (1 GB or greater per file), it takes time to export all events by using the `jevexport` command. Furthermore, if the output csv file is too large, an attempt to reference it might fail.

The use of an event filter when backing up the event database on a regular basis allows you to back up only those events that occurred after the previous backup.

The following event filter backs up JP1 events that have occurred during the past two days:

```
B.TIME WITHIN D 2
```

Shown below is an example of the `jevexport` command execution result when an event filter file in which the above-mentioned event filter is specified is used. When you specify `ON` for the `-t` option, the event filter specified in `filter.txt` is applied, and the registration times and arrival times of JP1 events are output in Western calendar notation.

```
jevexport -t ON -f filter.txt -o backup-file
```

For details about the `jevexport` command, see [jevexport](#) in *15. Commands*.

(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.

To recover common definition information on a set-up host, execute the following command to temporarily delete the common definition information for JP1/Base.

Physical host:

```
jbsunsetcnf -i -h JP1_DEFAULT -c JP1BASE
```

Logical host:

```
jbsunsetcnf -i -h logical-host-name -c JP1BASE
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

Execute the following command:

```
jbssetcnf name-of-backup-file-backed-up-in-(1)(b)
```

Important

If the logical host in question is used in a cluster system, execute the command on both the primary node and the secondary node. The backed-up common definition information must be restored on both the primary server and the secondary server.

(c) Recovering jp1hosts2 information

Execute the following command to recover `jp1hosts2` information backed up using the procedure in (1)(c) *Backing up jp1hosts2 information*:

```
jbshosts2import -r name-of-backup-file-backed-up-in-section-(1)-(c)
```

If you backed up `jp1hosts2` information for a logical host, execute the command as follows:

```
jbshosts2import -h logical-host-name -r name-of-backup-file-backed-up-in-section-(1)-(c)
```

For a logical host in a cluster environment, execute the command on the primary node.

(4) Recovering an event database

When you recover the event database from a backup, the highest serial number in the database will be the highest number at the time backup was taken.

Event servers that receive forwarded JP1 events (typically environments where JP1/IM Manager is installed) keep a record of the highest serial number in the event database from which the event was forwarded. The event server uses this information as the basis for a duplication registration check. As long as the serial number of a new JP1 event is greater than the highest on record, the event server considers the event to be original and registers it without conducting any further checks. However, if a lower serial number is reported, the event server searches the database for the same JP1 event to rule out the possibility that the forwarded event is a duplicate. A larger event database means more information to search, which can cause delays when forwarding events and in features that use the event service.

(a) When the forwarding settings file is not configured to forward JP1 events to other hosts

1. Stop all products that use JP1/Base.

2. Stop JP1/Base.
3. Move the backed-up files.

Move the files to the following directory:

```
/var/opt/jplbase/sys/event/servers/default/#
```

or

```
shared-directory/event/#
```

#: If you specified a different location to be used by the event server in the event server index file (`index`), place the files in that location.

4. Start JP1/Base.
5. Start the products that use JP1/Base.

(b) When the forwarding settings file is configured to forward JP1 events to other hosts

If the forwarding target is JP1/Base 11-10 or later and the duplication prevention table is in the file format, recover the event database with the following procedure:

1. Stop all products that use JP1/Base.
2. Stop JP1/Base.

3. Move the backed-up files.

Move the file to the following directory:

```
/var/opt/jplbase/sys/event/servers/default/#
```

or

```
shared-directory/event/#
```

#: If you specified a different location to be used by the event server in the event server index file (`index`), place the files in that location.

4. Start JP1/Base.
5. Send a JP1 event for clearing the duplication prevention table (user event) to the forwarding target to clear the maximum value for the source event database serial number of the forwarding source from the forwarding target's duplication prevention table.

```
> jevsendd -i 7FFF8001 -m "DPT CLEAR EVENT" -d target-event-server-name
```

If the forwarding target is a sub manager of JP1/IM - Manager, also send to its higher manager a JP1 event for clearing the duplication prevention table (user event).

6. Start the products that use JP1/Base.

If the forwarding target is a JP1/Base version earlier than 11-10 or the duplication prevention table is in the memory format, recover the event database with one of the following procedures:

- Initialize the event database.

Initialize the event database as described in *10.2.2 Initializing an event database while the event service is stopped*. You can view the contents of a backed-up event database by using the `jvexport` command to output them to a CSV file.

- Disable duplication registration checking on the event servers specified as forwarding destinations in the forwarding settings file.

Perform the following tasks on the forwarding destination:

1. Stop all products that use JP1/Base.
2. Stop JP1/Base.
3. Add the following line to the event server settings file (`conf`):
`repetition-noncheck-server event-server-to-be-recovered`
4. Start JP1/Base.
5. Start the products that use JP1/Base.

Perform the following task on the forwarding source:

Recover the database by following the procedure in *(a) When the forwarding settings file is not configured to forward JP1 events to other hosts* above.

When the forwarding target first receives a forwarded JP1 event, the event service resets the highest serial number recorded for the forwarding source. You can then re-enable duplication registration checking on the destination event server if you choose. Enable duplication registration checking on the target event server and re-create the duplication prevention table by executing the `jvdbmcrep` command before you start the event server.

4

Setup for Handling Possible Errors in JP1/Base

This chapter describes setups for handling possible errors in JP1/Base.

4.1 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:

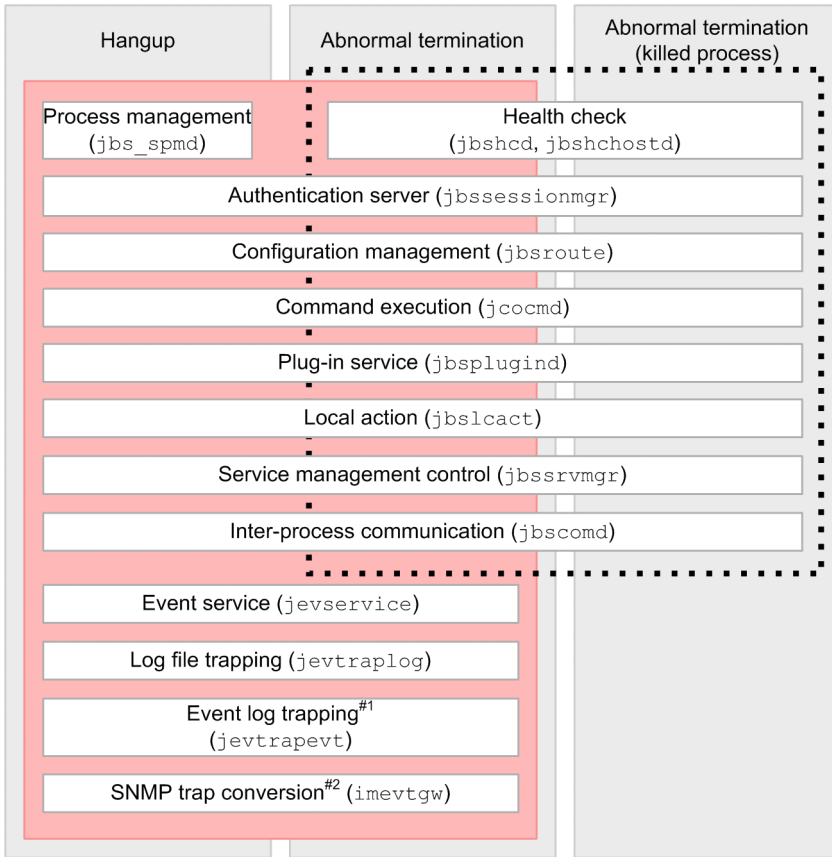
- Health check
The function can detect hangups (infinite loops or deadlocks) or abnormal termination (other than forced termination) of processes such as process management, the event service, and event conversion.
- Detection of errors by the process management function
The service can detect abnormal 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.
- Hitachi Network Objectplaza Trace Library (HNTRLib2)
JP1/Base uses the Hitachi Network Objectplaza Trace Library (HNTRLib2) to output log files that trace the system processing invoked in JP1/Base and in program products for which JP1/Base is a prerequisite program.
- Data collection when a problem occurs
Troubleshooting information can be collected when a problem occurs in JP1/Base.
- Threshold-based suppression of event forwarding
By setting a threshold to detect large numbers of events, you can automatically suppress forwarding of the events when large numbers of JP1 events occur.

4.1.1 Range of process errors that can be detected by the health check and process management functions

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 4–1: Range of process errors that can be detected by the health check and process management functions



Legend:

: Errors detected by health check function

: Errors detected by process management function

#1: Supported in Windows only.

#2: Linked with NNM version 8 or earlier.

4.2 Using health check function to detect process errors

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.

4.2.1 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. The settings of the health check function are registered in the common definition information.

For details on the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

For details on the common definition settings file (health check function), see *Common definition settings file (health check function)* in 16. *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 16. *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 16. *Definition Files*.

4. Restart all JP1/Base services.

The health check function starts and process monitoring begins.

If the health check action definition file contains an error, the line that contains the error is ignored. If that line contains a value that can be assumed to replace the ignored value, the function works by assuming that value.

(1) Upgrading from a cluster system environment with JP1/Base version 07-00 or earlier

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. The settings to enable the health check function must be performed after upgrading the logical host environment settings.

For details on the upgrade procedure, see [3.2.3\(5\) Overwrite installation](#) (for Windows) or [3.3.4\(5\) Overwrite installation](#) (for UNIX).

4.2.2 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 *15. Commands*. For details on the common definition information, see [Common definition settings file \(health check function\)](#) in *16. Definition Files*.

4.2.3 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 *16. Definition Files*.

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

Restart JP1/Base, or execute the `jbs_spmd_reload` command. For details on the `jbs_spmd_reload` command, see [jbs_spmd_reload](#) in *15. 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.

4.2.4 Disabling the health check settings

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 *16. 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 15. *Commands*.

3. Restart all JP1/Base services.

4.2.5 Notes on 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.

4.3 Detecting abnormal 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 *17. JP1 Events*.

4.3.1 Monitored processes

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

- `jbsessionmgr` (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)
- `jbsrvmgr` (service management control)
- `jbslcact` (local action)
- `jbscomd` (inter-process communication)

4.3.2 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

4.3.3 Setup process for detecting abnormal process termination and switching of the authentication server

To set up this functionality:

1. Edit the JP1/Base parameter definition file (`jp1bs_param_v7.conf`).

Specify 1 (issue JP1 event) for the parameter for which you want to issue JP1 events. For details on the JP1/Base parameter definition file, see *JP1/Base parameter definition file* in *16. 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 *15. Commands*.

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

The settings are applied.

4.4 Restarting abnormally terminated processes managed by the process management function

Starting JP1/Base causes multiple processes to be generated. In JP1/Base, if these processes terminate abnormally for some reason, they can automatically restart.

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.

4.4.1 Target processes

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

- `jbsessionmgr` (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)
- `jbsrvmgr` (service management control)
- `jbslcact` (local action)
- `jbscomd` (inter-process communication)

4.4.2 Setup procedure for restarting processes managed by the process management function

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 16. *Definition Files*.

2. Enable the setting.

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

4.5 Restarting an abnormally terminated event service process (UNIX only)

In the UNIX version of JP1/Base, an event service process that terminates abnormally on the physical host can be set to restart automatically. This feature 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.

4.5.1 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.

4.5.2 Setup procedure for restarting an abnormally terminated event service process

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 *16. Definition Files*.

4.6 Setting 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 default settings are as follows:

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

In Windows

```
system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2*.log
```

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

In UNIX:

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

Although there is usually no need to change these settings, you can view and change the default settings by executing the `hntr2utl2`, `hntr2conf`, or `hntr2getconf` command. For details on the commands, see *hntr2utl2 (Windows only)*, *hntr2utl2 (UNIX only)*, *hntr2conf*, *hntr2getconf* in *15. Commands*.

A message might be broken if the integrated trace log data is output from multiple processes at the same time. Therefore, enable the exclusive integrated trace log function to monitor a specific message by using the log file trap definition file. For details on exclusive functions, see *hntr2conf* in *15. Commands*.

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

JP1/Base provides the *data collection tool*, which allows you to collect data when a problem occurs. The tool can collect data such as OS system information and JP1/Base settings. Note, however, that the tool cannot collect user dumps. Therefore, if a problem occurs, you must collect user dumps in addition to the data collected by the data collection tool.

This section describes the settings for outputting user dumps.

4.7.1 Setting up user dump output

Use the following procedure to specify in the registry the settings for outputting user dumps. Great care should be taken because registry operation might affect the entire machine.

1. From the **Start** menu, enter `regedit` in the **Search programs and files** field, and then press Enter.

If the User Account Control window is displayed, click the **Yes** button.

2. In the tree on the left side of the window, expand the following key:

Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting`

3. Right click on the `Windows Error Reporting` key, and select **New**, and then select **Key**.

4. Enter `LocalDumps` in the new key.

5. Select the created `LocalDumps` key, and then create the following three registries:

No.	Name of the value	Type of the value	Data
1	<code>DumpFolder</code>	Expandable string (REG_EXPAND_SZ)	Desired dump output path (Example) <code>c:\dump</code>
2	<code>DumpCount</code>	DWORD (32-bit) value (REG_DWORD)	a (hexadecimal)
3	<code>DumpType</code>	DWORD (32-bit) value (REG_DWORD)	2 (hexadecimal)

4.8 Setting a threshold to detect large numbers of events

By setting a threshold to detect large numbers of events, you can automatically suppress forwarding of the events when large numbers of JP1 events occur. Please consider setting a threshold to detect large numbers of events, so as to prevent large numbers of events from being forwarded.

The threshold to detect large numbers of events is set in the forwarding setting file (`forward`) on the suppressed agent as conditions for the suppression of event-forwarding. For details on how to set conditions for the suppression of event-forwarding, see *10.1.9(1) Setting up the conditions for the suppression of event-forwarding*.

4.9 Function for automatically re-organizing the command execution log file

If an unexpected forced system termination or a power outage occurs while command execution logs are being written into the command execution log file that is used by the JP1/Base command execution function, the command execution log file might become corrupted.

The function for automatically re-organizing the command execution log file enables you to repair the command execution log file or detect file corruption at an early stage when you restart JP1/Base after an unexpected forced system termination. The initial setting is that this function is enabled.

The amount of time required for JP1/Base startup might increase depending on the size of the command execution log file. If the amount of startup time becomes an operation issue, consider either decreasing the number of records in the command execution log file or disabling the automatic re-organization function.

The amount of time required for automatically re-organizing the command execution log file can be estimated based on the sum of the amounts of the execution time of the commands below. Execution time becomes longer in proportion to the file size.

Command execution example

Stop JP1/Base before executing the following commands.

For Windows:

```
Jiscond installation-folder\log\COMMAND\ACTISAMLOGV8  
Jiscond installation-folder\log\COMMAND\CMDISAMLOGV8
```

For UNIX:

```
/opt/jplbase/bin/Jiscond /var/opt/jplbase/log/COMMAND/actisamlogv8  
/opt/jplbase/bin/Jiscond /var/opt/jplbase/log/COMMAND/cmdisamlogv8
```

The procedure for disabling this function is as follows:

1. Rename or delete `jplbs_spmd_pre.conf`.#
2. Restart JP1/Base and all products that use JP1/Base.

The function is disabled.

#

`jplbs_spmd_pre.conf` is stored in the following directory:

In Windows:

```
installation-folder\conf\  
shared-folder\jplbase\conf\ (applicable to cluster use)
```

In UNIX:

```
/etc/opt/jplbase/conf/  
shared-directory/jplbase/conf/ (applicable to cluster use)
```

Note:

On Windows, a locked file or record in the ISAM database may remain locked when a service ends abnormally. Unlock the file or record using the `Jislckfree` command.

5

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.

5.1 Overview of using JP1/Base in a cluster system

5.1.1 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.

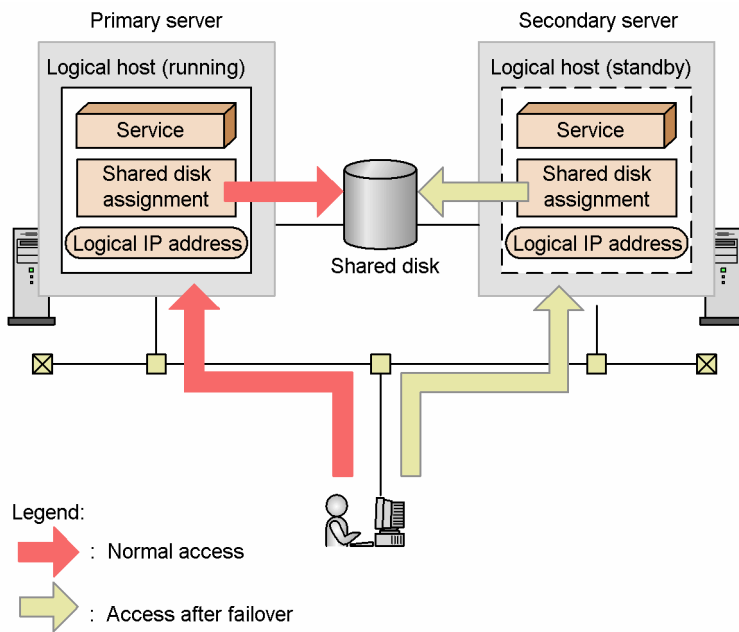
The following table shows the components of a logical host.

Table 5–1: 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 5–1: 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.

5.1.2 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.

5.2 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.

5.2.1 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 5–2: Prerequisites for a logical host environment

Logical host component	Prerequisites
Shared disk	<ul style="list-style-type: none">• 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.• Use storage connected via SCSI or SAN (Fibre) as the shared disk for JP1/Base. Do not use network connection disks (NFS, NAS, and others) as the shared disk. As performance varies depending on the disk, carry out investigations in advance.
Logical IP address	<ul style="list-style-type: none">• 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.

5.2.2 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 5–3: Prerequisites for a physical host environment

Physical host component	Prerequisites
Server	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.
Network	<ul style="list-style-type: none"> • Communication must be enabled using an IP address corresponding to the host name (result of the <code>hostname</code> 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.)
OS and clustering software	<ul style="list-style-type: none"> • 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.

5.2.3 Specifying a logical host

As a prerequisite for executing commands on a logical host, you must specify the logical host name. If you do not specify a logical host name, commands will be executed on physical hosts.

(1) Specifying a logical 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
<code>JP1_HOSTNAME</code> environment variable	Specify the logical host name in the <code>JP1_HOSTNAME</code> 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.
Command option	Specify the command option in the following format: <code>command -h logical-host-name</code> . 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.

(2) 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 32 bytes or less. You cannot specify a logical host name that is 33 bytes or more.

(3) Notes on logical host names

- 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 default event server index file (`index`). 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.

Note that, if you modify the event server index file (`index`), modify it while the event server instances on the physical hosts are stopped.

- Apply the contents of `jevlogical_setup.conf` to the common definition.

To allow JP1/Base to recognize an event service on a logical host that has the same name as the event service on the physical host, apply the contents of the `jevlogical_setup.conf` file to the common definition information.

In Windows:

```
jbssetcnf jevlogical_setup.conf#
```

In UNIX:

```
/opt/jp1base/bin/jbssetcnf jevlogical_setup.conf#
```

#: Use a full path if the JP1/Base `bin` folder is not specified in the `PATH` environment variable.

To undo these changes:

In Windows:

1. Create a definition file with the following contents.

You can choose any name for the definition file.

```
[JP1_DEFAULT\JP1BASE\  
"JEVSERVICE_LOGICAL"=dword:00000000
```


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\]
```

```
"JEVSERVICE_LOGICAL"=dword:00000000
```

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 *15. 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 32 bytes of the logical host name uniquely identify the host within the cluster system. This command determines the host by using the first 32 bytes and forcibly terminates the associated process. You cannot kill a process for a logical host name that is 33 bytes or more.

5.2.4 The scope 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 on the control over the clustering software.

If the prerequisites for a logical or physical host environment described above are not satisfied or if there is a problem in controlling the logical host environment, JP1 does not address 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.

5.3 Functions of JP1/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.

5.3.1 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.

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. If you execute the `jevlogstart` command without the `-s` option, JP1 events will be registered with the event service on the physical host.

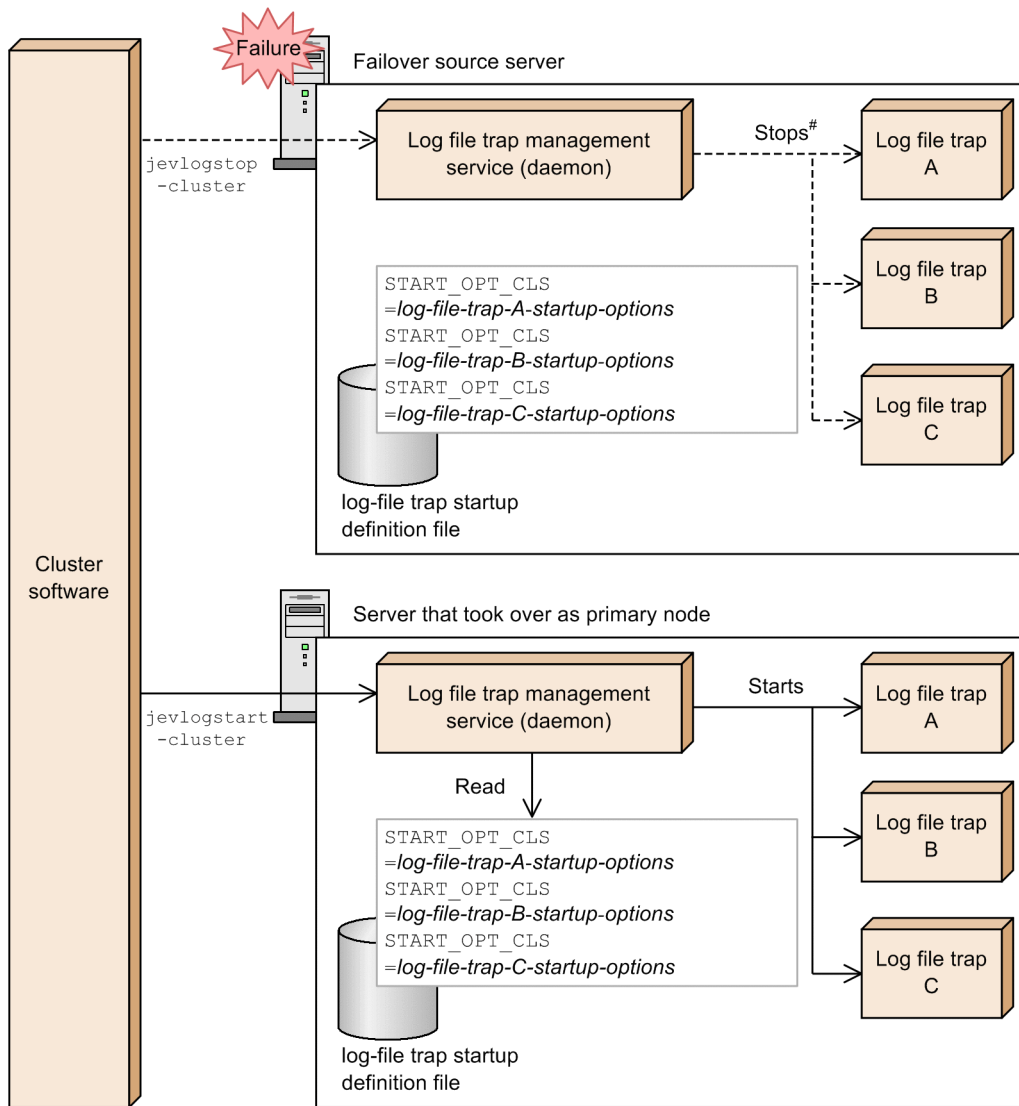
The following describes how to monitor log files on shared and local disks.

(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.

By using a log-file trap startup definition file, you can collectively stop and restart log file traps in the event of a failover. The following figure shows how the system stops and restarts log file traps as a batch:

Figure 5–2: Collectively stopping and starting log file traps



Legend:

- > : Flow of stopping log file trap
- > : Flow of starting log file trap

#: Stops log file traps started by the `jevlogstart -cluster` command.

To stop and restart log file traps as a batch, specify the log file traps that you want to stop and restart in a log-file trap startup definition file. You can then configure the cluster software to execute the `jevlogstop` and `jevlogstart` commands with the `-cluster` option in the event of a failover. When a failover occurs and the `jevlogstart -cluster` command is executed, the server that has taken over as the primary node reads the log-file trap startup definition file and starts the log file traps specified in the file. When the `jevlogstop -cluster` command is executed, JP1/Base stops the log file traps that were started by the `jevlogstart -cluster` command on the failed host.

If you use a log-file trap startup definition file, check whether the required log file traps have started by viewing the startup record (KAVA3661-I) and startup results (KAVA3662-I) output to the log-file trap startup execution results log.

To configure log file traps to start and stop collectively when a failover occurs:

1. Edit the log-file trap startup definition file.

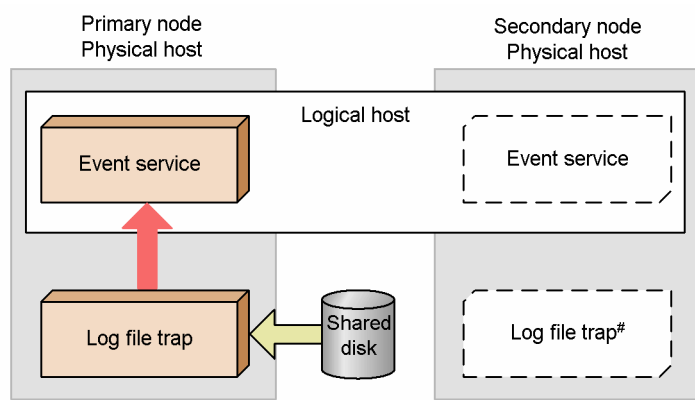
In the `START_OPT_CLS` parameter of the log-file trap startup definition file on the primary and secondary nodes, specify the log file traps that you want to stop and restart automatically when a failover occurs. Specify the `START_OPT_CLS` parameter in the same way on the primary and secondary nodes. In an environment that incorporates multiple cluster systems, specify the log file traps to be started and stopped for each system. For details on the log-file trap startup definition file, see *Log-file trap startup definition file* in 16. *Definition Files*.

2. Register the `jevlogstop` and `jevlogstart` commands (both for cluster environments only) with the cluster software.
For details on these commands, see *jevlogstop (cluster environment only)* and *jevlogstart (cluster environment only)* in 15. *Commands*.

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 5–3: Configuration example for monitoring log files on a shared disk



Legend:
 : Flow of JP1 events
 : Data flow
 : On standby

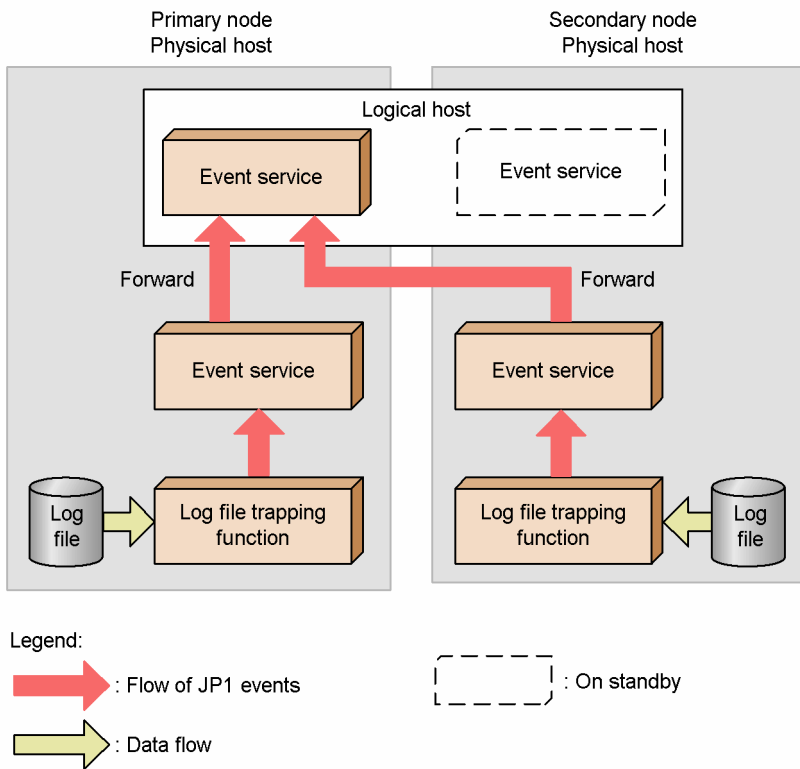
When a failover occurs, stop the log file trap on the failed server, and then restart it on the server that has taken over as the active system.

(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. Also, use the forwarding settings file (`forward`) to perform settings to forward to the event service on a separate host as necessary. For details on the forwarding settings file, see *Forwarding settings file* in 16. *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 5–4: Configuration example for monitoring, on a logical host, log files on local disks



5.3.2 Cluster operation with the event log trapping function

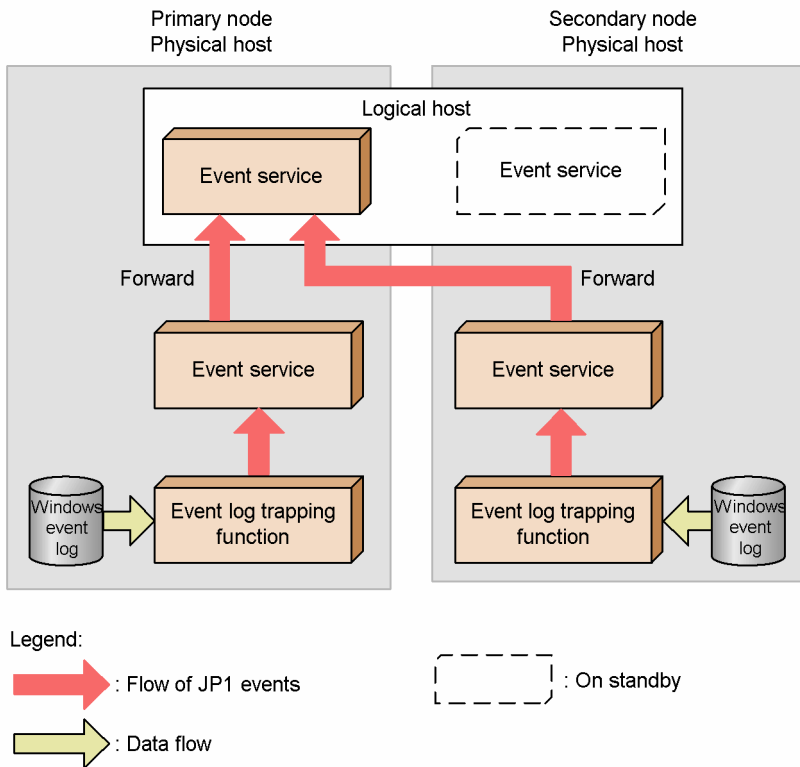
In a cluster system, you must start the event log trapping function separately on each physical host. You cannot start the function by specifying a logical host. However, you can specify whether JP1 events will be forwarded to the event service on a logical host where they can be centrally managed. Configure a forwarding destination that works well with how your system is run.

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. If you do not specify an event server name in the `server` parameter of the action definition file, JP1 events are registered with the event service on the physical host.

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 16. *Definition Files*.

A configuration example for monitoring event logs on both the primary and secondary nodes is shown in the following figure.

Figure 5–5: Configuration example for monitoring event logs on both primary and secondary nodes of the logical host



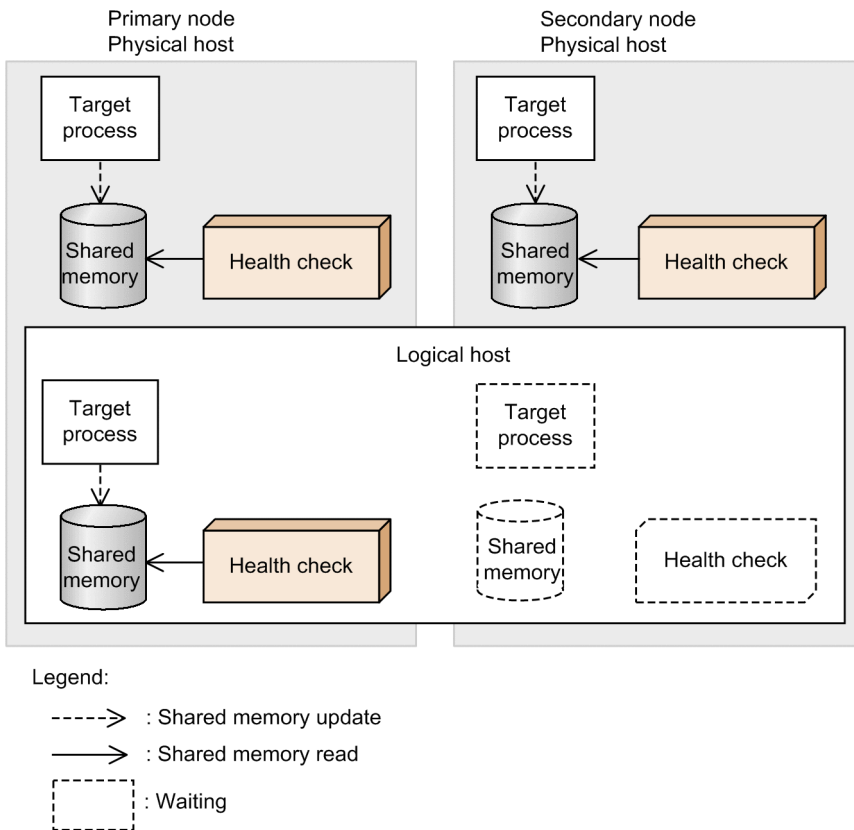
5.3.3 Cluster operation with the health check function

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 *16. Definition Files*.

The following figure shows a configuration example using the health check function in a clustering environment.

Figure 5–6: 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.

5.4 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.

5.4.1 Required environment settings

The following describes the required environment settings for using JP1/Base in a cluster system. For the actual setup procedure, see [5.4.3 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	<i>shared-folder</i> \jplbase\conf\
Log file	<i>shared-folder</i> \jplbase\log\
Event server settings file	<i>shared-folder</i> \jplbase\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 `\shdisk\node0` as a shared folder for logical host `node0`.

```
\shdisk\node0\jplbase\conf\  
\shdisk\node0\jplbase\log\
```

The event service can be set up to independently run in cluster mode. However, if you set up the environment according to [5.4.3 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 [2.10 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 [5.4.5 Settings to configure both physical and logical host environments on the same 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 by using the `jbsmkumap` command, the `jbssetumap` command, the `jbsrmumap` command, or the JP1/Base Environment Settings dialog box.
- Change the authentication server by using the `jbssetupsrv` command or the JP1/Base Environment Settings dialog box.
- Delete the common definition information on the logical host by using the `jbsunsetcnf` command or the `jplbshasetup` command.
- Change the password management information for an OS user by using the `jbsmkpass` command, the `jbspassmgr` command, the `jbsumappass` command, the `jbsrmumappass` command, or the JP1/Base Environment Settings dialog box.
- Change the `jplhosts` information by using the `jbshostsimport` command.
- Change the directory server to be linked by using the `jbschgds` command.
- Set the command execution environment by using the `jcocmddef` command.

When you change the common definition information, make the information consistent on all servers by following the procedures in [5.6 Follow-up tasks when changing settings in a cluster environment](#).

(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.

5.4.2 Installing JP1/Base

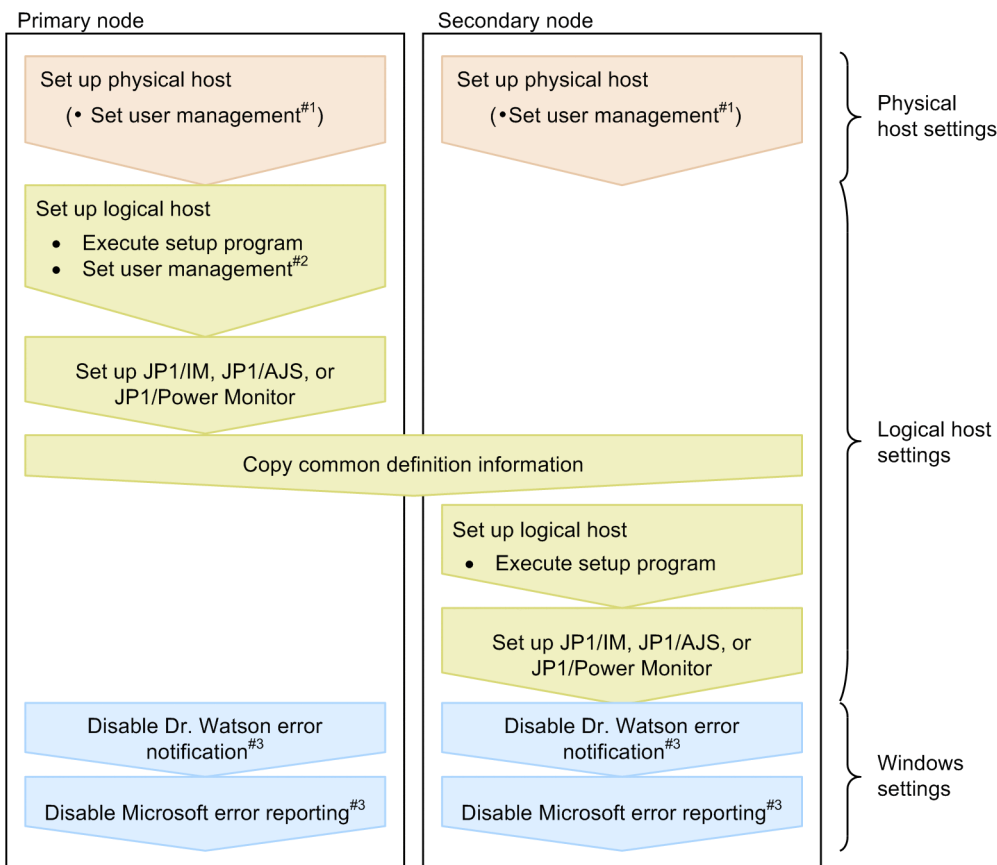
Install JP1/Base on both the primary and secondary node local disks. The installation drive and folder must be the same on both nodes. Do not install JP1/Base on a shared disk.

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 [3.2.3\(5\) Overwrite installation](#).

5.4.3 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 5–7: 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: This setting is required only in Windows Server 2003 and Windows XP.

(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.

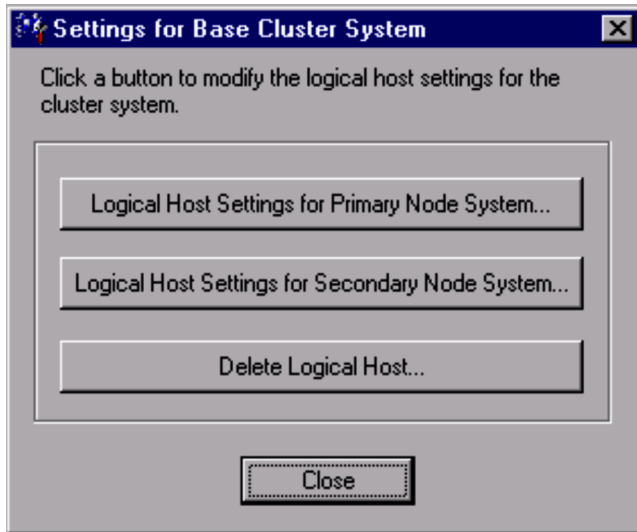
Specify this option if you want to run an authentication server on the physical host. For details on the user management function, see *8.1 User management setup (in Windows)*.

2. Set the logical host.

Setting up through GUI

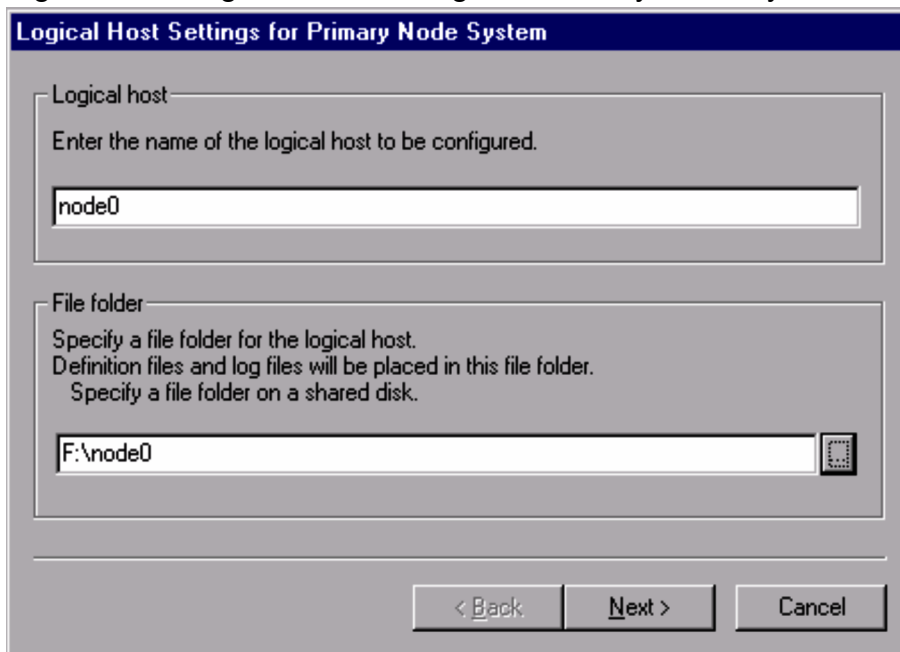
1. Execute `installation-folder\bin\jp1bshasetup.exe`.

Figure 5–8: Settings for Base Cluster System dialog box



2. In the Settings for Base Cluster System dialog box, click **Logical Host Settings for Primary Node System**.

Figure 5–9: Logical Host Settings for Primary Node System dialog box

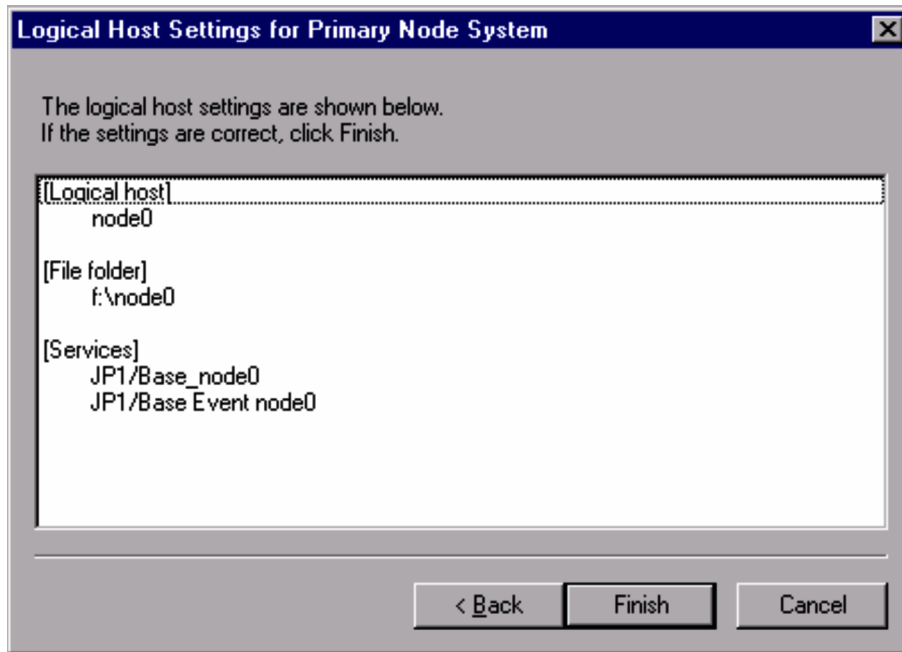


In this dialog box, specify the name of the logical host for which the information is being created, and a folder on the shared disk in which to create shared folders and shared files.

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.

Figure 5–10: Logical Host Settings for Primary Node System dialog box (confirmation window)



You can check the settings in the confirmation window of the Logical Host Settings for Primary Node System dialog box. If the settings are correct, click **Finish**.

This completes all the settings except the communication protocol for the event service.

4. Set up the authentication server on the logical host.

By default, the authentication servers for the logical host are the same as those set for the physical host. You can use the GUI to set authentication servers different from those for the physical host. For details, see [8.1.1 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 [15. Commands](#).

3. Set up user management for the logical host (only when using the logical host as the authentication server).

For details on setting user management function, see [8.1 User management setup \(in Windows\)](#).

Set up by using the GUI

1. From the Windows **Start** menu, choose **Programs, JP1_Base**, and then **JP1_Base Setup**.
2. In the Select Logical Host dialog box, select the logical host for which you want to set up user management.
3. Register the JP1 user.
4. Set JP1 user operating permissions.

Set up by using commands

1. Register the JP1 user.

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. Set JP1 user operating permissions.

The user permission level file (JP1_UserLevel) resides in the following location:

```
shared-folder\conf\user_acl\JP1_UserLevel
```

After editing this file (JP1_UserLevel), execute the `jbsaclreload` command to apply the settings.

4. Register the user mapping information in the common definition information.

For details about the user mapping information settings, see [8.1 User management setup \(in Windows\)](#).

Set up by using the GUI

1. From the Windows **Start** menu, choose **Programs, JP1_Base**, and then **JP1_Base Setup**.
2. In the Select Logical Host dialog box, select the logical host for which you want to set up user management function.
3. Select the **User Mapping** tab of the JP1/Base Environment Settings dialog box.
4. Set the user mapping information.

Set up by using commands

The user mapping definition file (`jp1BsUmap.conf`) resides in the following location:

```
shared-folder\jp1base\conf\user_acl\jp1BsUmap.conf
```

After editing this file (`jp1BsUmap.conf`), execute the following command to register the user mapping information.

```
jbsmkumap -h logical-host-name
```

If you want to check the registered user mapping information, execute the following command:

```
jbsgetumap -h logical-host-name
```

5. Change the JP1/Base communication protocol.

Change the communication protocol for JP1/Base on physical and logical hosts as required.

For details on whether changing the communication protocol is required and how to do so, see [6. JP1/Base Communication Settings According to Network Configurations](#).

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
```

6. Settings to configure both physical and logical host environments on the same host.

To configure both physical and logical host environments on the same host, you need to set up the network control.

For details, see [5.4.5 Settings to configure both physical and logical host environments on the same host](#).

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 [JP1/Integrated Management 3 - Manager Configuration](#)

Guide, JP1/Integrated Management 3 - Manager Administration Guide, JP1/Automatic Job Management System 3 System Design (Configuration) Guide, JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide, and the JP1/Automatic Job Management System 3 Administration Guide.

(2) Setup on the secondary node

To set up the physical and logical hosts 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.

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 [8.1 User management setup \(in Windows\)](#).

2. 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
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

3. Copy the backup file to the secondary node.

4. 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.

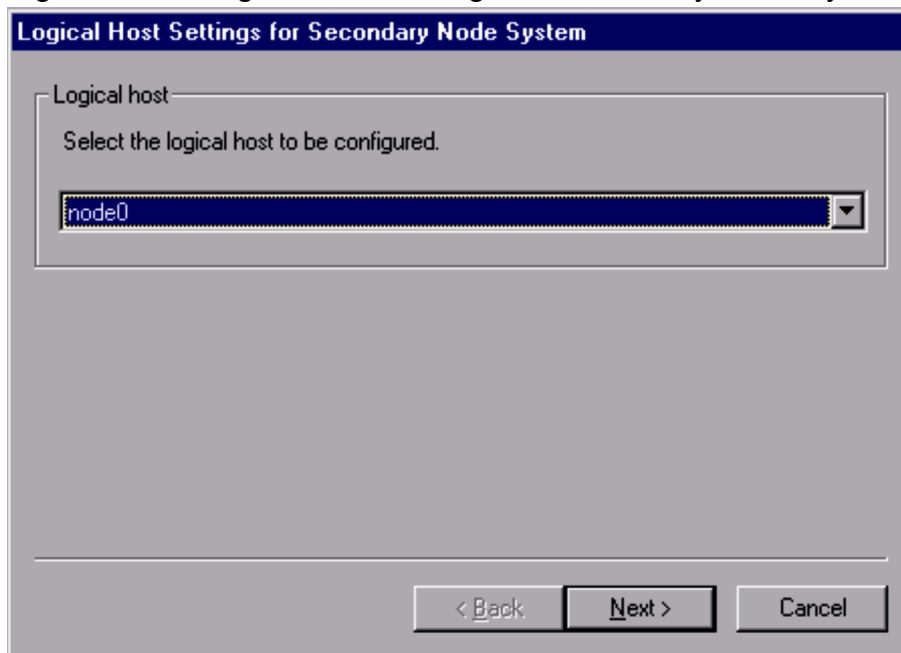
```
jbssetcnf backup-file-name
```

5. Set the logical host.

Setting up through GUI

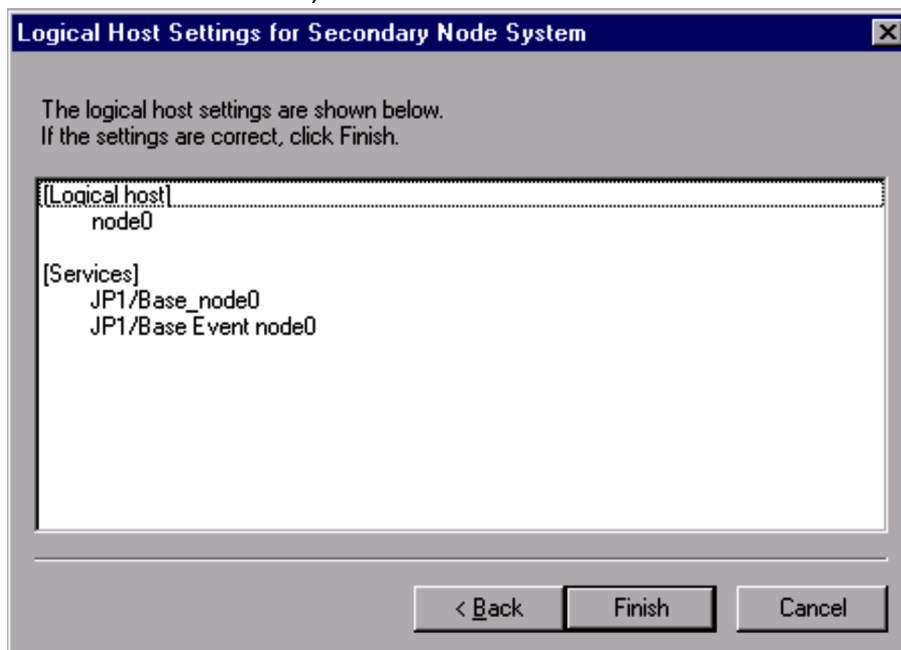
1. Execute `installation-folder\bin\jplbshasetup.exe`.
2. In the Settings for Base Cluster System dialog box, click **Logical Host Settings for Secondary Node System**. In the Logical Host Settings for Secondary Node System dialog box, select the logical host name assigned to the primary node.

Figure 5–11: Logical Host Settings for Secondary Node System dialog box



3. Click the **Next** button.

Figure 5–12: Logical Host Settings for Secondary Node System dialog box (confirmation window)



You can check the settings in the confirmation window of the Logical Host Settings for Secondary Node System dialog box. 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 15. *Commands*.

6. Change the communication protocol of JP1/Base.

Change the communication protocol of JP1/Base on physical hosts as required. This setting is not required on logical hosts.

For details on whether changing the communication protocol is required and how to do so, see [6. JP1/Base Communication Settings According to Network Configurations](#).

7. Settings to configure both physical and logical host environments on the same host.

To configure both physical and logical host environments on the same host, you need to set up the network control. For details, see [5.4.5 Settings to configure both physical and logical host environments on the same host](#).

This completes JP1/Base setup on the secondary node.

5.4.4 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_ <i>logical-host-name</i>	JP1_Base_ <i>logical-host-name</i>
JP1/Base Event <i>logical-host-name</i>	JP1_Base_Event <i>logical-host-name</i>

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 Event *logical-host-name*" first, and then start "JP1/Base_ *logical-host-name*". Make sure to start JP1/IM and JP1/AJS after JP1/Base_ *logical-host-name* has started. When stopping the products, stop them in the reverse order.

5.4.5 Settings to configure both physical and logical host environments on the same host

To configure both physical and logical host environments on the same host, you need to set up the network control. If you skip this process in Windows, the system operates as if the IP address of the logical host were assigned to the physical host, causing the physical host to receive requests intended for the logical host. Also, an IP address that is resolved from the physical host name might be converted to an unexpected IP address, causing malfunction of the JP1 communication. To avoid this scenario, use the following procedure to set up network control when you set up JP1/Base on the logical host.

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 `jp1hosts` information or `jp1hosts2` information to the common definition information.

For `jp1hosts` 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 *15. Commands*.

Also, change the communication settings for the event service.

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`
- Set the `ports` parameter in the event server settings file (`conf`) on the physical host.

Example:

```
jp1-node1:
ports 100.100.100.1 jplimevt jplevtapi
```

```
jp1-node2:
ports 100.100.100.2 jplimevt jplevtapi
```

- Add the `server` parameter in the API settings file (`api`).

Example:

```
server jp1-node1 keep-alive 100.100.100.1
server jp1-node2 keep-alive 100.100.100.2
```

- Start JP1/Base services on physical and logical hosts.

For `jp1hosts2` information:

Execute the `jbshosts2import` command to register the contents of the definition file with the physical host. For details on the `jbshosts2import` command, see [*jbshosts2import*](#) in *15. Commands*.

Note that you do not have to change the communication settings for the event service.

Example: Execute the `jbshosts2import` command as follows:

- Stop JP1/Base services on physical and logical hosts.
- Execute `jbshosts2import -o definition-file-name`
- Start JP1/Base services on physical and logical hosts.

If you set `0` for the `+PhysicalMerge` parameter in the `jp1hosts2` information for the logical host, you also need to register the definition file contents with the `jp1hosts2` information for the logical host.

3. Check the settings applied to the `jp1hosts` and `jp1hosts2` 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\jplping jp1-node1
LogicalHostnameKey : no define. use JP1_DEFAULT
jplhosts : Use jplhosts entry in JP1_DEFAULT
Search jplhosts : 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\jplping jp1-node2
LogicalHostnameKey : no define. use JP1_DEFAULT
jplhosts : Use jplhosts entry in JP1_DEFAULT
Search jplhosts : 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\jplping -h jp1-cluster jp1-node1
LogicalHostnameKey : jp1-cluster
jplhosts : Use jplhosts entry in jp1-cluster
Search jplhosts : jp1-node1 is found.
Resolved Host List : jp1-node1 -> 100.100.100.1(100.100.100.1)
...
```

```
c:\>installation-folder\bin\jplping -h jp1-cluster jp1-node2
LogicalHostnameKey : jp1-cluster
jplhosts : Use jplhosts entry in jp1-cluster
Search jplhosts : 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.

5.5 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.

5.5.1 Required environment settings

The following describes the required environment settings for using JP1/Base in a cluster system. For the actual setup procedure, see [5.5.3 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	<i>shared-directory</i> /jplbase/conf/
Log file	<i>shared-directory</i> /jplbase/log/
Event server settings file	<i>shared-directory</i> /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/jplbase/conf/  
/shdsk/node0/jplbase/log/
```

The event service can be set independently to run in cluster mode. However, if you set up the environment according to [5.5.3 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 [2.10 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 by using the `jbsmkumap` command, the `jbssetumap` command, or the `jbsrmumap` command.
- Change the authentication server by using the `jbssetusrsv` command.
- Delete the common definition information on the logical host by using the `jbsunsetcnf` command.
- Change the `jp1hosts` information by using the `jbshostsimport` command.
- Set the command execution environment by using the `jcocmddef` command.

When you change the common definition information, make the information consistent on all servers by following the procedures in [5.6 Follow-up tasks when changing settings in a cluster environment](#).

(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.	<code>jbs_start.cluster logical-host-name</code>
Stop	Stop JP1/Base.	<code>jbs_stop.cluster logical-host-name</code>
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.	<code>jbs_spmd_status -h logical-host-name</code>
Kill	Kill JP1/Base and release the resources it has been using.	<code>jbs_killall.cluster logical-host-name</code>

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.

- The automatic start script for logical hosts (`jbs_start.cluster`) performs an unsetup of the locale settings of `LC_ALL`, `LC_COLLATE`, `LC_CTYPE`, `LC_MONETARY`, `LC_NUMERIC`, `LC_TIME`, and `LC_MESSAGES` by default.

5.5.2 Installing JP1/Base

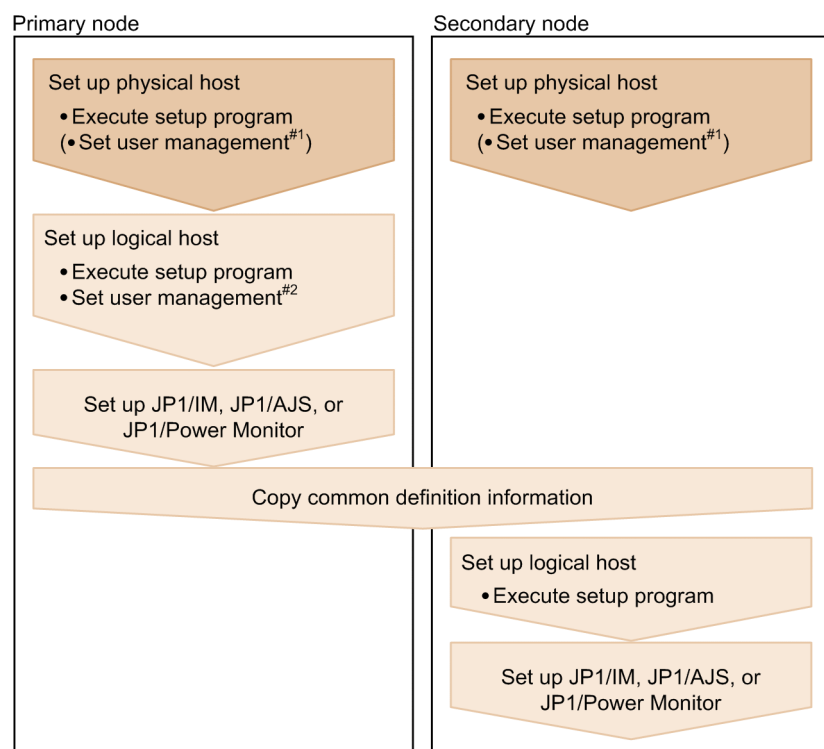
Install JP1/Base on the local disks of both the primary node and secondary node. Do not install JP1/Base on a shared disk.

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 [3.3.4\(5\) Overwrite installation](#).


5.5.3 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. Before you set up, you must specify the language on the physical host. The language set on the physical host is inherited to the logical host. For details on how to set the language, see [3.4.2 Setting the language \(for UNIX\)](#).

Figure 5–13: Setup procedure for a cluster system (in UNIX)



Legend:

 : Settings for physical hosts

 : Settings for logical hosts

#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 set up the physical and logical hosts 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 [8.3 User management setup \(in UNIX\)](#).

2. 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.

```
jplbase_setup_cluster -h node0 -d /shdisk/node0 -a node0 -s
```

For details on the `jplbase_setup_cluster` command, see [jplbase_setup_cluster \(UNIX only\)](#) in [15. Commands](#).

3. 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 users (only when the logical host is used 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 (`jplBsUmap.conf`) resides in the following location:

```
shared-directory/jplbase/conf/user_acl/jplBsUmap.conf
```

After editing the file (`jplBsUmap.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
```

- 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/jplbase/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 [8.3 User management setup \(in UNIX\)](#).

4. Change the JP1/Base communication protocol.

Change the communication protocol of JP1/Base on physical and logical hosts as required.

For details on whether changing the communication protocol is required and how to do so, see [6. JP1/Base Communication Settings According to Network Configurations](#).

Notes on operating authentication servers in a cluster system:

The settings files for authentication servers are stored in the following directory.

```
shared-directory/jplbase/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/jplbase/conf/user_acl/
```

When not using a cluster system:

```
/etc/opt/jplbase/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 `jplbase_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 `jplbase_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/jplbase/conf
cp -p jplbs_spmd.conf.session.model jplbs_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.

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 *JP1/Integrated Management 3 - Manager Configuration Guide*, *JP1/Integrated Management 3 - Manager Administration Guide*, *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *JP1/Automatic Job Management System 3 Administration Guide*.

(2) Setup on the secondary node

To set up the physical and logical hosts 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.

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 [8.3 User management setup \(in UNIX\)](#).

2. 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
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

3. Copy the backup file to the secondary node.

4. 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
```

5. Set the logical host.

Execute the command as follows:

```
jplbase_setup_cluster -h node0
```

For details on the `jplbase_setup_cluster` command, see [jplbase_setup_cluster \(UNIX only\)](#) in *15. Commands*.

6. Change the JP1/Base communication protocol.

Change the communication protocol of JP1/Base on physical hosts as required. This setting is not required on logical hosts.

For details on whether changing the communication protocol is required and how to do so, see [6. JP1/Base Communication Settings According to Network Configurations](#).

This completes JP1/Base setup on the secondary node.

5.5.4 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.
- Before registering the daemons to the cluster software, change the value of the `LANG` environment variable of `jbs_start.cluster` to the language specified in `jplbs_env.conf` for the logical host.

The information needed when registering JP1/Base into cluster software is shown below:

Functionality	Description
Start	Start JP1/Base. <ul style="list-style-type: none">• Command <code>jbs_start.cluster <i>logical-host-name</i></code>

Functionality	Description
	<ul style="list-style-type: none"> 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 Determine the result of starting JP1/Base based on the information in the operation monitoring section of this table. 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	<p>Stop JP1/Base.</p> <ul style="list-style-type: none"> Command <code>jbs_stop.cluster logical-host-name</code> 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 Determine the result of stopping JP1/Base based on the information in the operation monitoring section of this table. The return value of the stop command cannot be used for judgment because it is either 0 (normal end) or 1 (abnormal argument). <p>Remarks:</p> <p>After the stop command finishes, execute the <code>jbs_spmc_status</code> and <code>jevstat</code> commands to check whether JP1/Base has stopped normally. If JP1/Base has not stopped, execute the command described in the kill functionality below.</p>
Operation monitoring	<p>Use the return values from the <code>jbs_spmc_status</code> and <code>jevstat</code> 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.</p> <ul style="list-style-type: none"> Command <code>jbs_spmc_status -h logical-host-name</code> <code>jevstat logical-host-name</code> 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 <code>jbs_spmc_status</code> 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 <code>jbs_spmc_status</code> 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 <code>jevstat</code> command, this return value indicates an error for which retry is not possible.
Kill	<p>Kill JP1/Base and release the resources it has been using.</p> <ul style="list-style-type: none"> Command <code>jbs_killall.cluster logical-host-name</code> <p>When you execute the <code>jbs_killall.cluster</code> command, each process is forcibly stopped without performing any processing for stopping JP1/Base.</p>

Functionality	Description
	<p>Note</p> <p>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.</p>

#

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_spm�_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.

5.6 Follow-up tasks when changing settings in a cluster environment

JP1/Base and products for which JP1/Base is a prerequisite (JP1/IM, JP1/AJS, and JP1/Power Monitor) keep a set of common definition information for each logical host on a local disk. When you change a setting that affects the common definition information in a cluster system, you must make the information consistent between the logical hosts on the primary and secondary nodes.

5.6.1 Operations that result in changes to the common definition information on the primary node and how to apply the settings to the secondary node

The table below shows the operations that result in changes to the common definition information, and how to carry those changes over to the common definition information on the secondary node. Note that the operations listed in the table affect JP1/Base and all products for which JP1/Base is a prerequisite. We also recommend that you back up the common definition information before and after making any changes. For details on how to back up the common definition, see [3.5.2 Backup and recovery \(in Windows\)](#) or [3.5.3 Backup and recovery \(in UNIX\)](#).

Table 5–4: Operations that update common definition information on the primary node and how to apply the setting to the secondary node

Function	Action on primary node	Application to secondary node
General JP1/Base settings	Adding or changing the common definition information for JP1/Base or a product with JP1/Base as a prerequisite (JP1/IM, JP1/AJS, or JP1/Power Monitor).	See (1) <i>When common definition information is added or changed.</i>
User mapping information	Adding or changing user mapping information using the <code>jbsmkumap</code> command, the <code>jbssetumap</code> command, or the JP1/Base Environment Settings dialog box (Windows only).	See (1) <i>When common definition information is added or changed.</i>
	Deleting user mapping information using the <code>jbsmkumap</code> command, <code>jbsrmumap</code> command, or the JP1/Base Environment Settings dialog box (Windows only), or deleting the OS user mapped to a JP1 user.	See (2) <i>When user mapping information is deleted.</i>
	Adding, changing or deleting user mapping information using the <code>jbsmkumap</code> command, the <code>jbssetumap</code> command, the <code>jbsrmumap</code> command, or the JP1/Base Environment Settings dialog box (Windows only), or deleting the OS user mapped to a JP1 user.	See (1) <i>When common definition information is added or changed and</i> (2) <i>When user mapping information is deleted.</i>
Password information for OS users	Adding or changing password information for OS users using the <code>jbsmkpass</code> command, the <code>jbsumappass</code> command, the <code>jbspassmgr</code> command or the JP1/Base Environment Settings dialog box.	See (1) <i>When common definition information is added or changed.</i>
	Deleting password information for OS users using the <code>jbsmkpass</code> command, the <code>jbsrmumappass</code> command, the <code>jbspassmgr</code> command or the JP1/Base Environment Settings dialog box.	See (3) <i>When OS user password information is deleted.</i>
	Adding, changing or deleting password information for OS users using the <code>jbsmkpass</code> command, the <code>jbsumappass</code> command, the <code>jbsrmumappass</code> command, the <code>jbspassmgr</code> command or the JP1/Base Environment Settings dialog box.	See (1) <i>When common definition information is added or changed and</i> (3) <i>When OS user password information is deleted.</i>

Function	Action on primary node	Application to secondary node
jplhosts information	Adding or changing jplhosts information using the <code>jbshostsimport</code> command.	See (1) <i>When common definition information is added or changed.</i>
	Deleting jplhosts information using the <code>jbshostsimport</code> command.	See (4) <i>When jplhosts information is deleted.</i>
	Adding, changing or deleting jplhosts information using the <code>jbshostsimport</code> command.	See (1) <i>When common definition information is added or changed and</i> (4) <i>When jplhosts information is deleted.</i>
Directory server linkage	Changing a linked directory server using the <code>jbshchgds</code> command.	See (1) <i>When common definition information is added or changed.</i>
Command execution	Setting up the command execution environment using the <code>jcocmddef</code> command.	See (1) <i>When common definition information is added or changed.</i>
	After using the <code>jcocmddef</code> command to set up the command execution environment, specifying the command with the <code>-group</code> option to delete a host or host group.	See (5) <i>When a host or host group is deleted in the command execution environment.</i>
Authentication server	Adding or changing authentication server the <code>jbsssetusrsv</code> (UNIX only) command, the <code>jbsssetupsv</code> (Windows only) command, or the JP1/Base Environment Settings dialog box (Windows only).	See (1) <i>When common definition information is added or changed.</i>
	Deleting authentication server the <code>jbsssetusrsv</code> (UNIX only) command, the <code>jbsssetupsv</code> (Windows only) command, or the JP1/Base Environment Settings dialog box (Windows only).	See (6) <i>When authentication server is deleted.</i>
	Adding, changing or deleting authentication server the <code>jbsssetusrsv</code> (UNIX only) command, the <code>jbsssetupsv</code> (Windows only) command, or the JP1/Base Environment Settings dialog box (Windows only).	See (1) <i>When common definition information is added or changed and</i> (6) <i>When authentication server is deleted.</i>

(1) When common definition information is added or changed

When additions or changes are made to the common definition information by one of the operations listed in Table 5-4, you need to make the common definition information consistent on the primary and secondary nodes. If several of the operations in Table 5-4 are executed in succession, you only need to perform this procedure once to apply all the changes to the common definition information on the secondary node.

1. On the primary node, back up the common definition information by executing the `jbssgetcnf` command.

Execute the command as follows:

```
jbssgetcnf -h logical-host-name > backup-file-name
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

2. Copy the backup file to the secondary node.
3. Execute the `jbsssetcnf` command on the secondary node with the backup file specified as a command argument.

Execute the command as follows:

```
jbsssetcnf backup-file-name
```

(2) When user mapping information is deleted

If you used the `jbsmkumap` or `jbsrmumap` command or the JP1/Base Environment Settings dialog box (Windows only) to delete user mapping information, use the following procedure to make the common definition consistent between the primary and secondary nodes:

1. On the primary node, execute the `jbsgetumap` command to back up the user mapping information.

Execute the command as follows:

```
jbsgetumap -h logical-host-name > backup-file-name
```

2. Copy the backup file to the secondary node.
3. Execute the `jbsmkumap` command on the secondary node with the backup file specified as a command argument.

Execute the command as follows:

```
jbsmkumap -h logical-host-name -f backup-file-name
```

(3) When OS user password information is deleted (Windows only)

If you used the `jbsmkpass`, `jbsrmumappass`, or `jbspassmgr` command or the JP1/Base Environment Settings dialog box to delete password information for OS users, use the procedures below to make the common definition consistent on the primary and secondary nodes. Note that the way in which you apply the changes to the common definition information on the secondary node differs for each command.

(a) When an OS user is deleted by the `jbspassmgr` command

On the secondary node, execute the `jbspassmgr` command to delete the registered user you deleted from the primary node.

(b) When an OS user is deleted by the `jbsrmumappass` command

On the secondary node, execute the `jbsrmumappass` command to delete the OS user you deleted from the primary node.

(c) When an OS user is deleted by the `jbsmkpass` command

Use the following procedure to make the common definition consistent between the primary and secondary nodes:

1. Copy the password definition file used on the primary node to the secondary node.
2. Execute the `jbsmkpass` command on the secondary node with the password definition file specified as a command argument.

Execute the command as follows:

```
jbsmkpass -h logical-host-name -f password-definition-file
```

(d) When an OS user is deleted by the JP1/Base Environment Settings dialog box

On the secondary node, execute the JP1/Base Environment Settings dialog box to delete the registered user you deleted from the primary node.

(4) When jp1hosts information is deleted

If you used the `jbshostsimport` command to delete `jp1hosts` information, use the following procedure to make the common definition consistent between the primary and secondary nodes:

1. On the primary node, back up the `jp1hosts` information by executing the `jbshostsexport` command.

Execute the command as follows:

```
jbshostsexport -h logical-host-name > backup-file-name
```

2. Copy the backup file to the secondary node.
3. Execute the `jbshostsimport` command on the secondary node with the backup file specified as a command argument.

Execute the command as follows:

```
jbshostsimport -h logical-host-name -r backup-file-name
```

Note

In an environment in which `jp1hosts2` information is registered, also specify the `-f` option when executing the `jbshostsimport` command. For details on the `jbshostsimport` command, see [jbshostsimport](#) in *15. Commands*.

(5) When a host or host group is deleted in the command execution environment

If you use the `jcocmddef` command to set up the command execution environment and then specify the command with the `-group` option to delete a host or host group, use the following procedure to make the common definition consistent between the primary and secondary nodes:

1. Copy the host group definition file from the primary node to the secondary node.
2. Execute the `jcocmddef` command on the secondary node with the host group definition file specified as a command argument.

Execute the command as follows:

```
jcocmddef -host logical-host-name -group host-group-definition-file
```

(6) When authentication server is deleted

If you used the `jbsssetusrsvr` (UNIX only), or `jbsssetupsrv` (Windows only) command or the JP1/Base Environment Settings dialog box (Windows only) to delete authentication server, use the procedures below to make the common definition consistent on the primary and secondary nodes.

(a) When authentication server is deleted by the `jbsssetusrsvr` (UNIX only) command

On the secondary node, execute the `jbsssetusrsvr` command to delete the authentication server you deleted from the primary node.

(b) When authentication server is deleted by the jbssetupsrv (Windows only) command

On the secondary node, execute the `jbssetupsrv` command to delete the authentication server you deleted from the primary node.

(c) When authentication server is deleted by the JP1/Base Environment Settings dialog box (Windows only)

On the secondary node, execute the JP1/Base Environment Settings dialog box to delete the authentication server you deleted from the primary node.

5.7 Deleting logical hosts

5.7.1 Deleting logical hosts (in Windows)

In Windows, you can delete a logical host by using a command, or from the GUI. The logical host must be deleted from both the primary and secondary node.

Deleting logical hosts from the GUI:

1. Execute the `jplbshasetup.exe` command.
2. In the Settings for Base Cluster System dialog box, click the **Delete Logical Host** button.
3. Select the name of the logical host you want to delete.

Deleting logical hosts using a command:

Execute the following command:

```
jbs_setup_cluster -h node0 -r
```

For details on the `jbs_setup_cluster` command, see *jbs_setup_cluster (Windows only)* in *15. Commands*.

These operations delete the logical host information and services for JP1/Base, JP1/IM, and JP1/AJS, as well as the logical host information for JP1/Power Monitor. They do not delete the shared files and folders on the shared disk, so delete these files and folders manually.

Notes:

If the host names of the logical host and the physical host (as reported by the `hostname` command) are the same in your environment, perform the following additional tasks:

- Change the configuration of the event service environment.
Uncomment the line `server * default` which is included in the event server index file (`index`) by default.
- Restore the original definition in `jevlogical_setup.conf`.
 1. Create a definition file with the following contents.
You can choose any name for the file.

```
[JP1_DEFAULT\JP1BASE\  
"JEVSERVICE_LOGICAL"=dword:00000000
```
 2. Execute the following command to apply the file contents to the common definition information.

```
jbssetcnf definition-file-name
```

5.7.2 Deleting logical hosts (in UNIX)

In UNIX, you must delete the logical host on both the primary and secondary nodes.

Execute the following:

1. Execute the following command:

```
jbsunsetcnf -i -h logical-host-name
```

For details on the `jbsunsetcnf` command, see *jbsunsetcnf* in *15. Commands*.

2. Modify the settings of the event service environment.

Delete the line of the logical host to be deleted which is set in the event server index file (`index`).

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.

Uncomment the line `server * default` which is included in the event server index file (`index`) by default.

- Modify the settings for the environment setting directory.

1. Create a definition file with the following contents.

You can choose any name for the definition file.

```
[JP1_DEFAULT\JP1BASE\]
```

```
"JEVSERVICE_LOGICAL"=dword:00000000
```

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
```

5.8 Notes on using JP1/Base in a cluster system

5.8.1 Notes on cluster use (common to all OSs)

- 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 `jvsend` 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. However, as data is written to the disk each time a JP1 event is issued, the performance of JP1 event issuing may be degraded. As performance varies depending on the environment, carry out investigations in advance.
 - 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 to change the address specified in the `ports` parameter to the local host name, to the IP address of the local host, or to `<jp1hosts2>`. The event service on the physical host is set to `jp1host2` (for new installations) or `0.0.0.0` (for overwrite installations from version 09-00 or earlier) by default. However, an event service (on the physical host) that is set to `0.0.0.0` 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 *16. Definition Files*.
 - Suppose that the authentication server is used in a cluster system and JP1/IM and JP1/AJS are installed on the host on which the authentication server is set up. If 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 *jcocmddef* in *15. Commands*.
 - When the function for automatically re-organizing the command execution log file is enabled, the amount of JP1/Base startup time increases in proportion to the file size. If this causes failover errors, disable this function.

For details about the function for automatically re-organizing the command execution log file, see [4.9 Function for automatically re-organizing the command execution log file](#).

- We recommended that you set name resolution so that the IP address preferentially assigned to the physical host does not become a loop-back address (127.0.0.1) when JP1/Base of a physical host that communicates with other hosts is used in the environment where the logical host is created. Perform the settings as described below when the IP address preferentially assigned to the physical host must be a loop-back address (127.0.0.1):
 - Specify an IP address that can communicate with other hosts on the physical host using `jp1hosts`.
 - Specify an IP address that can communicate with other hosts in the `ports` parameter address of the event server setting file (`conf`).
 - Add the server parameter of the physical host name to the API setting file (`api`) and specify an IP address that can communicate with other hosts in an address of the setting file.

For operation in an environment where the network is separated, the above setting must be performed even in the environments where the logical host was not created.

5.8.2 Notes on cluster use (limited to 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 `jbsetconf` 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.
- The JP1/Base LogTrap service is required for using log file traps. This service enables JP1 events converted by log file traps to be registered with event services on physical or logical hosts. You must start the JP1/Base LogTrap service when you start a log file trap to register events with an event service on a logical host even if JP1/Base is not used on the physical 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.
- If you are using the event service on the physical hosts, you must edit the event server settings file (`conf`) for the event service on the physical host of both primary and secondary nodes. The event server settings file (`conf`) for the event service on the logical hosts defined by the `jp1bshsetup.exe` command resides in the following location:
folder-name-specified-on-shared-disk\jp1base\event\conf

- If the JP1/Base service fails to start or stop, JP1/Base processes may remain active in the system. If this happens, restart your computer.
- If you changed the `jplhosts` information and communication protocol on a physical host, the settings will be copied when you execute the `jplbshsetup` command to set up the logical hosts. If you want the `jplhosts` information and communication protocol for the logical hosts to be different from the settings for the physical host, you must re-enter the `jplhosts` information and protocol settings for the logical hosts.
- Do not use a disk at the network drive destination as a shared disk for JP1/Base.

5.8.3 Notes on cluster use (limited to UNIX only)

- The following procedure shows how to change the language setting for a logical host after setting up the cluster system environment. Shut down JP1/Base and related programs before proceeding.
 1. Change the language setting in the shared file `jplbs_env.conf` on the shared disk used by the logical host whose language you want to change.
For details on how to do so, see [3.4.2 Setting the language \(for UNIX\)](#).
 2. Create a text file in vi or another editor.
In this example, the language is set to EUC (Japanese) encoding.

```
[logical-host-name\JP1BASE\  
"LANG"="EUCJIS"
```


End the final line with a linefeed character.
 3. Save the text file you created.
You can give the file any name. In this example, the file name is `baselang.conf`.
 4. Execute the following command as a user with superuser or JP1/Base administrator permission.

```
/opt/jplbase/bin/jbssetcnf baselang.conf
```
 5. Edit the automatic start script for logical hosts (`jbs_start.cluster`).
Set the `LANG` environment variable of the automatic startup script for logical hosts (`jbs_start.cluster`) to the same language specified in `jplbs_env.conf` in step 1.
If you manually start a logical host event service without using the automatic start script (`jbs_start.cluster`), locale information used when the event service is started (for example, the `LANG` environment variable) must match the language specified in `jplbs_env.conf`.
If, for example, you specify `ja_JP.UTF-8` as the language for `jplbs_env.conf`, change the `LANG` environment variable of the automatic startup script for logical hosts (`jbs_start.cluster`) as follows:

```
## Set Environment-variables  
PATH=/sbin:/bin:/usr/bin:/opt/jplbase/bin  
LANG=ja_JP.UTF-8  
SHLIB_PATH=/opt/jplbase/lib:/opt/hitachi/common/lib
```
- 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 [15. 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/jplbase
cp -p jbs_stop.cluster.retry.model jbs_stop.cluster
```

- If a shell script for monitoring the operating status is registered in the cluster system, and the monitoring interval of the `jbs_spmc_status` command used by the shell script is a short time of 10 seconds or so, the next `jbs_spmc_status` command may execute before the previous `jbs_spmc_status` command completes, potentially causing an unexpected failover. The monitoring interval should therefore be at least 60 seconds. Also, if you changed the `jbs_spmc_status` command's timeout (`-t` option) from the default, set the monitoring interval to a longer time than the time set in the `-t` option.

5.9 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.

5.9.1 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*.

5.9.2 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 *5. 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 [5.9.3\(2\) Examples of setting up automatic startup and automatic termination](#).

5.9.3 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: *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_spm�_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) In AIX environment

1. Using the `mkitab` command, make the following entries in the `/etc/inittab` file:

```
# mkitab -i hntr2mon "unique-ID:2:wait:/etc/opt/jplbase/jbs_start.cluster
logical-host-name"
# mkitab -i unique-ID "unique-ID:2:wait:/etc/opt/jplajs2/jajs_start.cluste
r logical-host-name"
```

Note: Be sure to define *unique-ID* by using no more than 14 bytes, and use an ID that is unique within the file.

Example:

```
# mkitab -i hntr2mon "jplbase_ronril:2:wait:/etc/opt/jplbase/jbs_start.clu
ster logical-host-name"
# mkitab -i jplbase_ronril "jplajs2_ronril:2:wait:/etc/opt/jplajs2/jajs_st
art.cluster 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/jplajs2/jajs_stop.cluster && /etc/opt/jplajs2/jajs_stop.c
luster logical-host-name
test -x /etc/opt/jplbase/jbs_stop.cluster && /etc/opt/jplbase/jbs_stop.clu
ster logical-host-name
test -x /opt/hitachi/HNTRLlib2/etc/D002stop &&
/opt/hitachi/HNTRLlib2/etc/D002stop
```

The added lines execute termination processing for JP1 services when the system stops.

(c) Linux environment

1. Create a Unit file (for automatic startup and termination) for the logical host.

Location: `/etc/systemd/system/jp1_base_logical-host-name.service`

Example of a Unit file

```
[Unit]
# Service name
Description=JP1/Base logical-host-name Service
After=rsyslog.service network.target network.service HNTRLlib2D002.service
ConditionFileIsExecutable=/etc/opt/jplbase/jbs_start.cluster
ConditionFileIsExecutable=/etc/opt/jplbase/jbs_stop.cluster

[Service]
# Service type
Type=forking

# Service operations
```



```
ExecStart=/etc/opt/jplbase/jbs_start.cluster logical-host-name
ExecStop=/etc/opt/jplbase/jbs_stop.cluster logical-host-name

KillMode=none

StandardOutput=null
StandardError=null

[Install]
WantedBy=multi-user.target graphical.target
```

2. Enable the Unit file.

Execute the following command to enable the Unit file:

```
systemctl --system enable jpl_base_logical-host-name.service
```

When you configure a JP1 service to terminate automatically, you must also configure it to start automatically. The system will not execute the termination script for a JP1 service that is configured to terminate but not start automatically.

(d) 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 Linux:

For details about the settings to adjust the order in which JP1 services start and stop automatically between the logical host and physical host in Linux, see (e) below.

In AIX:

To start and stop the physical host automatically, additional settings are required. For details on the additional settings, see [7.2.1 Setting services to start and stop automatically](#).

(e) Settings to adjust the start order between a physical host and logical host (in a Linux environment)

You can adjust the order in which JP1 services start and stop automatically between a physical host and logical host in a Linux environment. To do this, you must specify the following settings in addition to the settings to start and stop JP1 services automatically on the logical host.

To start JP1 services on the physical host first:

Edit the Unit file for the logical host.

Location: /etc/systemd/system/*jpl_base_logical-host-name*.service

Part to edit: Add *jpl_base.service* to the end of the `After=` line.

Example of a Unit file

```
[Unit]
# Service name
Description=JP1/Base logical-host-name Service
```

```
After=rsyslog.service network.target network.service HNTRLib2D002.service
jpl_base.service
ConditionFileIsExecutable=/etc/opt/jplbase/jbs_start.cluster
ConditionFileIsExecutable=/etc/opt/jplbase/jbs_stop.cluster
```

To start P1 services on the logical host first:

Edit the Unit file for the logical host.

Location: `/etc/systemd/system/jpl_base_logical-host-name.service`

Part to edit: Add the `Before=` line, and then define `jpl_base.service`.

Example of a Unit file

```
[Unit]
# Service name
Description=JP1/Base logical-host-name Service
Before=jpl_base.service
After=rsyslog.service network.target network.service HNTRLib2D002.service
ConditionFileIsExecutable=/etc/opt/jplbase/jbs_start.cluster
ConditionFileIsExecutable=/etc/opt/jplbase/jbs_stop.cluster
```

(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.

6

JP1/Base Communication Settings According to Network Configurations

This chapter describes JP1/Base communication settings according to network configurations. The concepts discussed in this chapter also apply to products such as JP1/IM and JP1/AJS for which JP1/Base is a prerequisite. For details, see the documentation for each product.

For an overview of the communication protocol of JP1/Base, see [2.10 Communication protocols of JP1/Base](#).

6.1 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.

If you only use physical hosts, JP1/Base can be used in the default setting (ANY binding method). There is no need to change the communication settings.

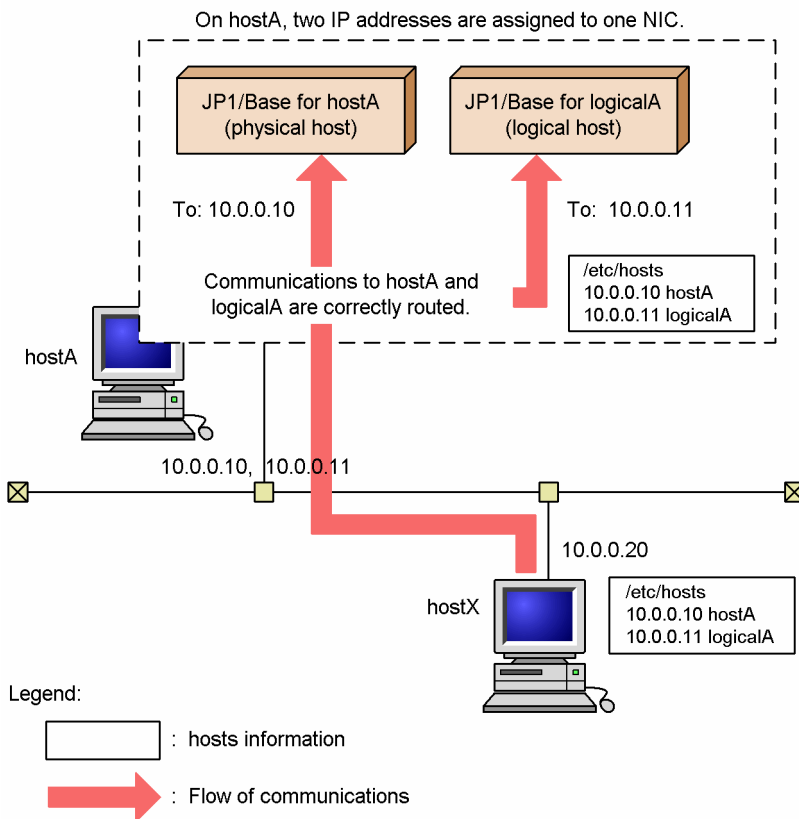
Even when you use JP1/Base in a cluster system, there is no need to change the communication settings if you configure JP1/Base for the cluster system by using either the GUI (`jp1bshasetup.exe`) or the `jbs_setup_cluster` command in Windows, or the `jp1base_setup_cluster` command in UNIX, which all 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.

Note:

If you perform an upgrade installation of JP1/Base version 09-00 or earlier in an environment that only uses physical hosts, you will need to set the event server settings file (`conf`) and API setting file (`api`) before using JP1/Base in a cluster environment.

Figure 6–1: Communication procedure of JP1/Base used in a cluster system on a single network



6.2 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 to multiple networks by multiple NICs, you can use the default settings (ANY binding method). There is no need to change the communication settings.

When an authentication server is started by a physical host, the server uses the highest priority IP address corresponding to the host name in the default state. For a host connected to multiple networks using multiple NICs, change the JP1/Base reception method to an IP binding method when changing the IP address used by the authentication server to addresses other than the highest priority IP address corresponding to the host name for starting the authentication server. The setting procedure is described below:

Note:

If you are using JP1/Base 12-00 or later, you do not need to perform the procedure below. If you are upgrading to JP1/Base 12-00 or later from an environment in which JP1/Base 09-10 or earlier is installed and the settings below have been performed, you do not need to edit items that have already been set. You can continue to use those settings as is and the product can be used without any problems.

1. Register the IP address you want to use for an authentication server in `jp1hosts`.

Edit the `jp1hosts` definition file as described below.

Host name IP address 1 for an authentication server (, IP address 2 for an authentication server, IP address 3 for an authentication server), the highest priority IP address corresponding to the host name

2. Execute the `jbshostsimport` command and register it in the common definition information.

Execute the command as described below.

```
jbshostsimport {-o|-r} jp1hosts-definition-file-name
```

3. Change the configuration of the communication method.

Execute the command described below, apply the communication method configuration file to the common definition information, and change the configuration of the communication method. The communication method configuration file is stored under the `installation-folder\conf\`.

- When transmissions are based on the ANY binding method

```
jbssetcnf physical_ipany.conf
```

- When transmissions are based on the IP binding method

```
jbssetcnf physical_ipip.conf
```

After the above procedure is performed, the authentication server receives communication from all IP addresses defined in `jp1hosts`. If you want to use only a single IP address for reception, place the relevant IP address at the top of the `jp1hosts` definition file, and then apply the contents of the communication method configuration file (`physical_recovery_0651.conf`) to the common definition information by using the `jbssetcnf` command as described below.

```
jbssetcnf physical_recovery_0651.conf
```

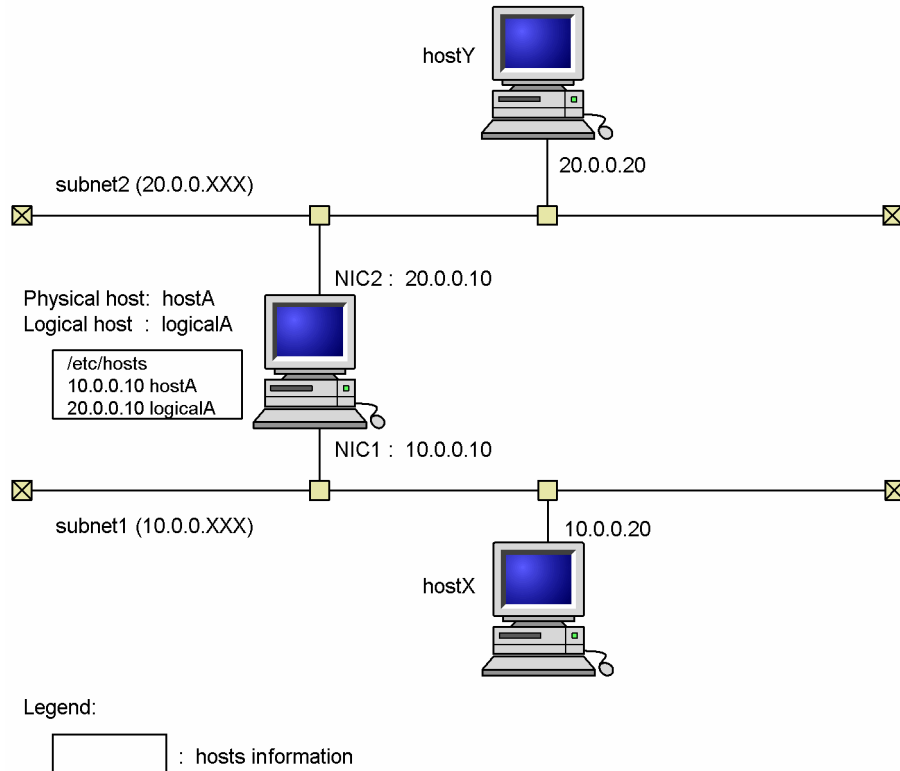
Be sure to restart JP1/Base when the JP1/Base communication setting is changed.

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.

6.2.1 Communication settings when JP1/Base is used on multiple networks

This subsection describes communication settings required when a logical host is used on a physical host that is connected with multiple networks through multiple NICs, based on the system configuration example shown in the following figure.

Figure 6–2: 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

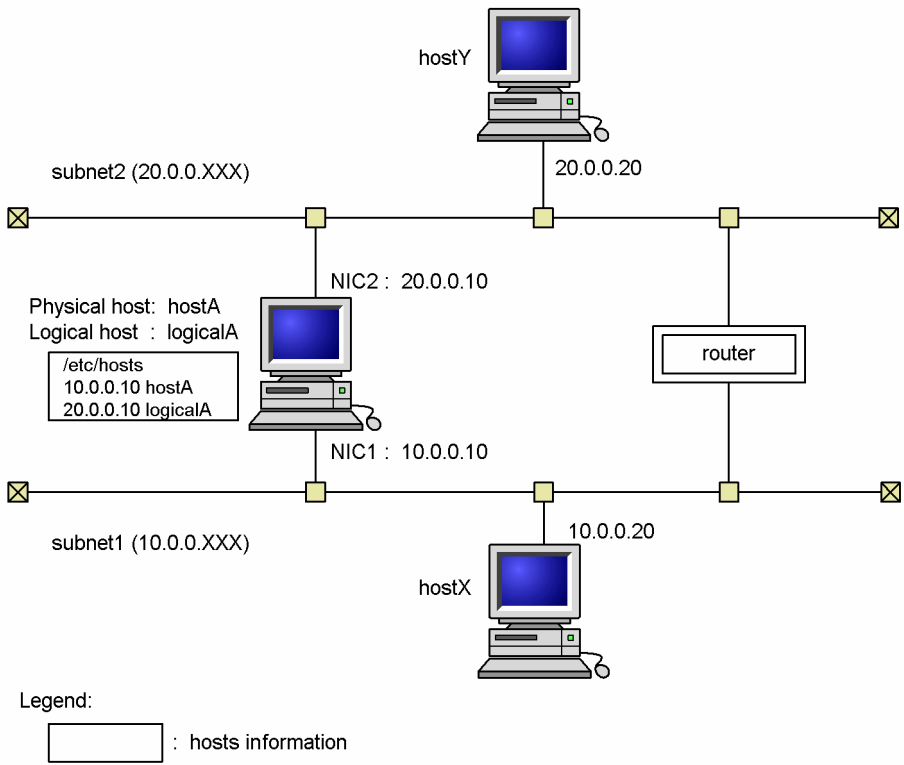
The physical host hostA is handled as a host within subnet1 and the logical host logicalA behaves as a host connected to subnet2 only. In this case, hostX in subnet1 can communicate with hostA, but not with logicalA. Similarly, hostY, which is in subnet2, can communicate with logicalA, but not with hostA. 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 6–3: 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 function is called *multi-LAN connectivity*. For details, see [6.5 Using JP1/Base in an environment of distinct networks \(with jp1hosts information\)](#) and [6.6 Using JP1/Base in an environment of distinct networks \(with jp1hosts2 information\)](#).

6.3 Setting up JP1/Base communication protocols

You can control the communication settings for JP1/Base independently from the system and other applications, allowing you to flexibly deal with various network configurations and operations. In JP1, this functionality is called *multiple LAN connections*.

By changing its communication protocol, you can use JP1/Base even when your network does not support routing or you do not want to allow communication between subnets.

6.3.1 Situations where the JP1/Base communication protocol must be changed

The communication protocol for JP1/Base needs to be changed when:

- You use JP1/Base on a host connected to multiple networks in a cluster configuration
- JP1/Base will communicate using multiple LANs in a cluster system environment with multiple LAN connections
- You want JP1/Base to communicate using a specific LAN in an environment with multiple LAN connections
- Multiple IP addresses are assigned in an environment with multiple LAN connections
- You want JP1/Base to communicate using a specific IP address in an environment with multiple LAN connections (a firewall is set up so that a specific IP address passes through)
- You create an environment of only physical hosts by deleting logical hosts from a cluster system (and changing to the ANY binding method)

You do not need to change the communication protocol if only physical hosts will be connecting to multiple networks.

6.3.2 Changing the JP1/Base communication protocol

You can change the communication protocol used by JP1/Base by applying the contents of communication protocol settings files to the common definition information.

You can specify the ANY binding method or IP binding method as the JP1/Base communication protocol.

(1) Procedure for changing the JP1/Base communication protocol

To apply the contents of a communication protocol settings file to the common definition information, execute the `jbssetcnf` command as follows:

```
jbssetcnf communication-protocol-settings-file
```

For details on the `jbssetcnf` command, see *jbssetcnf* in *15. Commands*.

(2) Communication protocol settings files

There are seven kinds of communication protocol settings file, each with a specific purpose.

File location:

In Windows: *installation-folder*\conf\

In UNIX: /etc/opt/jp1base/conf/

Table 6–1: Communication protocol settings files

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 to change the communication protocol for physical hosts that communicate over multiple LANs 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 to change the communication protocol for logical hosts that communicate over multiple LANs in a cluster system. You will need to edit this file.
physical_recovery_0651.conf	This file causes the communication protocol registered in the common definition information to revert back to the communication protocol used in version 06-51 or earlier. It is mainly used to change the communication protocol set for physical hosts back to the earlier communication protocol. The communication protocol used in version 06-51 or earlier does not support the IP binding method in an environment with multiple LAN connections.
logical_recovery_0651.conf	This file causes the communication protocol registered in the common definition information to revert back to the communication protocol used in version 06-51 or earlier. It is mainly used to change the communication protocol set for logical hosts back to the earlier communication protocol. You will need to edit this file. The communication protocol used in version 06-51 or earlier does not support the IP binding method in an environment with multiple LAN connections.
physical_anyany.conf	This file sets the ANY binding method for both sending and receiving. It is mainly used to return hosts that were operating in a cluster system to use only as physical hosts. Using this file changes the communication protocol of the physical hosts to the ANY binding method. Having done so, you can no longer use 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 with physical hosts to explicitly specify the sending IP address when going through a firewall, or to force a host to use a specific LAN. If you apply this setting to a host connected to multiple networks, the host will only be able to use one network.
logical_ipip.conf	This file sets the IP binding method for both sending and receiving. It is mainly used with logical hosts to explicitly specify the sending IP address when going through a firewall, or to force a host to use a specific LAN. You will need to edit this file. If you apply this setting to a host connected to multiple networks, the host will only be able to use one network.

For details about which JP1/Base features are compatible with the settings in each communication protocol settings file, see *H.9 Functionality supported in communication settings*.

For details on the parameters defined in the communication protocol settings file, see *H.10 Parameters defined in the communication protocol settings file*.

(3) Example of setting the JP1/Base communication protocol

To apply the contents of a communication protocol settings file to a physical host on a host connected to multiple networks, execute the `jbssetcnf` command as follows:

```
jbssetcnf physical_ipany.conf
```

To apply the contents of a communication protocol settings file to a logical host on a host connected to multiple networks, first open the `logical_ipany.conf` file in an editor. In *logical-host-name*\JP1BASE, enter the logical host name you specified when setting up the cluster system, and then execute the `jbssetcnf` command as follows:

```
jbssetcnf logical_ipany.conf
```

6.3.3 Specifying an ANY binding address

When ANY is set for the `JP1_BIND_ADDR` parameter in the common definition information, you can specify which version of the IP address to bind to the server. By doing so, you can force a host using the ANY binding method to use only IPv4 addresses or only IPv6 addresses for reception.

You can specify an ANY binding address for JP1/Base on the following operating systems:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Linux

(1) Procedure for specifying an ANY binding address

To apply an ANY binding address to the common definition information, execute the `jbssetcnf` command as follows:

```
jbssetcnf ANY-binding-address-settings-file
```

For details on the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

(2) ANY binding address settings files

An ANY binding address settings file specifies which IP address version to bind to the server.

File location:

In Windows Server 2016, Windows Server 2019, or Windows Server 2022: *installation-folder*\conf\

In Linux: `/etc/opt/jp1base/conf/`

Table 6–2: ANY binding address settings files

ANY binding address settings file	Purpose
<code>anybind_ipv4.conf</code>	Use this file to bind only IPv4 addresses to the server.
<code>anybind_ipv6.conf</code>	Use this file to bind only IPv6 addresses to the server.
<code>anybind_all.conf</code>	Use this file to bind IPv4 and IPv6 addresses to the server.

6.3.4 Checking the JP1/Base communication protocol

(1) Checking the JP1/Base communication protocol (on a physical host)

1. Execute the `jbsgetcnf` command as follows:

```
jbsgetcnf >config.txt
```

2. Open `config.txt` in a text editor.
3. Determine the communication protocol from the contents of the `[JP1_DEFAULT\JP1BASE]` key.

The following table shows the communication protocol corresponding to each value:

JP1_COM_VERSION	JP1_BIND_ADDR	JP1_CLIENT_BIND_ADDR	Communication protocol
0	Cannot be checked	Cannot be checked	The host is not configured with a communication protocol for multiple LAN connections.
1	ANY	ANY	<code>physical_anyany.conf</code> has been applied.
1	IP	ANY	<code>physical_ipany.conf</code> has been applied.
1	IP	IP	<code>physical_ipip.conf</code> has been applied.

(2) Checking the JP1/Base communication protocol (on a logical host)

1. Execute the `jbsgetcnf` command with the logical host specified.

```
jbsgetcnf -h logical-host-name >config.txt
```

Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up.

2. Open `config.txt` in a text editor.
3. Determine the communication protocol from the contents of the `[logical-host\JP1BASE]` key.

The following table shows the communication protocol corresponding to each value:

JP1_COM_VERSION	JP1_BIND_ADDR	JP1_CLIENT_BIND_ADDR	Communication protocol
0	Cannot be checked	Cannot be checked	The host is not configured with a communication protocol for multiple LAN connections.
1	IP	ANY	<code>logical_ipany.conf</code> has been applied.
1	IP	IP	<code>logical_ipip.conf</code> has been applied.

(3) Checking the ANY binding address setting

Check the common definition information by executing the `jbsgetcnf` command. For details on how to do so, see (1) *Checking the JP1/Base communication protocol (on a physical host)* and (2) *Checking the JP1/Base communication protocol (on a logical host)*.

The following table shows the ANY binding address setting corresponding to each value:

JP1_ANY_BIND	ANY binding address setting
IPv4	anybind_ipv4.conf has been applied.
IPv6	anybind_ipv6.conf has been applied.
ALL	anybind_all.conf has been applied.
Undefined [#]	Only an IPv4 address is bound to the server.

#:

This setting is undefined in new and upgrade installations.

6.3.5 Setting a duplicate communication protocol using IM configuration management

(1) Duplicate communication using IM configuration management

When a JP1/Base host communicates with another host by using the IM configuration management feature of JP1/IM - Manager, a TCP connection is established for a bidirectional `jp1bscom` service (port number = 20600/tcp) between the JP1/Base instances on the manager and agent hosts. A communication in which an agent connects to the manager is called a *duplicate communication*.

(2) Duplicate communication protocol

Duplicate communication uses the following two protocols:

- A communication protocol that connects to the IP address of the manager that was not resolved using name resolution (hereinafter called *the protocol without name resolution*)
- A communication protocol that connects to the IP address of the manager using name resolution (hereinafter called *the protocol with name resolution*)

If the protocol without name resolution is used, when the manager connects to an agent, the source IP address assigned to the manager is set as the destination IP address for duplicate communication. The protocol without name resolution is selected by default (as the initial setting after JP1/Base is installed).

(3) Selecting the duplicate communication protocol

Select the protocol with name resolution in the following cases:

- When the IP bind method is used for separated networks (when `physical_ipany.conf` or `logical_ipany.conf` is applied)
- When the address is converted (NAT) between the manager and agent hosts

(4) Setting the duplicate communication protocol

You can apply the protocol with name resolution by setting the common definition settings file (`jp1bscom_resultresolv_enable.conf`) on the manager host. `jp1bscom_resultresolv_enable.conf` is stored in the following directory:

In Windows:

installation-path\conf\ or *shared-directory*\conf\

In UNIX:

/etc/opt/jp1base/conf/ or *shared-directory/jp1base/conf/*

When you set the common definition settings file on the logical host, use an editor to open `jbscom_resultresolv_enable.conf`, and change the setting of `JP1_DEFAULT` to the logical host name specified for cluster setup on both the primary and secondary nodes.

To apply the protocol with name resolution:

1. Stop JP1/Base and the products that require JP1/Base as prerequisite software on the manager host.
2. Execute the `jbssetcnf` command on the manager host.

```
jbssetcnf jbscom_resultresolv_enable.conf
```

3. Start JP1/Base and the products that require JP1/Base as prerequisite software on the manager host.

If you change the protocol back to the one without name resolution, use the same procedure to set `jbscom_resultresolv_disable.conf`.

(5) Notes on the duplicate communication protocol

If you applied the protocol with name resolution, you must specify the settings that enable name resolution of the manager host name on the agent host. You must also set the IP address bound to the server by JP1/Base on the manager host as the primary IP address resolved from the name on the agent host. If you omit these settings, a communication error will occur when you use the IM configuration management to collect profile information, and collection of profile information will fail.

6.4 Setting JP1-specific hosts information

JP1/Base can keep its own set of hosts information, allowing it to perform name resolution independently of the OS. This dedicated hosts information is called *jp1hosts information* and *jp1hosts2 information*.

By setting `jp1hosts` or `jp1hosts2` information, JP1/Base can communicate using an IP address that does not correspond to a physical or logical host name on the destination host. For example, in an operating system that cannot natively resolve one host name to multiple IP addresses, you can define `jp1hosts` or `jp1hosts2` information that allows JP1/Base to resolve multiple IP addresses from a host name.

Using `jp1hosts2` information enables you to also manage IP address resolution for the event service in an integrated fashion. Also, when you use `jp1hosts2` information, restart of the services is not required when a connection destination is added. Therefore, we recommend that you use `jp1hosts2` information when you establish a new environment.

Note that `jp1hosts` information is supported in JP1/Base version 06-71 or later, and `jp1hosts2` information is supported in JP1/Base 10-00 or later.

6.4.1 When JP1-specific hosts information is required

There is no dedicated hosts information (`jp1hosts` or `jp1hosts2` information) in the system at installation of JP1/Base. This information should be set on a host-by-host basis as needed. Set `jp1hosts` or `jp1hosts2` information when:

- Using a host connected to multiple networks in a cluster system
 - JP1/Base cannot establish a connection with the IP address used to communicate with the destination host
 - You want to communicate using an IPv6 address
- To communicate using IPv6 addresses, set `jp1hosts2` information for the host in question. `jp1hosts` information does not support communication using IPv6 addresses.

For details about which JP1/Base features are compatible with `jp1hosts` and `jp1hosts2` information, see [H.9 Functionality supported in communication settings](#).

6.4.2 Setting JP1-specific hosts information

(1) Setting `jp1hosts` information

To apply `jp1hosts` information, edit the `jp1hosts` definition file and execute the `jbshostsimport` command to apply the file contents to the common definition information. For details, see [6.5.2 Defining `jp1hosts` information](#).

(2) Setting `jp1hosts2` information

To apply `jp1hosts2` information, edit the `jp1hosts2` definition file and execute the `jbshosts2import` command to apply the file contents to the common definition information. For details, see [6.6.2 Defining `jp1hosts2` information](#).

6.4.3 Behavior when both `jp1hosts` information and `jp1hosts2` information are defined

This section describes how name resolution is performed by JP1/IM - Manager, JP1/AJS3 - Manager, and JP1/Software Distribution in an environment where both `jp1hosts` information and `jp1hosts2` information are defined.

When a product for which JP1/Base is a prerequisite performs name resolution in an environment where both `jp1hosts` information and `jp1hosts2` information are defined, the product references only one of the definitions. This means that even if the product cannot find a definition of the host name to be resolved in `jp1hosts2` information, it does not reference `jp1hosts` information. Similarly, if the product cannot find a definition of the host name to be resolved in `jp1hosts` information, it does not reference `jp1hosts2` information.

(1) Products that reference `jp1hosts2` information (for example, JP1/IM - Manager and JP1/AJS3 - Manager)

A product that references `jp1hosts2` information (for example JP1/IM - Manager and JP1/AJS3 - Manager), will reference `jp1hosts2` information if you define `jp1hosts2` information in an environment where `jp1hosts` information is defined. In this case, `jp1hosts` information is no longer referenced. If `jp1hosts2` information is deleted, the product will reference `jp1hosts` information, which was originally defined.

In the sections that follow, an environment where specified `jp1hosts` information is ignored assumes an environment such as JP1/IM - Manager and JP1/AJS3 - Manager.

(2) Products that do not reference `jp1hosts2` information (for example, JP1/Software Distribution)

Products such as JP1/Software Distribution that utilize user authentication functionality of JP1/Base do not reference `jp1hosts2` information. Therefore, `jp1hosts` is referenced in an environment where both `jp1hosts` information and `jp1hosts2` information are defined. Even if you define `jp1hosts2` information in an environment where `jp1hosts` information is defined, `jp1hosts` definition is maintained in JP1/Software Distribution.

(3) Notes when both `jp1hosts` information and `jp1hosts2` information are defined

In an environment where both `jp1hosts` information and `jp1hosts2` information are defined, one of the definitions is referenced depending on the product. For details, check for each product.

When JP1-specific hosts information is used for name resolution, define `jp1hosts` information in JP1/Software Distribution, which does not reference `jp1hosts2` information. To define `jp1hosts` information in an environment in which `jp1hosts2` is defined, you need to specify the `-f` option when executing the `jbshostsimport` command. For details on the `jbshostsimport` command, see *jbshostsimport* in 15. *Commands*.

6.4.4 Differences between `jp1hosts` and `jp1hosts2` information

The following table describes how aspects of JP1/Base operation differ when using `jp1hosts` information and when using `jp1hosts2` information. `jp1hosts` information is defined for compatibility with JP1/Base Version 9 or earlier. If you establish a new environment, we recommend that you use `jp1hosts2` information.

Table 6–3: Differences between using `jp1hosts` and `jp1hosts2` information

No.	Item	<code>jp1hosts</code> information	<code>jp1hosts2</code> information
1	Restarting JP1/Base to apply the imported definitions	JP1/Base must be restarted each time you apply the file.	You do not need to restart JP1/Base when you add an IP address for another host.
2	Definitions for physical and logical hosts	Host definitions are required for physical and logical hosts.	Host definitions set for physical hosts are merged with those for logical hosts.
3	Application to logical hosts in a cluster system	The file contents need to be imported to the primary and secondary nodes.	The file contents need to be imported to the primary node only.
4	Registration in common definition information	The file contents are registered with the common definition information.	The file contents are not registered with the common definition information. The contents are saved as a binary file instead.
5	Maximum number of hosts	No limit.	Maximum of 10,000.
6	Length of single record in definition file	Maximum of 256 bytes.	No limit.
7	Importing a definition file without a host definition	Generates an error.	Results in a valid definition.
8	Import a definition file whose settings match the existing definition exactly	Results in a valid definition.	Generates an error.
9	IPv6 addresses	Cannot be set.	Can be set.
10	Communication with the event service	Partially unavailable.#	Possible.

#

Even if you set `<jp1hosts2>` in the address component of the `server` parameter in the API settings file (`api`), `jp1hosts` information cannot be viewed. To use `jp1hosts` information, as the communication settings for the event service, specify the conventional settings that were used until JP1/Base Version 9.

(1) Restarting JP1/Base to apply imported definitions

Each time you redefine `jp1hosts` information, you need to restart JP1/Base, products with JP1/Base as a prerequisite, and programs that have dependency relationships with JP1/Base.

When you add an IP address for a new host to `jp1hosts2` information, the change takes effect when you import the definition. You do not need to restart JP1/Base, products with JP1/Base as a prerequisite, and programs that have dependency relationships with JP1/Base on the manager host when you add an agent host to the network. A restart is required for all other definition changes.

(2) Definitions for physical and logical hosts

When using `jp1hosts` information, the host definitions used for name resolution must be set individually for each physical and logical host.

The `jp1hosts2` information on the physical host can merge with the `jp1hosts2` information on a logical host. This is called the *physical merge mechanism*, and is enabled by the `+PhysicalMerge` parameter in the `jp1hosts2` information for the logical host.

The `+PhysicalMerge` parameter is enabled by default. With the physical merge mechanism enabled, the host definitions in the `jp1hosts2` information for the physical host merge with the `jp1hosts2` information for the logical

host. This means that you do not need to specify a host definition for a logical host, except in circumstances where the logical host needs to resolve to a different IP address from the physical host where it resides.

For details on the `+PhysicalMerge` parameter, see *jp1hosts2 definition file* in *16. Definition Files*.

Notes on the physical merge mechanism

Note the following when `jp1hosts2` information is set for the physical host:

- `jp1hosts` information set for the logical host is ignored, and JP1/Base performs name resolution based on the `jp1hosts2` information defined for the physical host. This note does not apply to products that do not reference `jp1hosts2` information, in which case the specified `jp1hosts` information will not be ignored.
- If neither `jp1hosts` nor `jp1hosts2` information is set for a logical host, JP1/Base performs name resolution based on the `jp1hosts2` information defined for the physical host.

(3) Applying definitions to logical hosts in a cluster system

When you set `jp1hosts` information for a logical host in a cluster system, you need to import the definition information into the primary and secondary nodes.

When you set `jp1hosts2` information for a logical host in a cluster system, if you have imported the definition information to the primary node, there is no need to repeat the process at the secondary node.

(4) Registering definitions with common definition information

`jp1hosts` information is registered in the common definition information.

On the other hand, `jp1hosts2` information is not registered in the common definition information, but in binary files (`hostdb{0|1}.bin`). For details on the location of these files, see *A. List of Files and Directories*.

(5) Maximum number of defined hosts

There is no limit to the number of hosts you can define in `jp1hosts` information.

In `jp1hosts2` information, you can define a maximum of 10,000 hosts.

(6) Length of each record in the definition file

`jp1hosts` information limits the length of each record (line) in the definition file to 256 bytes.

In `jp1hosts2` information, there is no limit to the length of the records (lines) in the definition file.

(7) Importing definition files that do not contain host definitions

If you attempt to define `jp1hosts` information by importing a definition file in which no host definitions exist, an error occurs, the import process stops, and message KAVA0427-E is output.

On the other hand, when defining `jp1hosts2` information, the import process will proceed normally if you import a definition file in which no host definitions exist. This means that you can import a definition file containing nothing more than a `+DefaultResolve` or `+PhysicalMerge` parameter. You can also import a definition file containing no definitions at all. In this case, the default is set for all parameters.

(8) Importing a definition file that matches the existing definition

With `jp1hosts` information, if the definition file you import does not result in any changes to the existing `jp1hosts` information, the update process goes ahead in the usual way.

With `jp1hosts2` information, JP1/Base only imports the definition file if it would result in changes to the existing `jp1hosts2` information. If there are no changes, the import process stops and message KAVA0456-I is output. When importing a definition file to a logical host, the system uses the result of the physical merge mechanism to check whether the file would result in any changes.

(9) IPv6 addresses

You cannot use IPv6 addresses in `jp1hosts` information.

In `jp1hosts2` information, you can use IPv6 addresses. For details on how to configure JP1/Base to communicate using IPv6 addresses, see [6.11 Using JP1/Base in IPv6 environments](#).

(10) Communication with the event service

When you use `jp1hosts` information to resolve the name used for event service communication, specify the conventional settings that were used until JP1/Base Version 9. Specifically, you must explicitly specify the IP addresses for the `ports` and `remote-server` parameters in the event server settings file (`conf`) and for the `server` parameter in the API settings file (`api`).

In contrast, `jp1hosts2` information can be used to perform name resolution for communication with the event service. By default, a new installation of JP1/Base will use `jp1hosts2` information to communicate with the event service. To use `jp1hosts2` information in an overwrite installation, you need to modify the event server settings file (`conf`) and API settings file (`api`). For details on the changes you need to make, see [6.4.5 Migrating from `jp1hosts` information to `jp1hosts2` information](#).

6.4.5 Migrating from `jp1hosts` information to `jp1hosts2` information

In a new installation of JP1/Base, you can enable the use of `jp1hosts2` information by executing the `jbshosts2import` command. If you performed an overwrite installation, you need to reconfigure the environment from one that uses `jp1hosts` information to one that uses `jp1hosts2` information.

This section describes how to migrate from a `jp1hosts` environment to one that uses `jp1hosts2` information.

(1) Stop JP1/Base and products with JP1/Base as a prerequisite

Before migrating to `jp1hosts2` information, stop JP1/Base and products for which JP1/Base is a prerequisite. This allows you to modify the `jp1hosts` information and change the configuration of the event service.

(2) Migrate `jp1hosts` information to `jp1hosts2` information (in a system using `jp1hosts` information)

To migrate the definitions in `jp1hosts` information to `jp1hosts2` information:

For physical hosts

1. Execute the `jbshostsexport` command to acquire the `jp1hosts` information.

```
jbshostsexport > jp1hosts-definition-file-name
```

2. Define the information (standard output results) you acquired in step 1 in a `jp1hosts2` definition file (`jp1hosts2.conf`).
3. Execute the `jbshosts2import` command to import the `jp1hosts2` definition file (`jp1hosts2.conf`).

```
jbshosts2import -o file-defined-in-step-2
```

For logical hosts

1. Execute the `jbshostsexport` command to acquire the `jp1hosts` information.

```
jbshostsexport -h logical-host-name > jp1hosts-definition-file-name
```
2. Define the information (standard output results) you acquired in step 1 in a `jp1hosts2` definition file (`jp1hosts2.conf`).
3. Execute the `jbshosts2import` command to import the `jp1hosts2` definition file (`jp1hosts2.conf`).

```
jbshosts2import -h logical-host-name -o file-defined-in-step-2
```

Perform steps 2 and 3 on the logical host at the primary node.

If the import process would not result in changes to the existing `jp1hosts2` information, the message `KAVA0456-I` is output when you execute the `jbshosts2import` command in step 3, and the import process stops. This indicates that the necessary changes have already been made to the logical host, and the migration process is unnecessary.

(3) Modify the event server settings file (conf)

Change the communication settings of the event server so that it uses `jp1hosts2` information.

Specify `<jp1hosts2>` in the address component of the `ports` and `remote-server` parameters of the event server settings file (`conf`):

```
ports <jp1hosts2> jp1imevt jp1imevtapi  
remote-server event-server-name communication-type <jp1hosts2>
```

Also, delete the `client-bind` parameter from the file.

(4) Modify the API settings file (api)

Change the communication settings of application programs that connect to the event server, so that they use `jp1hosts2` information.

Specify `<jp1hosts2>` in the address component of the `server` parameter of the API settings file (`api`):

```
server event-server-name communication-type <jp1hosts2>
```

(5) Start JP1/Base

The environment when you start JP1/Base now uses `jp1hosts2` information containing the same definitions as the `jp1hosts` information that was in effect before the migration process.

6.4.6 Checking jp1hosts or jp1hosts2 information

You can determine whether a host is using `jp1hosts` information or `jp1hosts2` information from the output of the `jbshosts2export` command.

Execute the `jbshosts2export` command on both a physical host and a logical host to determine whether `jp1hosts2` information has been defined. If `jp1hosts2` information has not been defined, the message KAVA0470-I is output.

Table 6–4: Determining settings from output of `jbshosts2export` command

No.	Result of <code>jbshosts2export</code>		Current setting
	Physical host	Logical host	
1	Defined.	Defined.	All hosts are using <code>jp1hosts2</code> information.
2	Defined.	Not defined.	
3	Not defined.	Defined.	<ul style="list-style-type: none"> The physical host is using <code>jp1hosts</code> information, or the hosts and DNS settings of the operating system. The logical host is using <code>jp1hosts2</code> information.
4	Not defined.	Not defined.	All hosts are using <code>jp1hosts</code> information, or the hosts and DNS settings of the operating system.

For details on the `jbshosts2export` command, see *jbshosts2export* in *15. Commands*.

Notes

- Execution result of the `jbshosts2export` command applies only to products that reference `jp1hosts2` information, such as JP1/IM - Manager and JP1/AJS3 - Manager. Products that do not reference `jp1hosts2` information work by referencing `jp1hosts` information.
- For products that do not reference `jp1hosts2` information, such as JP1/Software Distribution, execute the `jbshostsexport` command to check the definition of `jp1hosts` information. For details on the `jbshostsexport` command, see *jbshostsexport* in *15. Commands*.
- When the setting for merging the `jp1hosts2` information on the physical host with the `jp1hosts2` information on the logical host is specified, make sure that the `jp1hosts2` information on the physical host can be used as the host definition for the logical host, and then merge it with the `jp1hosts2` information on the logical host. For details on the setting specified to merge the `jp1hosts2` information on the physical host with the `jp1hosts2` information on the logical host, see *6.4.4(2) Definitions for physical and logical hosts*.

6.5 Using JP1/Base in an environment of distinct networks (with jp1hosts information)

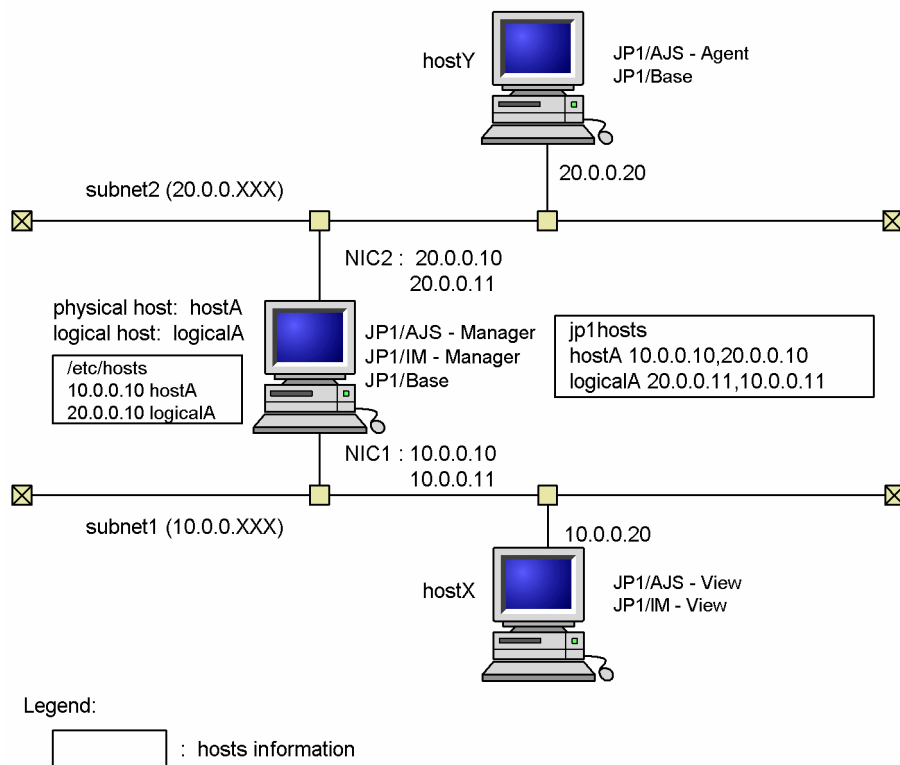
In this section, we discuss some issues when you use JP1/Base in an environment of distinct networks using multi-LAN connectivity. Then we describe how to configure the communication settings for this use.

The discussion in this section assumes an environment using `jp1hosts` information.

6.5.1 Issues when using JP1/Base in an environment of distinct networks (with jp1hosts information)

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, the user can log in to JP1/IM - Manager on `hostA` from JP1/IM - View on `hostX` to monitor `hostY` and to execute automated actions on `hostY`.

Figure 6–4: Example system configuration when using JP1/Base in an environment of distinct networks (with `jp1hosts` information)



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 when you change the communication settings, you need to restart JP1/Base, products for which JP1/Base is a prerequisite, and programs that have dependency relationships with JP1/Base.

(1) Whether you will adopt the JP1/Base communication protocol.

After installation, JP1/Base initially operates with the communication settings supported in version 06-71 or later. 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. In this case, you can define `jp1hosts` information that allows JP1/Base to resolve IP addresses.

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 `ifconfig` 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.

(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 6-4.

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`.

In general, if you set JP1/Base for use in a cluster system, both transmission and reception settings of the communication protocol are set to the IP binding method, except for an event service. Therefore, you need to change the transmission setting to the ANY binding method. To change the communication settings for JP1/Base, use the `jbssetcnf` command to apply the contents of the communication protocol settings file to the common definition information.

For details on communication protocols, see [6.3 Setting up JP1/Base communication protocols](#). For details on communications protocols in a cluster setup, see [H.12 Communication protocols in a cluster setup](#).

(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 (2) *Definition of `jp1hosts` information (for the main part of JP1/Base)* and (3) *Selection of communication protocol to transmit/receive data (for the main part of JP1/Base)*. For details, see [6.5.3 Changing communication settings of event services](#).

Note

If you set JP1/Base for use in a cluster system, `<jp1hosts2>` is specified in the `ports` and `remote-server` parameters of the event server settings file (`conf`) on the logical host. If `jp1hosts` information is used under that setting, the event service references `jp1hosts` information. However, if `<jp1hosts2>` is specified in the `server` parameter of the API setting file (`api`), programs that register and obtain JP1 events, such as a log file trapping function, do not reference `jp1hosts` information when connecting with an event service. Therefore, communication settings for the event service and for programs that register and obtain JP1 events might not match. Change communication settings to use `jp1hosts2` information, or change the communication settings for the event service to that used in V9 or earlier.

(5) Restart JP1/Base

When you change the communication settings, you need to restart JP1/Base, products for which JP1/Base is a prerequisite, and programs that have dependency relationships with JP1/Base.

6.5.2 Defining `jp1hosts` information

JP1/Base can hold its own hosts information, which enables resolution of IP addresses independently of the OS.

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`.

To register `jp1hosts` information with the common definition information:

1. Edit the `jp1hosts` definition file.

A `jp1hosts` definition file (`jp1hosts`) is provided by default. However, you cannot use this file without editing it first. If you create your own `jp1hosts` definition file, store it in the same folder as the default `jp1hosts` file. For details on the format of the `jp1hosts` definition file, see [*jp1hosts* definition file](#) in [16. 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} jplhosts-definition-file-name [-h logical-host-name]
```

Use the `jbshostsexport` command to check the `jplhosts` information registered with the common definition information. For details on these commands, see [15. Commands](#).

6.5.3 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 [16. Definition Files](#).

You need to set these parameters in the event server settings file (`conf`) 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 the event server settings file (`conf`) in a text editor or similar.

When editing an event server settings file (`conf`) file for a logical host, edit the file you 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 event server settings file (`conf`) does not already contain it. If the host is not being used in a cluster system, you can keep the default setting of the `ports` parameter, as follows:

```
ports 0.0.0.0 jplimevt jplimevtapi
```

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 jplimevt jplimevtapi
```

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 *16. Definition Files*.

6.5.4 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.

6.6 Using JP1/Base in an environment of distinct networks (with jp1hosts2 information)

This section discusses the use of JP1/Base in an environment of distinct networks using multi-LAN connectivity. It also describes how to configure the communication settings for this scenario.

The discussion in this section assumes an environment using `jp1hosts2` information.

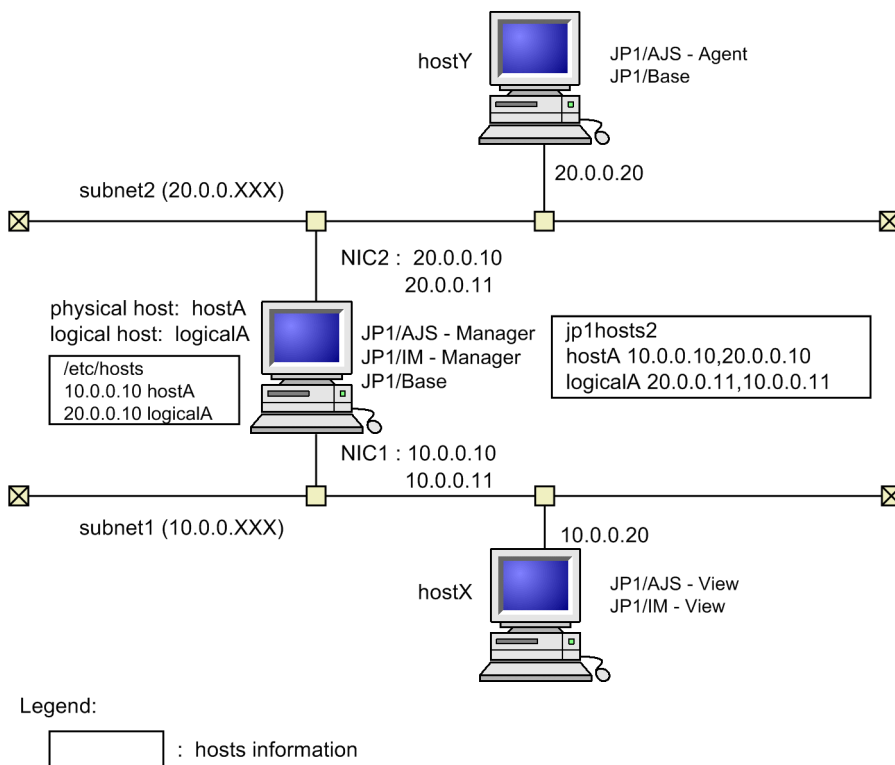
Note

Version 10-00 or later of JP1/Base must be installed on a host that uses `jp1hosts2` information.

6.6.1 Issues when using JP1/Base in an environment of distinct networks (with jp1hosts2 information)

This section discusses the use of JP1/Base in an environment of distinct networks, based on the system configuration example shown in the following figure. This example 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, the user can log in to JP1/IM - Manager on `hostA` from JP1/IM - View on `hostX` to monitor `hostY` and to execute automated actions on `hostY`.

Figure 6–5: Example system configuration when using JP1/Base in an environment of distinct networks (with `jp1hosts2` information)



Consider the following when configuring JP1/Base in such an environment:

- Whether you will use the JP1/Base communication protocol.
- How you will want to configure the communication settings of JP1/Base.

These communication settings determine how data other than JP1 events is exchanged between hosts. This includes data for user authentication, distribution of configuration definition information, and remote commands (for JP1/IM). The following two points are important in terms of the communication settings of JP1/Base:

- Definition of `jp1hosts2` information
- Selection of the communication protocols for sending and receiving data

In products such as JP1/IM - Manager and JP1/AJS3 - Manager that reference `jp1hosts2` information, if you define `jp1hosts2` information, definition of `jp1hosts` information is ignored. When you define `jp1hosts2` information, any `jp1hosts` information you had defined becomes invalid. If you add `jp1hosts2` to an environment that uses `jp1hosts` information, you need to migrate the environment from `jp1hosts` to `jp1hosts2` information. For details on how to do so, see [6.4.5 Migrating from `jp1hosts` information to `jp1hosts2` information](#).

When you add an IP address for a host (such as a newly added agent host) to `jp1hosts2` information, you do not need to restart JP1/Base, products for which JP1/Base is a prerequisite, and programs that have dependency relationships with JP1/Base. However, you do need to restart these products and programs if you change the communication settings of the event server or change the IP address of a local or remote host in the `jp1hosts2` information.

(1) Whether to adopt the JP1/Base communication protocol

After installation, JP1/Base initially operates with the communication settings supported in version 06-71 or later. First, consider whether to adopt the JP1/Base communication protocol.

(2) Required settings when performing overwrite installations from JP1/Base version 09-00 or earlier

When you perform an overwrite installation from JP1/Base version 09-00 or earlier, perform the following settings to adopt the JP1/Base communication protocol.

(a) Modify the event server settings file (`conf`)

To allow the event server to communicate using the communication protocol of JP1/Base, specify `<jp1hosts2>` in the address component of the `ports` and `remote-server` parameters of the event server settings file (`conf`), and delete the `client-bind` parameter from the file.

Before	After
<pre>ports hostA jplimevt jplimevtapi remote-server hostY close 20.0.0.20 client-bind 192.168.0.3</pre>	<pre>ports <jp1hosts2> jplimevt jplimevtapi remote-server hostY close <jp1hosts2></pre>

(b) Modify the API settings file (`api`)

To allow application programs to communicate with the event server using the communication protocol of JP1/Base, specify `<jp1hosts2>` in the address component of the `server` parameter of the API settings file (`api`).

Before	After
<pre>server hostA keep-alive 10.0.0.10</pre>	<pre>server * keep-alive <jp1hosts2></pre>

(3) Defining `jp1hosts2` information (for main part of JP1/Base)

Some OSs do not allow resolution of one host name into multiple IP addresses. If this is the case, you can define `jp1hosts2` information that allows JP1/Base to resolve IP addresses.

To allow physical and logical hosts to both use `subnet1` and `subnet2`, assign the IP addresses of the physical and logical hosts to both NICs (use the `ifconfig` command in UNIX). Then, define the assignments as the `jp1hosts2` information.

When you execute `ping logicalA` on `hostX`, the name might resolve to `20.0.0.11` in `subnet2`, preventing a connection from being established. You can avoid this issue by defining `jp1hosts2` information on `hostX`.

When you define `jp1hosts2` information for a physical host, the definition merges with that of the logical host. Only define an IP address in the `jp1hosts2` information for a logical host if you need the physical and logical hosts to resolve to different IP addresses.

(4) Selecting the communication protocols for sending and receiving data (for main part of JP1/Base)

When you use JP1/Base on a host connected to multiple networks in a cluster system, you need to change the communication protocol. This subsection briefly describes how to select the communication protocol based on Figure 6-5.

A host connected to multiple networks uses both physical and logical hosts. If you change the reception protocol to the ANY binding method, logical hosts might receive data intended for physical hosts and vice versa. For this reason, you must use the IP binding method as the reception protocol.

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`.

In general, if you set JP1/Base for use in a cluster system, both transmission and reception settings of the communication protocol are set to the IP binding method, except for an event service. Therefore, you need to change the transmission setting to the ANY binding method. To change the communication settings for JP1/Base, use the `jbsetcnf` command to apply the contents of the communication protocol settings file to the common definition information.

For details on communication protocols, see [6.3 Setting up JP1/Base communication protocols](#). For details on communications protocols in a cluster setup, see [H.12 Communication protocols in a cluster setup](#).

(5) Restart JP1/Base

When you change the communication settings of JP1/Base, you need to restart JP1/Base, products for which JP1/Base is a prerequisite, and programs that have dependency relationships with JP1/Base.

6.6.2 Defining `jp1hosts2` information

JP1/Base can keep its own set of hosts information, allowing it to perform name resolution independently of the OS.

Note

When you define `jp1hosts2` information, JP1/Base does not reference the definitions in the `hosts` file and DNS for the host names and IP addresses defined in the `jp1hosts2` information.

Example:

jp1hosts2 information:

```
hostA 100.0.0.10, 200.0.0.10
```

hosts file:

```
100.0.0.10 hostA hostB  
200.0.0.10 hostC
```

With these definitions, the `hosts` file is not referenced for `hostA` and the IP addresses `100.0.0.10`, and `200.0.0.10`.

To register `jp1hosts2` information:

1. Edit the `jp1hosts2` definition file.

A `jp1hosts2` definition file (`jp1hosts2.conf`) is provided by default. If you create your own `jp1hosts2` definition file, store it in the same folder as the default `jp1hosts2.conf` file. For details on the format of the `jp1hosts2` definition file, see *jp1hosts2 definition file* in *16. Definition Files*.

2. Execute the `jbshosts2import` command to register the file.

Execute the command as follows:

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name] [-h logical-host  
-name]
```

Use the `jbshosts2export` command to check the `jp1hosts2` information you registered. For details on the commands used in this section, see *15. Commands*.

Note

In products that reference `jp1hosts2` information, such as JP1/IM - Manager and JP1/AJS3 - Manager, if you define `jp1hosts2` information in an environment where `jp1hosts` information is already defined, the existing `jp1hosts` information becomes invalid. If you delete the `jp1hosts2` information (by executing the `jbshosts2import` command with the `-d` option specified), the `jp1hosts` information becomes valid again. However, this does not apply to products that do not reference `jp1hosts2` information, in which case definition of `jp1hosts` information will not become invalid.

6.6.3 Changing communication settings for event services

In versions 09-00 and earlier of JP1/Base, the event service was limited to the communication settings defined in the event server settings file (`conf`). However, from JP1/Base version 10-00, the event service can use the same communication settings as JP1/Base. In most circumstances, the same communication setting as JP1/Base can be used by following the procedures in *6.6.1 Issues when using JP1/Base in an environment of distinct networks (with jp1hosts2 information)*.

Although you can apply dedicated communication settings for the event server in the same way as in JP1/Base version 09-00 and earlier, you cannot use IPv6 addresses to communicate if you do so.

Note

The event service does not support the communication protocols of JP1/Base 06-51 or earlier, but does support communication protocols of JP1/Base 06-71 or later. For the differences between the communication settings of JP1/Base 06-51 or earlier and JP1/Base 06-71 or later, see *H.11 Differences between communication protocols of JP1/Base 06-51 or earlier and JP1/Base 06-71 or later*.

6.6.4 Restart JP1/Base as needed

JP1/Base must be restarted in the situations listed below. When you change the communication settings on a host, stop and restart JP1/Base, programs with JP1/Base as a prerequisite (such as JP1/IM and JP1/AJS), and programs that have dependency relationships with JP1/Base that are running on that host.

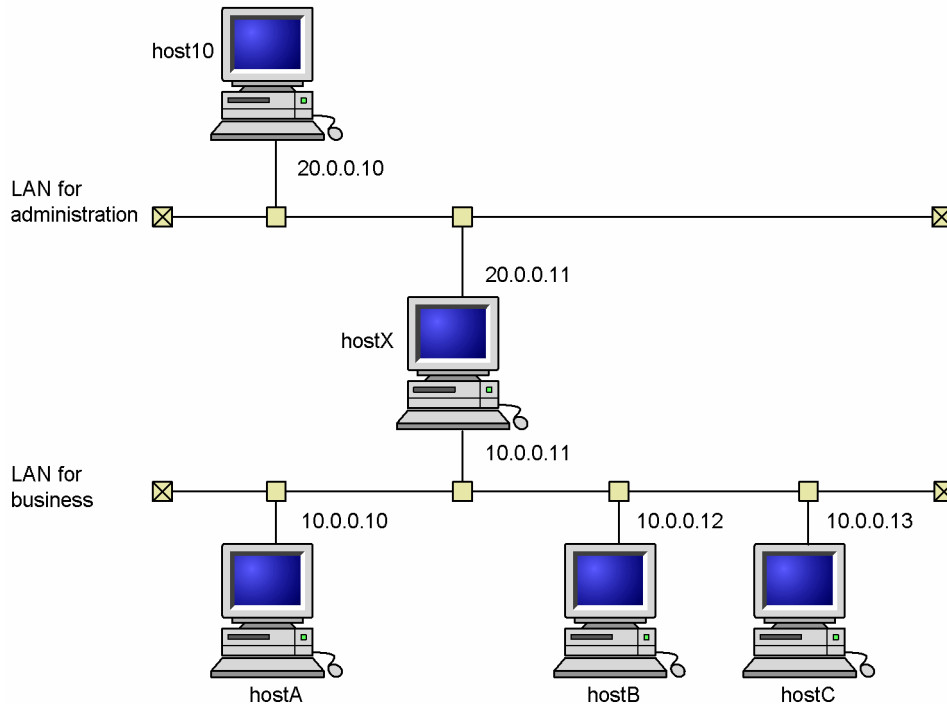
- You change the JP1/Base communication protocol
- You change the communication settings for the event service
- You change the IP address of the local host in the `jp1hosts2` information
- You change the IP address of a remote host with which JP1/Base is already communicating

You can find out whether you need to restart JP1/Base after changing `jp1hosts2` information by checking the information the `jbshosts2import` command outputs to standard output.

6.7 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 6–6: A system configuration example when JP1/Base is not used in a cluster system (in an environment of distinct networks)



6.7.1 Changing communication settings (with jp1hosts information)

This subsection describes how to change communication settings of each host.

The following table shows whether you need to change the communication settings for the hosts in the system configuration shown in Figure 6-6.

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

(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`).

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).

6.7.2 Changing communication settings (with `jp1hosts2` information)

This subsection describes how to change communication settings of each host.

The following table shows whether you need to change the communication settings for the hosts in the system configuration shown in Figure 6-6.

Host name	Communication settings of JP1/Base		Communication settings of event services (edit of <code>conf</code>)
	<code>jp1hosts2</code> information	Communication protocol settings	
host10	Required	Not required	Not required
hostX	Not required	Not required	Not required
hostA	Not required	Not required	Not required

Host name	Communication settings of JP1/Base		Communication settings of event services (edit of conf)
	jp1hosts2 information	Communication protocol settings	
hostB	Not required	Not required	Not required
hostC	Not required	Not required	Not required

(1) Changes required for host10

Unlike the other hosts, host10 connects to hostX with the IP address 20.0.0.11. This IP address does not correspond to the physical host name, which is hostX. You need to let JP1/Base recognize 20.0.0.11 as the IP address that corresponds to hostX. You can do this with the `jp1hosts2` definition file.

1. Edit the `jp1hosts2` definition file.

Edit the `jp1hosts2` definition file as follows:

```
# Associate the IP address 20.0.0.11 with hostX
hostX 20.0.0.11
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

This completes the communication settings for host10.

(2) Changes required for hostX

You do not need to change the communication setting for hostX.

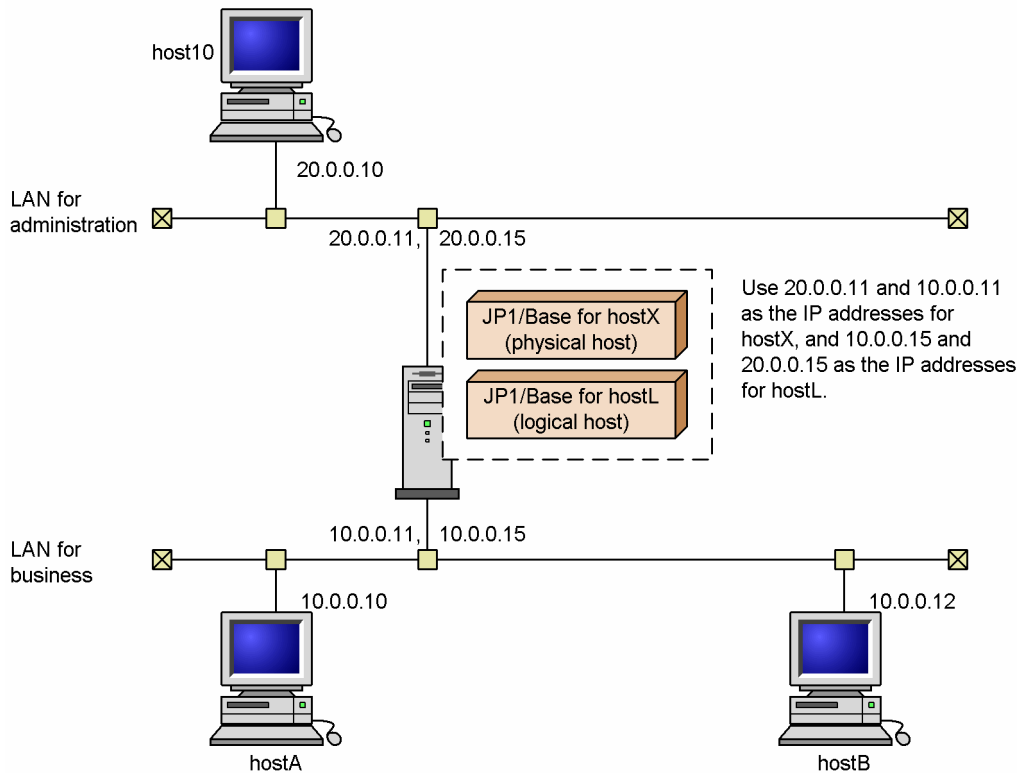
(3) Changes required for hostA, hostB, and hostC

You do not need to change the communication setting for hostA, hostB, and hostC, because they connect to hostX using the IP address 10.0.0.11, which corresponds to the physical host name (which is hostX).

6.8 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 6–7: A system configuration example when JP1/Base is used in a cluster system (in an environment of distinct networks)



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 (edit of conf)
	jp1hosts information	Communication protocol settings	
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

6.8.1 Changing communication settings (with jp1hosts information)

This subsection describes how to change communication settings of each host.

The following table shows whether you need to change the communication settings for the hosts in the system configuration shown in Figure 6-7.

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 (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

(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`).

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 (physical 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 `jplhosts` definition file.

Edit the `jplhosts` 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} jplhosts-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 jplimevt jplimevtapi  
client-bind 0.0.0.0
```

7. Edit the API settings file (`api`).

```
server hostX keep-alive 10.0.0.11
```

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 hostX.

(3) Changes required for hostL (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 `jplhosts` definition file.

Edit the `jplhosts` 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} jplhosts-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 jplimevt jplimevtapi
client-bind 0.0.0.0
```

8. Edit the API settings file (`api`).

9. `server hostL keep-alive 10.0.0.15`

10. Restart JP1/Base.

Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.



Note

In cluster operation, also perform steps 3 through 6, and 8, on the secondary logical host.

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.

6.8.2 Changing communication settings (with `jp1hosts2` information)

This subsection describes how to change communication settings of each host.

The following table shows whether you need to change the communication settings for the hosts in the system configuration shown in Figure 6-7.

Host name	Communication settings of JP1/Base		Communication settings of event services (edit of conf)
	jp1hosts2 information	Communication protocol settings	
host10	Required	Not required	Not required
hostX (physical host)	Required	Required	Not required
hostL (logical host)	Not required	Required	Not required
hostA	Not required	Not required	Not required
hostB	Not required	Not required	Not required

(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 recognize 20.0.0.11 and 20.0.0.15 as IP addresses that correspond to hostX and hostL. You can do this with the `jp1hosts2` definition file.

1. Edit the `jp1hosts2` definition file.

Edit the `jp1hosts2` definition file as follows:

```
# Associate the IP addresses 20.0.0.11 and 20.0.0.15 with the
# connection target hosts
hostX 20.0.0.11
hostL 20.0.0.15
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

This completes the communication settings for host10.

(2) Changes required for hostX (physical host)

1. Stop products for which JP1/Base is a prerequisite and which have dependency relationships with JP1/Base.
2. Stop JP1/Base.
3. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
# Associate the IP addresses with the host name
hostX 10.0.0.11, 20.0.0.11
hostL 10.0.0.15, 20.0.0.15
```

4. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

5. Execute the `jbssetcnf` command.

```
jbssetcnf physical_ipany.conf
```

6. Start JP1/Base again.

Also start products for which JP1/Base is a prerequisite and which have dependency relationships with JP1/Base.

This completes the communication settings for hostX.

(3) Changes required for hostL (logical host)

1. Stop products for which JP1/Base is a prerequisite and which have dependency relationships with JP1/Base.
2. Stop JP1/Base.

3. Edit `logical_ipany.conf`.

Open `logical_ipany.conf` in a text editor or similar, locate the `[LOGICALHOSTNAME\JP1BASE]` parameter, and change it to `[hostL\JP1BASE]`.

4. Execute the `jbssetcnf` command.

```
jbssetcnf logical_ipany.conf
```

5. Start JP1/Base again.

Also start products for which JP1/Base is a prerequisite and which have dependency relationships with JP1/Base.



Note

In cluster operation, apply the the common definition information of the logical host to the secondary node.

This completes the communication settings for hostL.

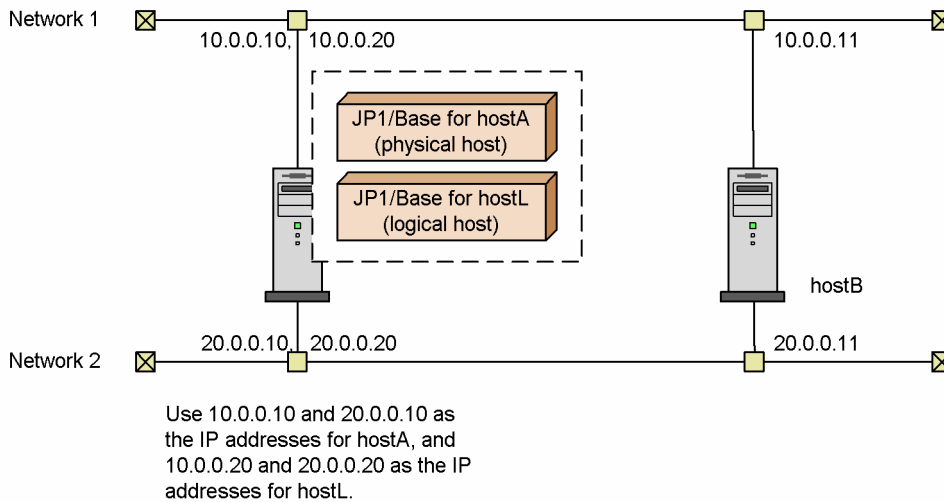
(4) Changes required for hostA and hostB

You do not need to change the communication setting for hostA and hostB because they connect to hostX and hostL with IP addresses that correspond to the physical and the logical host names.

6.9 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 6–8: System configuration example when using JP1/Base (within a specific network in an environment with multiple networks)



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.

6.9.1 Changing communication settings (with jp1hosts information)

This subsection describes changing the communication settings of the respective hosts.

The following table shows whether you need to change the communication settings for the hosts in the system configuration shown in Figure 6-8.

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

(1) Changes required for hostA (physical host)

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.

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.
2. Stop JP1/Base.

3. Edit the `jplhosts` definition file.

Edit the `jplhosts` 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} jplhosts-definition-file-name
```

5. Execute the `jbssetcnf` command.

```
jbssetcnf physical_ipip.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 jplimevt jplimevtapi
remote-server hostL close 20.0.0.20
```

7. Edit the API settings file (`api`).

Add the server parameters in the API settings file (`api`) as follows:

```
server hostA keep-alive 20.0.0.10
server hostL keep-alive 20.0.0.20
server hostB keep-alive 20.0.0.11
```

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 hostA.

(2) Changes required for hostL (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 `jplhosts` definition file.

Edit the `jplhosts` 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} jplhosts-definition-file-name -h hostL
```

5. Edit the `logical_ipip.conf`.

Open the `logical_ipip.conf` using a text editor, look for `[LOGICALHOSTNAME\JP1BASE]`, and change it to `[hostL\JP1BASE]`.

6. Execute the `jbssetcnf` command.

```
jbssetcnf logical_ipip.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 jplimevt jplimevtapi
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.



Note

In cluster operation, also perform steps 3 through 6, and 8, on the secondary logical host.

This completes the communication settings for `hostL` (a logical host).

(3) Changes 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 `jplhosts` definition file.

Edit the `jplhosts` 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} jplhosts-definition-file-name
```

5. Execute the `jbssetcnf` command.

```
jbssetcnf physical_ipip.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 jplimevt jplimevtapi
remote-server hostL close 20.0.0.20
```

7. Edit the API settings file (api).

Add the server parameters in the API settings file (api) as follows:

```
server hostA keep-alive 20.0.0.10
server hostL keep-alive 20.0.0.20
server hostB keep-alive 20.0.0.11
```

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 hostB.

6.9.2 Changing communication settings (with jp1hosts2 information)

This subsection describes changing the communication settings of the respective hosts.

The following table shows whether you need to change the communication settings for the hosts in the system configuration shown in Figure 6-8.

Host name	Communication settings of JP1/Base		Communication settings of event services (edit of conf)
	jp1hosts2 information	Communication protocol settings	
hostA (physical host)	Required	Required	Not required
hostL (logical host)	Not required	Required	Not required
hostB	Required	Required	Not required

(1) Changes required for hostA (physical host)

Set up the jp1hosts2 definition file so that JP1/Base on each host recognizes the correct IP address.

1. Stop products for which JP1/Base is a prerequisite and which have dependency relationships with JP1/Base.
2. Stop JP1/Base.
3. Edit the jp1hosts2 definition file.

Edit the file as follows:

```
# Associate 20.0.0.10 with hostA and 20.0.0.20 with hostL
hostA 20.0.0.10
hostB 20.0.0.11
hostL 20.0.0.20
```

4. Execute the jbshosts2import command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

5. Execute the `jbssetcnf` command.

```
jbssetcnf physical_ipip.conf
```

6. Restart JP1/Base.

Also restart products for which JP1/Base is a prerequisite and programs which have dependency relationships with JP1/Base.

This completes the communication settings for hostA.

(2) Changes required for hostL (logical host)

1. Stop products for which JP1/Base is a prerequisite and programs which have dependency relationships with JP1/Base.

2. Stop JP1/Base.

3. Edit `logical_ipip.conf`.

Open `logical_ipip.conf` in a text editor or similar, locate the `[LOGICALHOSTNAME\JP1BASE]` parameter, and change it to `[hostL\JP1BASE]`.

4. Execute the `jbssetcnf` command.

```
jbssetcnf logical_ipip.conf
```

5. Restart JP1/Base.

Also restart products for which JP1/Base is a prerequisite and programs which have dependency relationships with JP1/Base.



Note

In cluster operation, apply the the common definition information of the logical host to the secondary node.

This completes the communication settings for hostL (logical host).

(3) Changes required for hostB

1. Stop products for which JP1/Base is a prerequisite and programs which have dependency relationships with JP1/Base.

2. Stop JP1/Base.

3. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
# Associate 20.0.0.11 with hostB and 20.0.0.20 with hostL
hostB 20.0.0.11
hostL 20.0.0.20
```

4. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

5. Execute the `jbssetcnf` command.

```
jbssetcnf physical_ipip.conf
```

6. Restart JP1/Base.

Also restart products for which JP1/Base is a prerequisite and programs which have dependency relationships with JP1/Base.

This completes the communication settings for hostB.

6.10 Resetting JP1/Base to a single network after use on multiple networks

This section describes how to undo changes you made to the communication settings when moving to an environment of distinct networks. Use these procedures to return JP1/Base back to operation on a single network.

6.10.1 Resetting JP1/Base to single network use (with jp1hosts information)

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:

- If a logical host environment is present on the same host:

```
jbssetcnf physical_ipany.conf
jbssetcnf physical_recovery_0651.conf
```
- In an environment with only a physical host:

```
jbssetcnf physical_anyany.conf
```

For logical hosts, open the `logical_ipany.conf` and `logical_recovery_0651.conf` by using a text editor or similar, look for `[LOGICALHOSTNAME\JP1BASE]`, and then replace `LOGICALHOSTNAME` with the logical host name you specified when setting up the cluster system. Then execute the `jbssetcnf` command in the following format:

```
jbssetcnf logical_ipany.conf
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.

6.10.2 Resetting JP1/Base to single network use (with jp1hosts2 information)

1. Delete `jp1hosts2` information.

If you registered `jp1hosts2` information, delete it by executing the `jbshosts2import` command as follows:

```
jbshosts2import -d [-h logical-host-name]
```

2. Apply the communication protocol settings file to the common definition information.

Execute the `jbssetcnf` command to apply the file contents to the common definition information.

For a physical host, execute the `jbssetcnf` command as follows.

- If a logical host environment is present on the same host:
`jbssetcnf physical_ipany.conf`
`jbssetcnf physical_recovery_0651.conf`
- In an environment with a physical host only:
`jbssetcnf physical_anyany.conf`

For logical hosts, open the `logical_ipany.conf` and `logical_recovery_0651.conf` by using a text editor or similar, look for `[LOGICALHOSTNAME\JP1BASE]`, and then replace `LOGICALHOSTNAME` with the logical host name you specified when setting up the cluster system. Then, execute the `jbssetcnf` command as follows:

```
jbssetcnf logical_ipany.conf  
jbssetcnf logical_recovery_0651.conf
```

3. Restart JP1/Base.

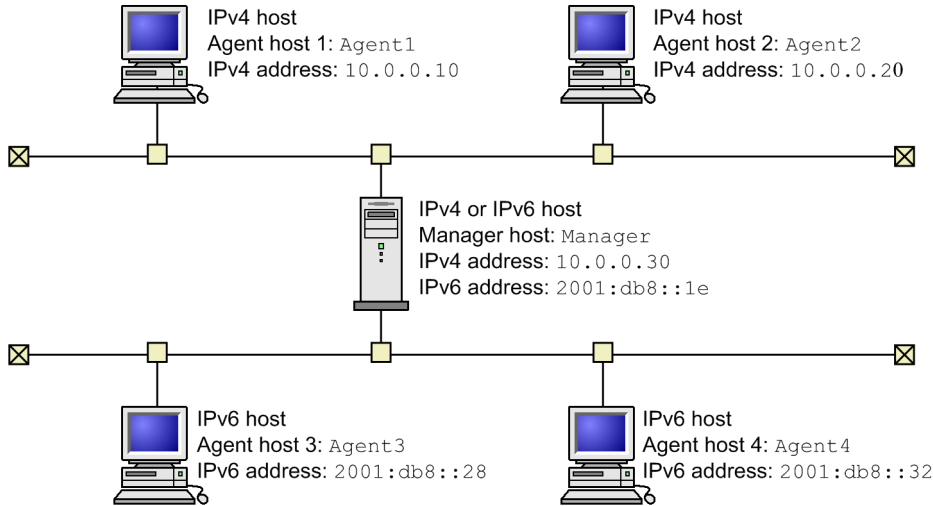
Also restart products for which JP1/Base is a prerequisite and programs which have dependency relationships with JP1/Base.

6.11 Using JP1/Base in IPv6 environments

This section describes the communication settings when using JP1/Base in an IPv6 environment.

An *IPv6 environment*, as shown in the figure below, is a network environment that incorporates hosts that communicate using IPv4 addresses, and hosts that communicate using IPv6 addresses.

Figure 6–9: Example system configuration in IPv6 environment



IPv4 host

A host to which only an IPv4 address is assigned.

IPv6 host

A host to which only an IPv6 address is assigned.

IPv4 or IPv6 host

A host to which both an IPv4 and an IPv6 address is assigned.

6.11.1 Prerequisites for an IPv6 environment

Manager host

- The host is an IPv4 or IPv6 host.
- The OS is Windows Server 2016, Windows Server 2019, Windows Server 2022 or Linux.

Agent hosts

- Each host is an IPv4 host, an IPv6 host, or an IPv4 or IPv6 host.
- The OS of IPv6 hosts and IPv4 or IPv6 hosts is Windows Server 2016, Windows Server 2019, Windows Server 2022, or Linux.

When communicating in an IPv6 environment, the connection source (agent host) must use the same version (type) of IP address as the connection destination (manager host).

You cannot use the following features in an IPv6 environment:

- IPv4-mapped addresses and IPv4-compatible addresses
- Devices that convert IPv4 addresses to IPv6 addresses and vice versa (protocol translators)

6.11.2 Communication settings when using JP1/Base in an IPv6 environment

The following describes how to change the communication settings when adding agent host 3 and agent host 4 to the system configuration shown in Figure 6-9.

The communication settings when communicating using IPv6 addresses in an IPv6 environment differ depending on whether you use the ANY binding method or the IP binding method.

(1) Changes required for ANY binding method

(a) Set the ANY binding addresses

When you specify the ANY binding addresses, choose one of the files to bind IP addresses to the servers.

- IPv6 addresses (`anybind_ipv6.conf`)
- IPv4 and IPv6 addresses (`anybind_all.conf`)

■ Examples

Settings required on the manager host:

1. Execute the `jbssetcnf` command with the `anybind_all.conf` file specified.

In Windows:

```
jbssetcnf installation-folder\conf\anybind_all.conf
```

In Linux:

```
jbssetcnf /etc/opt/jplbase/conf/anybind_all.conf
```

Settings required on agent host 3 and agent host 4:

1. Execute the `jbssetcnf` command with the `anybind_ipv6.conf` file specified.

In Windows:

```
jbssetcnf installation-folder\conf\anybind_ipv6.conf
```

In Linux:

```
jbssetcnf /etc/opt/jplbase/conf/anybind_ipv6.conf
```

(b) Set `jp1hosts2` information

In the `jp1host2` information for each host, set the IPv6 addresses of any destination hosts that use an IPv6 address. Also set the IPv6 address of the local host in the `jp1host2` information of each IPv6 host.

■ Examples

Settings required on the manager host:

1. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
Agent3 2001:db8::28
```

```
Agent4 2001:db8::32
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

Settings required on agent host 3:

1. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
Manager 2001:db8::1e
Agent3 2001:db8::28
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

Settings required on agent host 4:

1. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
Manager 2001:db8::1e
Agent4 2001:db8::32
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

(2) Changes required for IP binding method

(a) Set `jp1hosts2` information

In the `jp1host2` information for each host, set the IPv6 addresses of any destination hosts to communicate with using IPv6 addresses, and the IPv6 address of the local host.

■ Examples

Settings required on the manager host:

1. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
Manager 10.0.0.30 2001:db8::1e
Agent3 2001:db8::28
Agent4 2001:db8::32
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

Settings required on agent host 3:

1. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
Manager 2001:db8::1e
Agent3 2001:db8::28
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

Settings required on agent host 4:

1. Edit the `jp1hosts2` definition file.

Edit the file as follows:

```
Manager 2001:db8::1e
```

```
Agent4 2001:db8::32
```

2. Execute the `jbshosts2import` command.

```
jbshosts2import {-o|-r} [jp1hosts2-definition-file-name]
```

(3) Set `jp1hosts2` information and the `+DefaultResolve` parameter

The `+DefaultResolve` parameter in the `jp1hosts2` information specifies how the system resolves host names that are not defined in the `jp1hosts2` information. If you want JP1/Base to always use the hosts and DNS settings of the operating system to resolve IPv6 addresses, set 1 (resolve IPv4 and IPv6 addresses) as the value of the `+DefaultResolve` parameter.

However, when using JP1/Base in a network environment that contains IPv4 hosts and IPv6 hosts, we recommend that you define `jp1hosts2` information to make it clear which IP addresses are IPv6 addresses.

The default value of the `+DefaultResolve` parameter is 0 (resolve IPv4 addresses only). For this reason, you do not need to set the `+DefaultResolve` parameter if you specify the IP addresses of IPv6 hosts in the `jp1hosts2` information.

6.11.3 Checking IP addresses

When communicating in an IPv6 environment, the connection source (agent host) must use the same version (type) of IP address as the connection destination (manager host).

You can find out if the hosts are using the same type of IP address by checking whether the following IP addresses are the same type:

- The primary IP address of the connection destination resolved at the connection source
- The IP address of the local host resolved at the connection source
- The IP address of the local host resolved at the connection destination

The IP addresses resolvable for the local host at the connection source and the connection destination must include an IP address of the same type as the primary IP address resolved for the connection destination at the connection source.

The following describes how to check each IP address.

(1) Checking the primary IP address resolved for the connection destination at the connection source

At the connection source:

1. Execute the `jp1ping` command with the `-v` option and the name of the connection destination host specified.
2. Of the IP addresses resolved from the host name of the destination host, check the type of the IP address displayed first (the primary IP address).

(2) Checking the IP address resolved for the local host at the connection source

At the connection source:

1. Execute the `jp1ping` command with the local host name specified.

2. Identify the address type of the IP address resolved from the local host name.

(3) Checking the IP address resolved for the local host at the connection destination

At the connection destination:

1. Execute the `jplping` command with the local host name specified.
2. Identify the address type of the IP address resolved from the local host name.

6.12 Situations that require communication settings

This section describes the situations in which you need to enter communication settings in a definition file.

6.12.1 Situations that require communication settings for definition files

Situations (1) to (3) include those in which the host cannot be accessed using the IP address obtained by the operating system's name resolution process.

(1) When the OS cannot resolve the IP address of the connection destination host

In a `jp1hosts` definition file or `jp1hosts2` definition file, set the IP address used by JP1/Base at the connection destination host. For details on the `jp1hosts` definition file and the `jp1hosts2` definition file, see [jp1hosts definition file](#) and [jp1hosts2 definition file](#) in *16. Definition Files*.

(2) When the OS cannot resolve the IP address of the event server that receives JP1 events

When using `jp1hosts2` information, enter the IP address used by the destination event server in the `jp1hosts2` definition file.

When using `jp1hosts` information, enter the IP address used by the destination event server in the `remote-server` parameter of the event server settings file (`conf`). For details on the event server settings file, see [Event server settings file](#) in *16. Definition Files*.

(3) When the OS cannot resolve the IP address of an event server specified in an event search in JP1/IM - View

When using `jp1hosts2` information, enter the IP address used by the event server in the `jp1hosts2` definition file.

When using `jp1hosts` information, enter the IP address used by the event server in the `server` parameter of the API settings file (`api`). For details on the API settings file, see [API settings file](#) in *16. Definition Files*.

(4) When running JP1/Base services on a physical and logical host on the same host in a Windows environment

In a `jp1hosts` definition file or a `jp1hosts2` definition file, enter the IP address used by JP1/Base on the physical host.

(5) When setting up a cluster system

When using `jp1hosts` information, enter the IP address or host name of the physical host and logical host in the `ports` parameter of the event server settings file (`conf`). For the physical host, we recommend that you specify an IP address.

(6) When you want to communicate using multiple LANs in a cluster system in an environment with multiple LAN connections

Configure the communication settings as follows:

- Enter the IP address of the local host in a `jp1hosts` definition file or a `jp1hosts2` definition file.
- Apply the contents of the following communication protocol files to the common definition information:
 - For a physical host environment: `physical_ipany.conf`
 - For a logical host environment: `logical_ipany.conf`Open the file in an editor, locate the `[LOGICALHOSTNAME\JP1BASE]` parameter, and replace it with `[logical-host-name\JP1BASE]`.

For details on the communication protocol files, see [6.3.2\(2\) Communication protocol settings files](#).

- When using `jp1hosts` information, enter the IP address of the local event server in the `ports` parameter of the event server settings file (`conf`).
- When using `jp1hosts` information, specify `0.0.0.0` in the `client-bind` parameter of the event server settings file (`conf`).

(7) When you want to communicate using a specific LAN in an environment with multiple LAN connections

Configure the communication settings as follows:

- Enter the IP address of the local host in a `jp1hosts` definition file or a `jp1hosts2` definition file.
- Apply the contents of the following communication protocol files to the common definition information:
 - For a physical host environment: `physical_ipip.conf`
 - For a logical host environment: `logical_ipip.conf`Open the file in an editor, locate the `[LOGICALHOSTNAME\JP1BASE]` parameter, and replace it with `[logical-host-name\JP1BASE]`.
- When using `jp1hosts` information, enter the IP address of the local event server in the `ports` parameter of the event server settings file (`conf`).
- When using `jp1hosts` information, specify the destination IP address for JP1 events in the `client-bind` parameter of the event server settings file (`conf`).

(8) When you want to connect to the event server using a specific LAN in an environment with multiple LAN connections

Enter the IP address to use to connect to the event server in the `client` parameter of the API settings file (`api`).

(9) When you want to delete a logical host from a cluster system and revert to an environment of physical hosts only

Configure the communication settings as follows:

- When you apply the communication protocol settings file (`physical_anyany.conf`) to the common definition information, the communication protocol reverts to the ANY binding method.

- When using `jp1hosts` information, specify `0.0.0.0` in the `ports` parameter of the event server settings file (`conf`).
- When using `jp1hosts` information, delete the `client-bind` parameter from the event server settings file (`conf`).
- Delete the `jp1hosts` definition file or `jp1hosts2` definition file as needed.

(10) You specify an IP address in the `ports` parameter of the event server settings file that is not the one obtained by the OS's name resolution process

In the `server` parameter of the API settings file (`api`), enter the IP address specified in the `ports` parameter of the event server settings file.

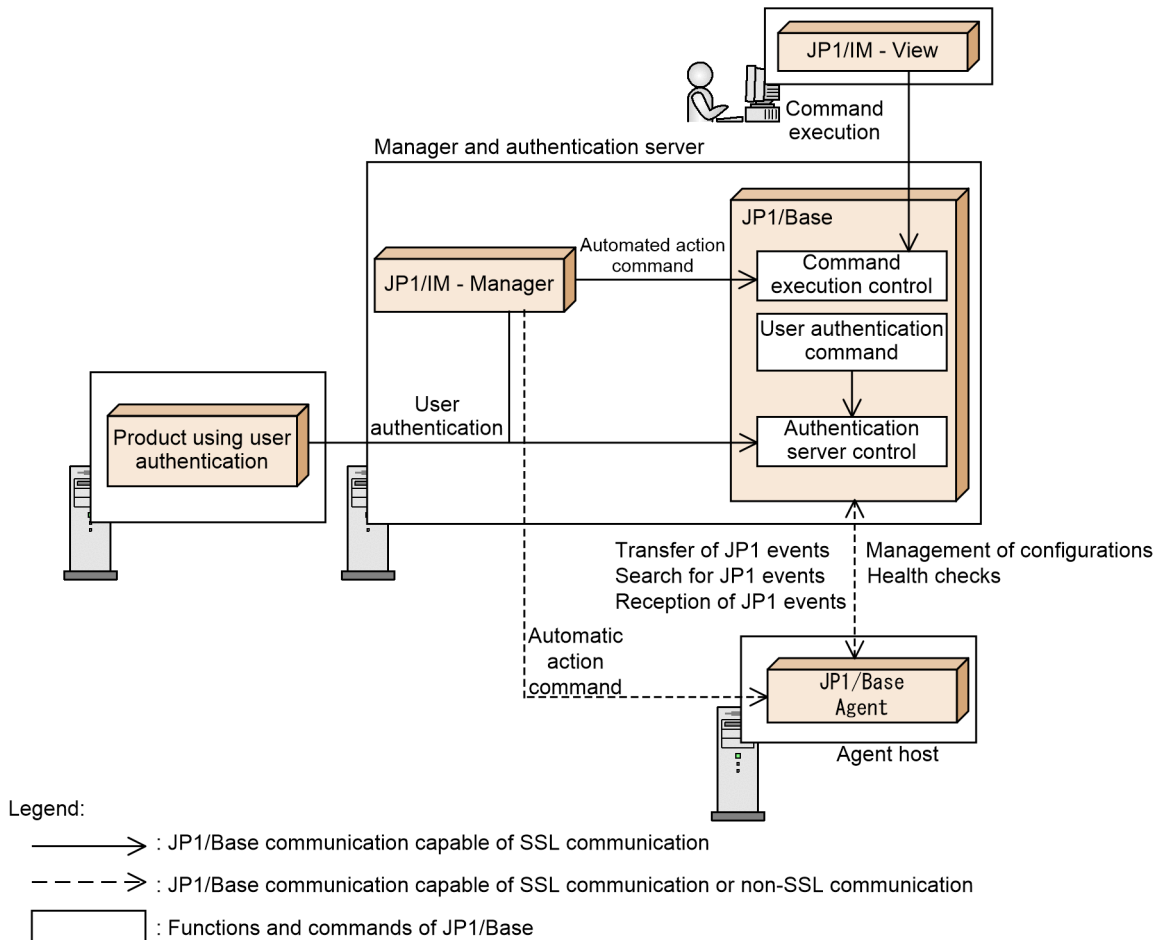
6.13 Communication encryption in JP1/Base

JP1/Base can encrypt communication through SSL during the following communications:

- Communication associated with an authentication server (user authentication)
 - Communication for user authentication between products using JP1/Base user authentication and an authentication server
 - Communication for commands[#] related to JP1/Base user authentication
[#] Commands related to JP1/Base user authentication are as follows:
`jbsadduser, jbschgpasswd, jbsrmuser, jbslistuser, jbsaclreload, jbslistacl, jbssetacl, jbsrmacl`
- Communication associated with command execution by JP1/IM
 - Communication for automated action between JP1/IM - Manager and JP1/Base on a manager host
 - Communication for command execution between JP1/IM - View and JP1/Base on a manager host
- Communication associated with the monitoring of agent hosts
 Transfer of JP1 events, search for JP1 events, reception of JP1 events, automatic action, execution of commands, management of configurations, and health checks performed between the manager host's JP1/IM - Manager and JP1/Base and the agent host's JP1/Base

The following figure shows an overview of JP1/Base communication capable of SSL communication.

Figure 6–10: JP1/Base communication capable of SSL communication



Note that to use SSL communication, the version of JP1/Base on the host (server side) at the connection destination and the hosts (client side) connecting to that host must be 11-00 or later. (When communication associated with agent host monitoring is to be encrypted, the version of JP1/Base on these hosts must be 12-10 or later.)

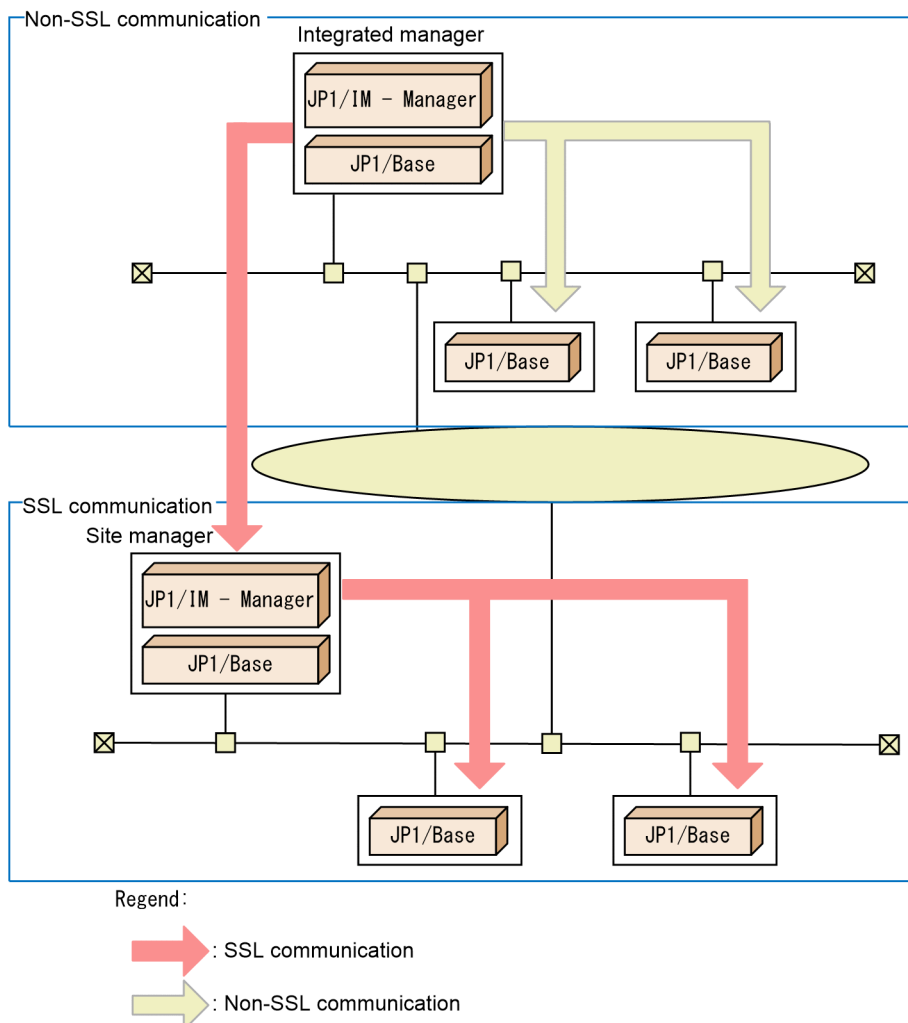
Note on using SSL communication on an authentication server (user authentication)

If SSL communication is enabled on an authentication server host, SSL communication must also be enabled on each host that connects to that authentication server. If hosts that do not use SSL communication must be authenticated, you need to install an authentication server that does not use SSL communication to separate the user authentication block.

Furthermore, if you set hosts that do not support SSL communication in the non-SSL communication host configuration file (`jp1bs_nosslhost.conf`), communication associated with the monitoring of agent hosts can take place in accordance with the SSL communication settings of the agent host. For details on the non-SSL communication host configuration file, see *Non-SSL communication host configuration file* in 16. *Definition Files*.

The following figure shows an example of a system configuration where both SSL communication and non-SSL communication take place.

Figure 6–11: Example of a system configuration where both SSL communication and non-SSL communication take place



In this example, the integrated manager uses non-SSL communication to access the instances of JP1/Base located within the same LAN. On the other hand, to access a site manager or the instances of JP1/Base located within the same LAN as the site manager, the integrated manager uses SSL communication.

6.13.1 Files required for SSL communication

To use SSL communication, you need to prepare files required for SSL communication on the server host and client hosts. Files required for SSL communication are described below.

Files required for SSL communication on the server host:

- Private key
- Server certificate issued by CA (certificate authority)
- Root certificate corresponding to the server certificate

Files required for SSL communication on the client hosts:

- Root certificate corresponding to the server certificate on the server side

The following figure shows the relationship of certificates required for SSL communication.

Figure 6–12: Relationship diagram of certificates required for SSL communication (for an authentication server (user authentication))

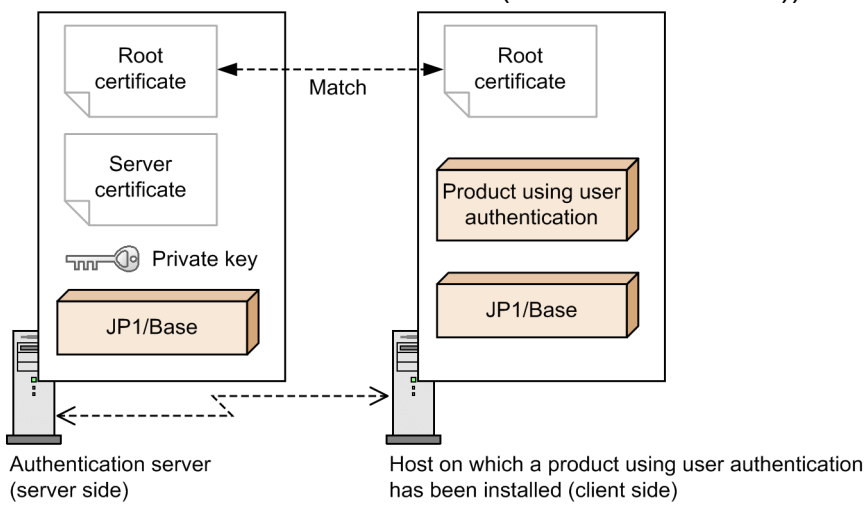


Figure 6–13: Relationship diagram of certificates required for SSL communication (for command execution by JP1/IM)

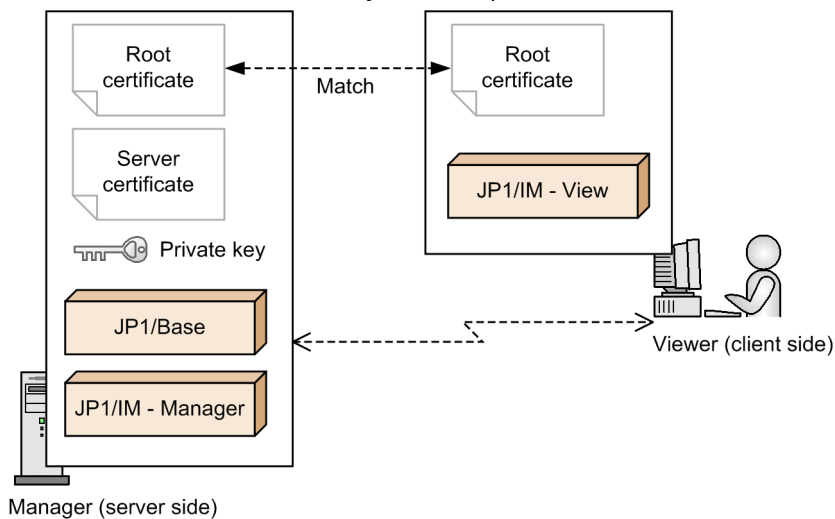
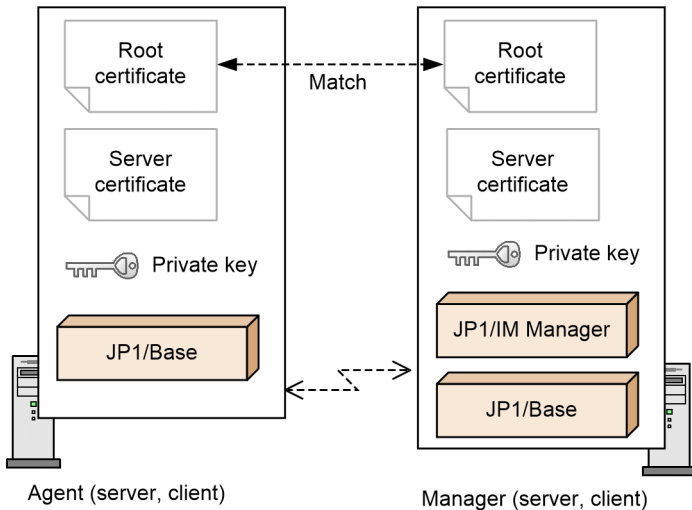


Figure 6–14: Relationship diagram of certificates required for SSL communication (for monitoring an agent host)



For details about the communication encryption function (SSL communication) of JP1/IM, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

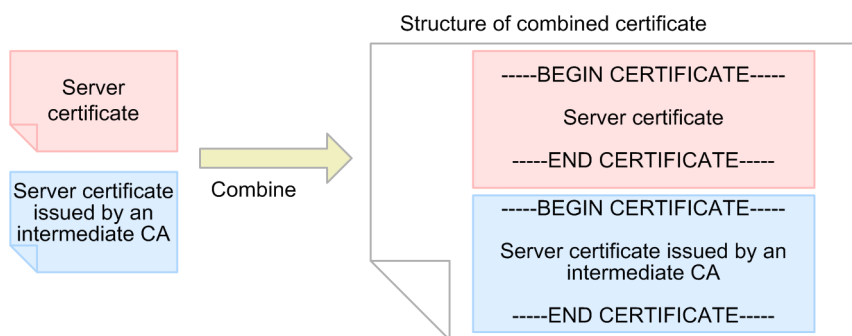
(1) Notes on private keys, server certificates, and root certificates

- Use of private keys with a passphrase is prohibited. Remove a passphrase before using a private key.
- Only private keys, server certificates, and root certificates in X509 PEM format can be used.
- Certificates (wildcard certificates) in which a wildcard is used for the CN host name can also be used for server certificates.

Example: `CN=*.example.com`

- To use a server certificate issued by an intermediate CA, you need to combine certificates according to the hierarchical structure of certificates.

Combine certificates according to the following hierarchical structure:



To use a cross root certificate, you must combine certificates in the following order:

1. Server certificate
2. Server certificate issued by an intermediate CA
3. Cross root certificate

6.13.2 Setting up an SSL communication environment on the server side

This subsection describes how to create a private key required on the server side for using SSL communication, and how to issue a server certificate and root certificate. The procedure is as follows:

1. Creating a private key
2. Creating a CSR (certificate signing request)
3. Issuing a server certificate and root certificate
4. Locating the private key, server certificate, and root certificate

Use commands of OpenSSL to create a private key and CSR. For details about the commands, see *openssl* in 15. *Commands*.

(1) Creating a private key

1. Execute the `openssl` command to create a private key.

An example of command execution is as follows:

When using elliptic-curve cryptography (ECC)

```
openssl ecparam -genkey -noout -name cipher-name# -out private-key-file-name
```

#

The length of the private key created varies based on the cipher name. For details, see the description of `openssl-ecparam` on the official OpenSSL website.

When using RSA encryption

Create a 2,048-bit private key.

```
openssl genrsa -out private-key-file-name
```

(2) Converting the private key (only when using elliptic-curve cryptography)

1. Convert the private key using the `openssl pkcs8` command.

When using elliptic-curve cryptography, convert the private key to PKCS#8 format. A command execution example is provided below.

```
openssl pkcs8 -topk8 -in private-key-file-name -out PKCS#8-type-private-key-file-name -nocrypt
```

(3) Creating a CSR (certificate signing request)

1. Execute the `openssl req` command to create a CSR.

Create a CSR with the created private key (when using elliptic-curve cryptography, this is the private key created before being converted into PKCS#8 format) specified. In the following example of command execution, a CSR for a certificate whose effective period is one year is created.

```
openssl req -new -days 365 -key private-key-file-name -out CSR-file-name
```

2. Enter the DN (distinguished name) to be registered in the certificate interactively.

Input example of the command prompt window:

```

C:\Program Files (x86)\Hitachi\JP1Base\ssl_\32mt\bin>openssl req -new -days 365 -key server.key -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Yokohama
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi
Organizational Unit Name (eg, section) []:JP1
Common Name (e.g. server FQDN or YOUR name) []:hostjp1.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

```

The CSR is created.

(4) Requesting the issuance of a server certificate and root certificate

Submit the created CSR to the CA (certificate authority) to request the CA to issue a server certificate and root certificate.

(5) Locating the private key, server certificate, and root certificate

Store the private key, server certificate, and root certificate in a folder on the server side. If monitoring an agent host in an environment where the communication encryption function (SSL communication) for JP1/Base 12-10 or later is enabled, a private key, server certificate, and root certificate are required not only for the manager host but also for the agent host.

Note that you must match the storage location and file name of each file to those defined in the SSL communication definition file created in [6.13.4 Setting up the communication encryption function of JP1/Base](#).

6.13.3 Setting up an SSL communication environment on the client side

Store the root certificate issued in [6.13.2\(4\) Requesting the issuance of a server certificate and root certificate](#) in a folder on the client side.

Note that you must match the storage location and file name of the file to those defined in the SSL communication definition file created in [6.13.4 Setting up the communication encryption function of JP1/Base](#).

6.13.4 Setting up the communication encryption function of JP1/Base

Set up the communication encryption function of JP1/Base. You must specify settings such as whether to enable SSL communication and the file names of a server certificate and root certificate for the communication encryption function. This setup is required in JP1/Base on the server and client sides.

To set up the communication encryption function:

1. Create an SSL communication definition file (`jp1bs_ssl.conf`).

Define the SSL communication settings information such as whether to enable SSL communication, the file name of a server certificate, and the storage location of a root certificate in the SSL communication definition file. For details about the SSL communication definition file, see *SSL communication definition file* in 16. *Definition Files*.

2. Execute the `jbssetcnf` command.

```
jbssetcnf jp1bs_ssl.conf
```

The information of the SSL communication definition file is registered in the common definition information. For details about the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

3. Restart JP1/Base.

The settings of the common definition information will take effect.

Note:

- You cannot change the settings of the communication encryption function while JP1/Base is running. Before changing the settings of the communication encryption function (to replace the server certificate or root certificate due to expiration), stop JP1/Base.
- Even if you upgrade from the environment in which the communication encryption function (SSL communication) provided by JP1/Base 11-00 or later is enabled, the communication encryption function (SSL communication) supported by 12-10 does not get enabled. To enable SSL communication, add `jp1bsagent` to `BASESSL` in the SSL communication definition file, and then restart JP1/Base.

6.13.5 Notes on using event services

Suppose that the communication encryption function provided by JP1/Base is enabled in your environment. For SSL communication to be used for event services that take place between the local host acquiring JP1 events and the host to which the acquired JP1 events are transferred in this environment, one physical host or logical host must be up and running. If a host other than a physical host is up and running, specify the host of event services in the API settings file for event services.

For details on how to specify the host of event services, see *API settings file* in 16. *Definition Files*.

7

Startup and Termination

This chapter describes how to start and stop JP1/Base.

7.1 Starting and stopping JP1/Base (in Windows)

The following table lists the services provided in the Windows version of JP1/Base.

Table 7–1: 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
Hitachi Network Objectplaza Trace Library (HNTRLib2) 64bit	Hitachi Network Objectplaza Trace Monitor 2 (x64)
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 Services dialog box, do not change the **Log On As** setting from 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.

7.1.1 Starting services

In Windows, the following services are registered as **Automatic** by default and configured to start automatically when the system starts.

- Hitachi Network Objectplaza Trace Monitor 2 (Hitachi Network Objectplaza Trace Library)
- Hitachi Network Objectplaza Trace Monitor 2 (Hitachi Network Objectplaza Trace Library for 64bit)
- 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.

By default, the following services are configured 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 [9. 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.

When using in October 2034 or later

The JP1/Base command execution service (process) cannot be used from October 2034 onwards. Therefore, by the end of September 2034, you must perform the following procedure to change the settings. The change will prevent the command execution service (process) from starting.

1. Check the status of the JP1/Base startup process.

A different configuration procedure is used based on whether the authentication server is running. With JP1/Base started, execute the `jbs_spmd_status` command to confirm whether the authentication server has been started. If `jbsessionmgr` is listed in the information shown after the command is executed, the authentication server is running.

2. Copy the model file of the 2038-compliant startup process definition file to create a startup process definition file.

If the authentication server has not been started:

```
copy installation-folder\conf\jp1bs_spmd.conf.2038_model installation-  
folder\conf\jp1bs_spmd.conf
```

If the authentication server has been started:

```
copy installation-folder\conf\jp1bs_spmd.conf.session.2038_model installation-  
folder\conf\jp1bs_spmd.conf
```

3. Start or restart JP1/Base.

Start JP1/Base to apply the settings. If JP1/Base is already running, restart JP1/Base.

4. Check that the command execution service (process) is not running.

Execute the `jbs_spmd_status` command and confirm that the command execution service (process) is not running. If `jcocmd` is not included in the information shown when the command is executed, the command execution service (process) is not running.

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 *16. Definition Files*.
- The JP1/Base service may not start properly if the `jbs_spmd_status`, `jbs_spmd_reload`, or `jbs_spmd_stop` command is executed while the service is starting. Do not execute any of these commands while the JP1/Base service is starting.

- Upon the startup of the authentication server, password policy definitions are checked. When there is a mistake in the definitions, the authentication server starts up assuming that the default values, which are applied when the parameters are omitted, are set for the parameters.

7.1.2 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 service is configured to start services other than the Hitachi Network Objectplaza Trace Monitor 2 and JP1/Base EventlogTrap services. For details on the startup control, see [9. Setting the Service Start and Stop Sequences \(Windows Only\)](#). For details on how to start services without using the startup control, see [7.1.1 Starting services](#).

7.1.3 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 [9. Setting the Service Start and Stop Sequences \(Windows Only\)](#).

If you want to terminate each service without using JP1/Base Control Service (startup control) or JP1/Power Monitor, do so from the Services dialog box under the Control Panel.

If you want to terminate the event service (JP1/Base Event), first terminate the process management (JP1/Base), including user management; the log file trap management service (JP1/Base LogTrap); and the event log trapping service (JP1/Base Eventlog Trap). Then, terminate the event service.

7.2 Starting and stopping JP1/Base (in UNIX)

On a UNIX system, you can start and stop services using commands.

Table 7–2: 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#5#6}	jbs_stop.model ^{#4#5#6}

#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 `jbs_stop.model` command after you execute `jevlogdstop`.

#5: `jbs_start.model` and `jbs_stop.model` are configured according to the encoding that was set in the LANG environment variable during installation. To use the commands with a different language to start and stop JP1/Base, change the configuration by using the following steps, rather than editing the model files:

1. Copy `jbs_start.model` and `jbs_stop.model` as files with different names.
2. Edit the copied files to change the LANG environment variable.

The LANG environment variable must be configured according to the language that is specified in `jp1bs_env.conf` and `jp1bs_param.conf`.

#6: If you change the LANG environment variable in `jbs_start.model` and `jbs_stop.model`, your changes are reset during an overwrite installation of JP1/Base. To prevent this, change the LANG environment variable by using steps described in #5.

For details on the above commands, see [15. Commands](#).

When using in October 2034 or later

The JP1/Base command execution service (process) cannot be used from October 2034 onwards. Therefore, by the end of September 2034, you must perform the following procedure to change the settings. The change will prevent the command execution service (process) from starting.

1. Check the status of the JP1/Base startup process.

A different configuration procedure is used based on whether the authentication server is running. With JP1/Base started, execute the `jbs_spmd_status` command to confirm whether the authentication server has been started. If `jbsessionmgr` is listed in the information shown after the command is executed, the authentication server is running.

2. Copy the model file of the 2038-compliant startup process definition file to create a startup process definition file.

If the authentication server has not been started:

```
cp -p /etc/jp1base/conf/jp1bs_spmd.conf.2038_model /etc/opt/jp1base/conf/jp1bs_spmd.conf
```

If the authentication server has been started:

```
cp -p /etc/jp1base/conf/jp1bs_spmd.conf.session.2038_model /etc/opt/jp1base/conf/jp1bs_spmd.conf
```

3. Start or restart JP1/Base.

Start JP1/Base to apply the settings. If JP1/Base is already running, restart JP1/Base.

4. Check that the command execution service (process) is not running.

Execute the `jbs_spm�_status` command and confirm that the command execution service (process) is not running. If `jcocmd` is not included in the information shown when the command is executed, the command execution service (process) is not running.

Note

JP1/Base may not start properly if the `jbs_start` or `jbs_start.cluster` command is executed at the same time as a `jbs_spm�` command. Do not execute these commands at the same time.

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.

7.2.1 Setting services to start and stop 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, set a log-file trap startup definition file.
- You can use `jbs_start` to automatically start a log file trap by editing the `jbs_start` file as needed. Edit the file so that log file trapping starts after the event service and the log-file trap management daemon have started.
- The automatic startup and termination settings are specified according to the encoding that is set for the `LANG` environment variable during installation. However, if the set encoding is not shown in [Table 3-5 in 3.4.2 Setting the language \(for UNIX\)](#), the `LANG` environment variable is set to `C`.
- When you change the language in `jp1bs_env.conf` or `jp1bs_param.conf`, you must also change the `LANG` environment variable of the automatic start script accordingly.
- The automatic start script (`jbs_start`) performs an unsetup of the locale settings of `LC_ALL`, `LC_COLLATE`, `LC_CTYPE`, `LC_MONETARY`, `LC_NUMERIC`, `LC_TIME`, and `LC_MESSAGES` by default.

In AIX environment

To automatically start and stop services in an AIX environment, perform the following procedure in addition to the above operations.

1. Specify the settings to automatically start services.

Using the `mkitab` command, make the following entries in the `/etc/inittab` file:

```
mkitab -i hnr2mon "jp1base:2:wait:/etc/opt/jp1base/jbs_start"
```

2. Check the settings.

Use the `lsitab` command to check settings in the `/etc/inittab` file.

```
lsitab -a
```

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 `jplbase`).

```
init:2:initdefault:
brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase 3 of system boot
...
...
hntr2mon:2:once:/opt/hitachi/HNTRLlib2/etc/D002start
jplbase:2:wait:/etc/opt/jplbase/jbs_start
```

Note

When JP1/Base is uninstalled, the entry `hntr2mon:2:once:/opt/hitachi/HNTRLlib2/etc/D002start` is deleted if no other products are using Hitachi Network Objectplaza Trace Library.

3. 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/jplbase/jbs_stop && /etc/opt/jplbase/jbs_stop
test -x /opt/hitachi/HNTRLlib2/etc/D002stop && /opt/hitachi/
HNTRLlib2/etc/D002stop
```

4. 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.

Notes

The automatic startup and termination settings are specified according to the encoding that is set for the `LANG` environment variable during installation. However, if the set encoding is not shown in [Table 3-5 in 3.4.2 Setting the language \(for UNIX\)](#), the `LANG` environment variable is set to `C`.

When you change the language in `jplbs_env.conf` or `jplbs_param.conf`, you must also change the `LANG` environment variable of the automatic start script accordingly.

The automatic start script (`jbs_start`) performs an unsetup of the locale settings of `LC_ALL`, `LC_COLLATE`, `LC_CTYPE`, `LC_MONETARY`, `LC_NUMERIC`, `LC_TIME`, and `LC_MESSAGES` by default.

In AIX, the OS issues `SIGKIL` when there is not enough memory. A JP1/Base process might be terminated in this case. To avoid this problem, set the environment variable `PSALLOC=early` and start JP1/Base.

Set the environment variable `NODISCLAIM = true` at the same time `PSALLOC` is set to `early`.

An example of the setting for an automatic start script is given below.

1. Search for the part below in the automatic script.

```
export PATH LANG SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF
```

2. Add the following lines after the line found in step 1.

```
PSALLOC=early
NODISCLAIM=true
export PSALLOC NODISCLAIM
```

In Linux environment

To set up automatic startup and automatic termination of JP1/Base, you need to create both of the following files.

```
/etc/opt/jplbase/jbs_start  
/etc/opt/jplbase/jbs_stop
```

When JP1/Base is started or terminated without the files `jbs_start` and `jbs_stop`, the following messages are output to the `syslog` file. Even though the messages below are output to the `syslog` file, automatic startup and automatic termination are not performed because the settings have not been specified.

At the time of startup: Started JP1/Base Service.

After enabling the JP1/Base automatic startup and termination, if you want to start or stop JP1/Base manually, execute the following command. After executing the command, use the `jbs_spmc_status` command and `jevstat` command to check the status of the process.

Starting JP1/Base

For the physical host;

```
systemctl start jpl_base.service
```

For the logical host;

```
systemctl start jpl_base_logical-host-name.service
```

Stopping JP1/Base

For the physical host;

```
systemctl stop jpl_base.service
```

For the logical host;

```
systemctl stop jpl_base_logical-host-name.service
```

When you use commands other than the `systemctl` command, such as `jbs_start` or `jbs_start.cluster`, `jbs_stop` or `jbs_stop.cluster`, `jbs_spmc`, and `jbs_spmc_stop`, to start or stop the program, the automatic stop for JP1/Base will not be performed (the script for stopping the system will not operate but the automatic startup and termination settings remain enabled). If you want JP1/Base to automatically stop when the system stops, perform the operation for activation by executing the `systemctl` command again. To check whether JP1/Base stops automatically, execute the following command and see whether "active" is displayed.

For the physical host;

```
systemctl is-active jpl_base.service
```

For the logical host;

```
systemctl is-active jpl_base_logical-host-name.service
```

When SELinux is enabled on Linux 8 or later, set the context type to `bin_t` for `jbs_start` and `jbs_stop`.

A setting example is shown below:

```
# semanage fcontext -a -t bin_t '/etc/opt/jplbase/jbs_start'  
# semanage fcontext -a -t bin_t '/etc/opt/jplbase/jbs_stop'  
# restorecon -F /etc/opt/jplbase/jbs_start  
# restorecon -F /etc/opt/jplbase/jbs_stop
```

When SELinux is enabled on Linux 9 or later, set the context type to `usr_t` for all files in `/opt/hitachi/HNTRLib2/etc`.

A setting example is shown below:

```
# semanage fcontext -a -t usr_t '/opt/hitachi/HNTRLib2/etc(/.*)?'  
# restorecon -R -F /opt/hitachi/HNTRLib2/etc
```

7.2.2 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 List of processes \(in UNIX\)](#). If your desired JP1/Base functionality is not activated, use the relevant command to start it. For details on commands, see [15. 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. For details on the `hntr2mon` command, see [hntr2mon \(UNIX only\)](#) in [15. Commands](#).

8

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.

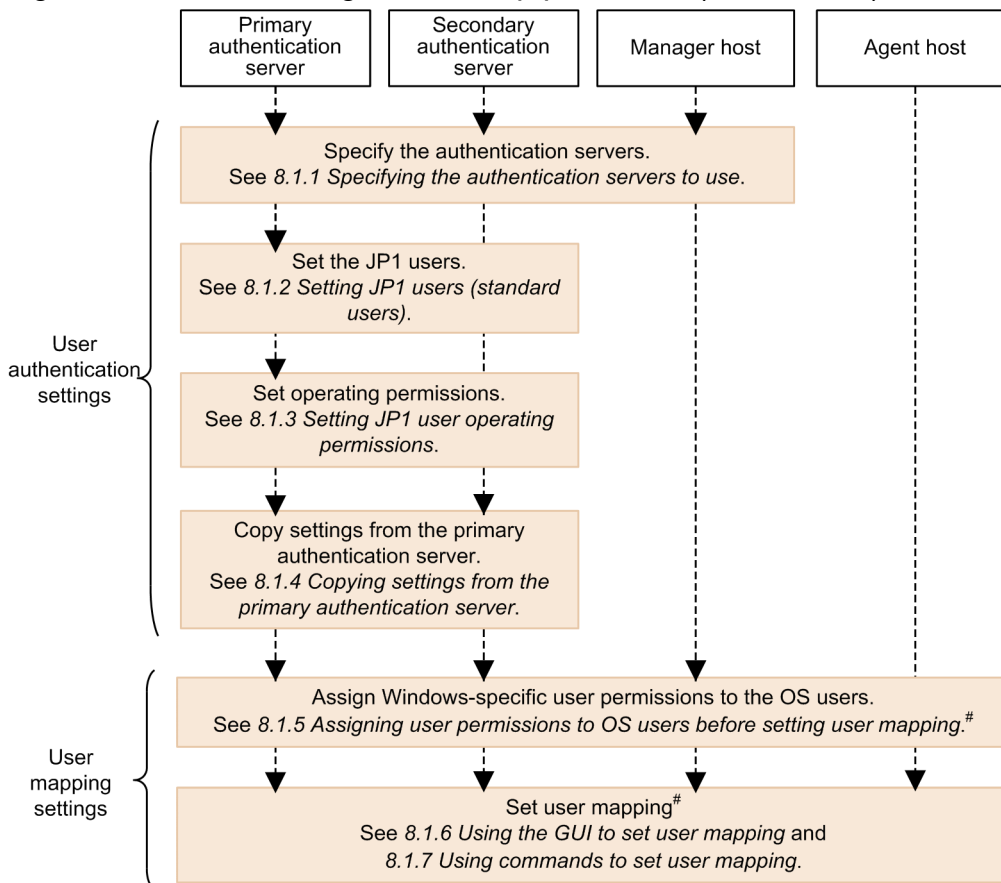
8.1 User management setup (in Windows)

If you use automatic setup to install JP1/Base, JP1/Base is installed with the default settings. For details on the default settings that apply when you set up JP1/Base automatically, see [3.2.1 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 8–1: User management setup procedure (in Windows)



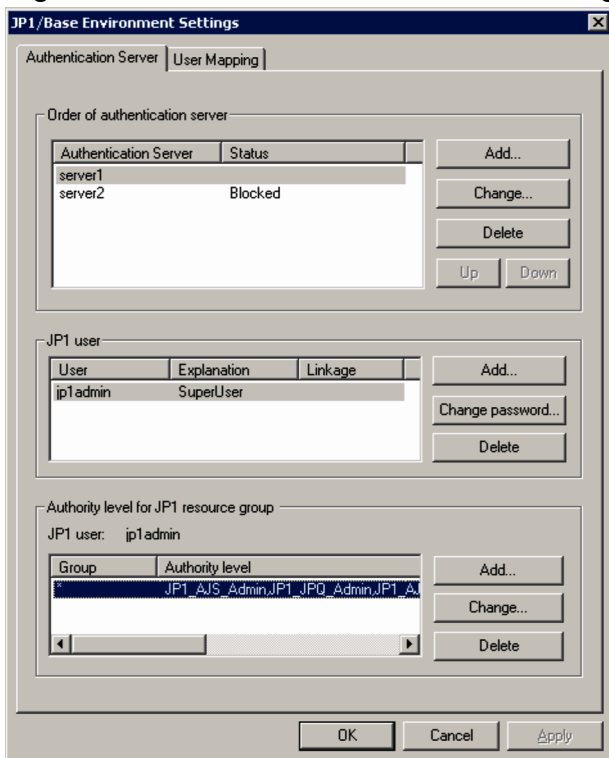
Legend:

-----> : 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 **JP1_Base Setup**. 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 8–2: JP1/Base Environment Settings dialog box



8.1.1 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)
- A host on which a product that utilizes JP1/Base user authentication, such as JP1/IM - Manager and JP1/AJS - Manager, is installed

A host specified as an authentication server manages JP1 users and the operating permissions for JP1 resource groups. When JP1/IM, JP1/AJS, or other products that use user authentication provided by JP1/Base access the authentication server through SSL communication, you have to enable the SSL communication setting on the host on which JP1/Base is installed. To be able to use SSL communication, the required version of JP1/Base must be 11-00 or later in all products that use user authentication provided by JP1/Base.

Note that if the communication encryption function (SSL communication) is enabled on an authentication server host, SSL communication must also be enabled on each host that connects to that authentication server. If hosts that do not use SSL communication must be authenticated, you need to install an authentication server that does not use SSL communication to separate the user authentication block. Also note that to use SSL communication, the version of JP1/Base on the authentication server host and the hosts connecting to the authentication server host must be 11-00 or later.

You can use the GUI or commands to set up an authentication server.

(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.

1. Click the **Add** button.
2. In the Authentication Server dialog box, enter the authentication server name and 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:

1. From the **Authentication Server** field, select the authentication server you want to delete.
2. Click the **Delete** button.

Changing an authentication server:

1. From the **Authentication Server** field, select the authentication server you want to change.
2. Click the **Change** button.

Change the authentication server in the Authentication Server 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 *15. 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-s  
erver-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 *15. Commands*.

If you specified the local host as the primary authentication server, go to *8.1.2 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 *8.1.4 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.

8.1.2 Setting JP1 users (standard users)

In this section, you can set up JP1 users (standard users) for whom user authentication is performed from an authentication server. In cases performing user authentication through linking with a directory server (to use a linkage user or DS user), see *8.2 Setup for user authentication linking with the directory server (Windows only)*. Unless otherwise specified, *JP1 user* means *JP1 user (standard user)* in this section.

JP1 users must be set on a host specified as 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.

You can use the GUI or commands to set up JP1 users.

When an attempt is made to register a JP1 user or to change a JP1 user's password, the authentication server uses the password policy definitions to check the specified password. If the specified password is not compliant with the password policy, the authentication server outputs a warning message to the integrated trace log. By referring to the integrated trace log, you can identify the reason for non-compliance.

An error is output unless the specified password satisfies all the policy conditions set in the password policy definitions.

! Important

When a password check based on the password policy definitions is enabled, entering a non-compliant password upon the execution of a command causes the KAVA5908-E message to be output.

(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 [8.4 Setup for handling the blocked status \(using a secondary authentication server\)](#).

Clicking the **Add** button displays the JP1 User dialog box.

Figure 8–3: JP1 User dialog box



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 8–1: 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	When no password policy is defined: \ " : and spaces and tabs

Item	Number of bytes	Prohibited characters
		When a password policy is defined: As per the setting specified in the password policy definition file

#

For details on how to enable a password check that is based on a password policy, see [2.1.1\(3\) Password policy-based management](#).

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 [15. 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. For details on the characters that can be specified for user names and passwords, see [Table 8-1](#).

When a password check based on the password policy definitions is enabled, a check is performed to verify if a password set upon the registration of a JP1 user is compliant with the password policy.

Changing the password of a JP1 user:

To change the password of a registered JP1 user, execute the following command:

```
jbschgpasswd JP1-user-name
```

When a password check based on the password policy definitions is enabled, a check is performed to verify if a password set during the process of changing a JP1 user's password is compliant with the password policy.

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
```

8.1.3 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.

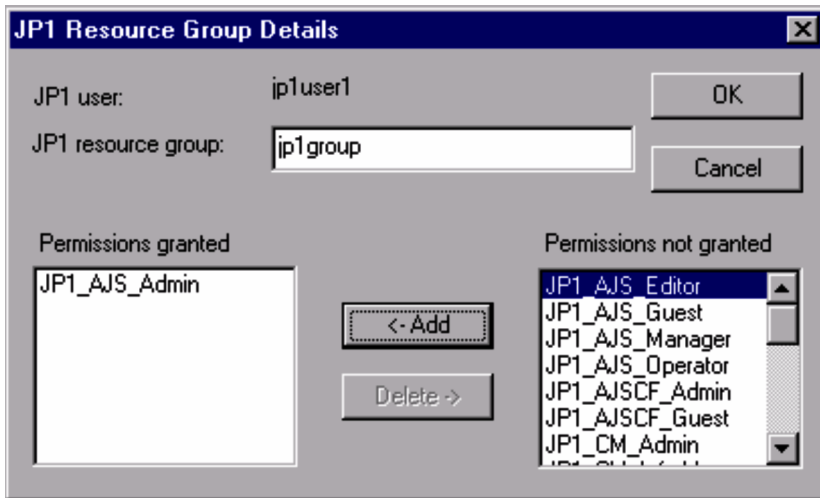
(1) Using the GUI to set JP1 user operating permissions

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 8–4: JP1 Resource Group Details dialog box



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 do not 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 *15. Commands*. For details on the user permission level file, see [User permission level file](#) in *16. 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 user permission definition file that describes operating permissions given to each JP1 user you want to register.

You can create a user permission 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 *16. Definition Files*.

After preparing a user permission definition file, execute the following command to register the information in the definition file with the authentication server: Specify also the `-d` option to register operating permission to a DS user.

```
jbssetacl -f user-permission-definition-file-name
```

For details on the `jbssetacl` command, see [jbssetacl](#) in *15. 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 *15. Commands*.

8.1.4 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 [8.1.2 Setting JP1 users \(standard users\)](#) or [8.2.1\(2\) Setting JP1 users \(linked users\)](#).

For details on the settings of the JP1 user operating permissions, see [8.1.3 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\jplbase\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 [15. 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.
- Ensure that the same password save format is set for the primary and secondary authentication servers. Because the default format has been changed from hash level 1 to hash level 2 in JP1/Base version 12-00 and later, the settings on the two authentication servers might not match. To check the password save format, check message KAVA1692-I, which appears when the authentication server host is started. For details on how to set the password save format, see [3.4.6 Setting the password save format](#).

8.1.5 Assigning user permissions to OS users 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 OS users who are mapped.

You can use the OS functionality to assign these rights to OS users. The setting procedure differs between an Active Directory-based domain environment and a non-domain environment. The following describes the rights required by OS users, and how to assign those rights.

(1) User rights required by mapped OS users

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, or to execute a local action in JP1/Base:

Log on locally

(2) Assigning user rights to an OS user

The procedure for assigning user rights to an OS user differs between an Active Directory domain environment and a non-domain environment. The procedure also differs between a host with a domain controller and a local host within a domain. Note that, depending on settings, assigning a user right to an OS user on a host with a domain controller eliminates the need for configuration on a local host within the domain. The following shows how to set user rights for each host.

Notes

- In Active Directory environments, by default, the domain controller assigns **Log on locally** right to all OS users who belong to the Administrators group. Do not re-assign **Log on locally** user right to OS users who already belong to the Administrators group.
- 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.

Assigning user rights to an OS user in an Active Directory domain environment

The following describes how to assign user rights to an OS user in an Active Directory domain environment.

Specifically, the following describes the respective procedures for setting user rights on a domain controller host, and on a local host within a domain.

Setting user rights on a domain controller host:

The following describes how to set a user right on a domain controller host, where the scope of the user right covers the whole domain:

1. In the Domain Security Policy dialog box of the domain controller host, select the user rights you want to grant, and then add domain users or domain groups.
2. On a domain controller host, use the commands to reflect the updated security policy.

Execute the following commands on a local host:

```
gpupdate /target:user
```

```
gpupdate /target:computer
```

You can use the event viewer to confirm that the settings are in effect.

Because the required permissions are set on the domain controller host, you do not need to set a user right on the local host.

The following describes how to set a user right on a domain controller host, where the scope of the user right is limited to the domain controller host:

1. On a domain controller host, select the desired user right in the **Default Domain Controllers Policy** dialog box or **Local Security Policy** dialog box, and then add a domain user or users.
2. Use the commands to reflect the updated security policy.

Execute the following commands on the domain controller host:

```
gpupdate /target:user  
gpupdate /target:computer
```

You can use the event viewer to confirm that the settings are in effect.

Setting user rights on a local host within a domain:

The following describes how to set a user right on a local host within a domain:

1. On a local host, select a desired user right in the **Local Security Policy Setting** dialog box, and then use a command for adding a domain user or users to reflect the updated policy.

Execute the following commands on the local host:

```
gpupdate /target:user  
gpupdate /target:computer
```

You can use the event viewer to confirm that the settings are in effect.

Setting user rights to an OS user in a non-Active Directory environment

The following describes how to set a user right on a local host.

1. On a local host, select the desired user right, and then add an OS user or users in the **Local Security Policy Setting** dialog box.
2. Use the commands to reflect the updated security policy.

Execute the following commands on the local host:

```
gpupdate /target:user  
gpupdate /target:computer
```

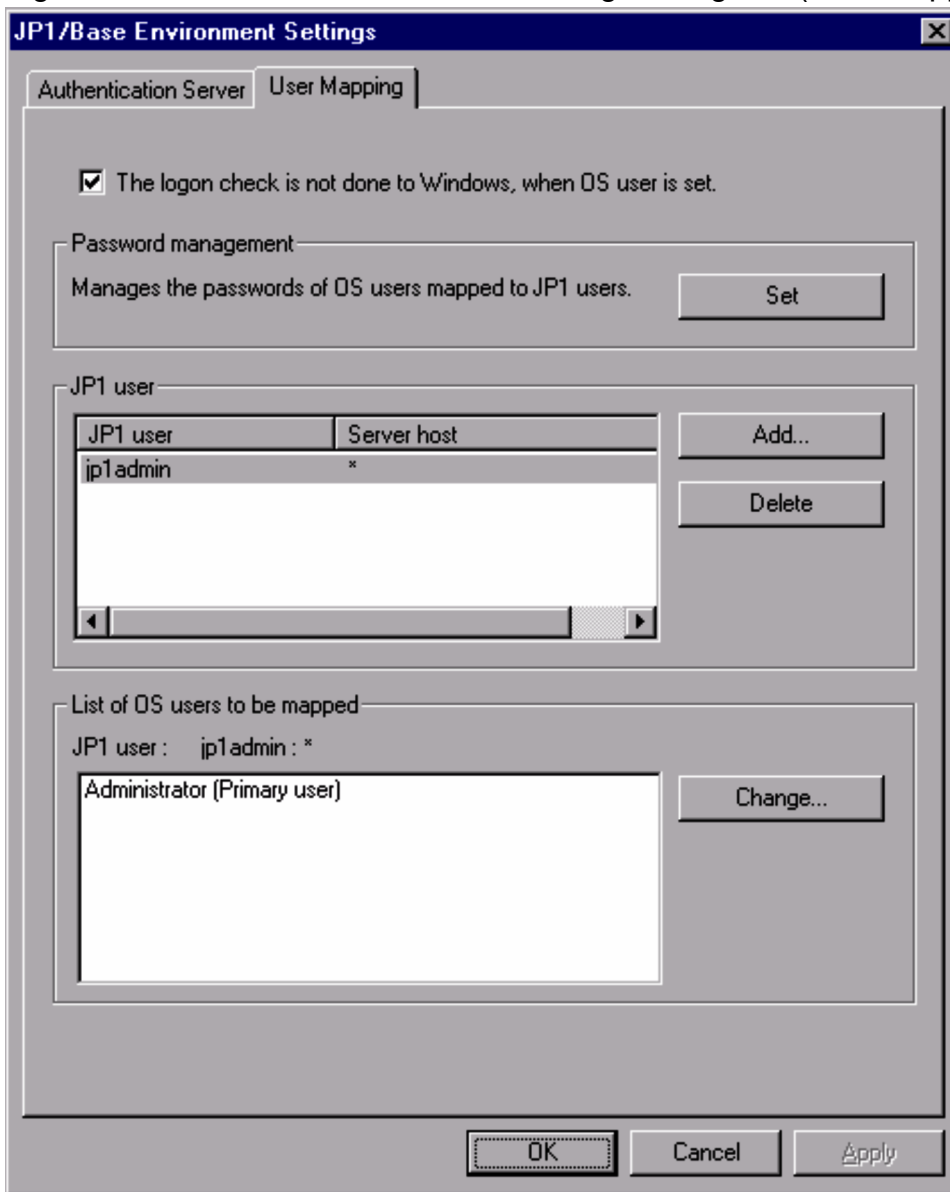
You can use the event viewer to confirm that the settings are in effect.

These are representative procedures, and might not apply to your specific environment. In that case, see the online help or related documentation for your OS.

8.1.6 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 8–5: JP1/Base Environment Settings dialog box (User Mapping page)



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 OS users who are mapped. For details, see [8.1.5 Assigning user permissions to OS users 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.

You can also use the **Password management** area to register information-search users, registration of which is used for user authentication linking with the directory server, but you cannot use this area to map them.

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.

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 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.

- Before you delete an OS user, make sure that the user is not mapped to any JP1 user. You can check the user mapping information by using either of the following:
 - List of OS users to be mapped in the **User mapping** tab of JP1/Base Environment Settings
 - `jbsgetumap` command

To set password management information:

1. In the **Password management** area, click the **Set** button.
2. You can then register, change, or delete OS users and their password information in the Password Manager dialog box.

Figure 8–6: Password Manager dialog box



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.

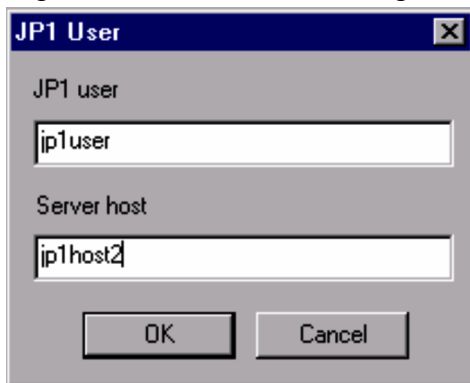
(2) Settings in the JP1 user area

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.

1. Click the **Add** button.

In the JP1 User dialog box, you can then set the JP1 user to map to the OS user, and the server host from which the user issues 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.

Figure 8–7: JP1 User dialog box



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, also add the host name definition in FQDN format.

Specifying a logical host in **Server host**

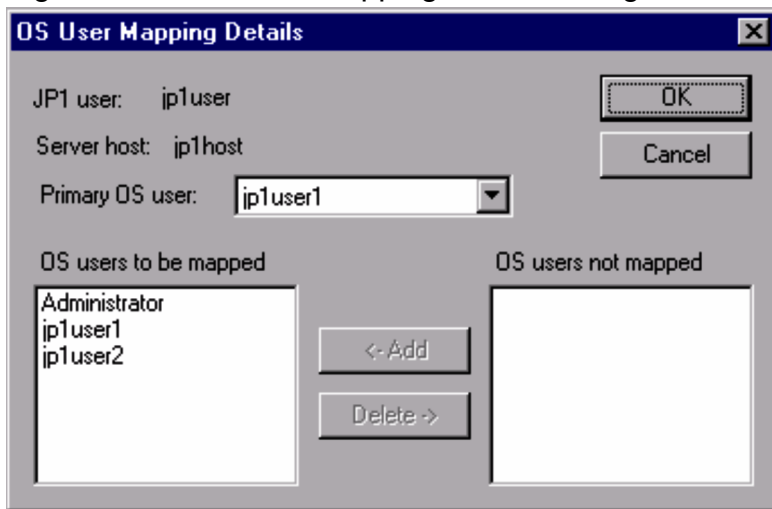
Specify the logical host name. If you are using domain names with the DNS service without defining logical hosts in `jp1hosts` or `jp1hosts2` information, also add the logical host name definition in FQDN format.

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 *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *JP1/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 8–8: OS User Mapping Details dialog box



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. Note that, however, you cannot map information-search users.

As the primary OS user, specify the 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:

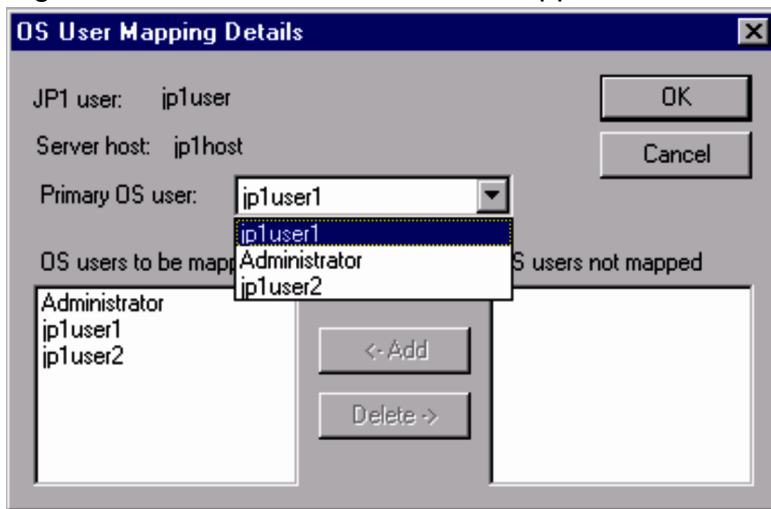
1. In the **JP1 user** area, select a user name listed in the **JP1 user** field to redefine the mapping relationships for that JP1 user.

The **List of OS users to be mapped** area displays the names of the OS users mapped to that user.

2. Click the **Change** button.

3. In the OS User Mapping Details dialog box, you can change which OS users are mapped and not mapped to the OS user, and set the primary OS user.

Figure 8–9: A list of the OS users mapped to the selected JP1 user



4. Click the **OK** button.

This completes the mapping of the JP1 user to OS users.

8.1.7 Using commands to set user mapping

Before setting user mapping, you need to assign certain Windows user permissions to OS users who are mapped. For details, see *8.1.5 Assigning user permissions to OS users 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 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.

JP1/Base provides a number of commands for setting password management information. The following table lists these commands and their purpose.

Table 8–2: Commands for setting password management information

Command name	Purpose	See:
jbspasmgr	Displays the Password Manager dialog box.	(1)
jbsmkpass	Sets password management information for multiple OS users in one operation from a definition file.	(2)

Command name	Purpose	See:
<code>jbsumappass</code>	Adds a specific OS user or changes the password of an OS user registered in the password management information.	(3)
<code>jbsrmumappass</code>	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.

Table 8–3: Commands for setting user mapping information

Command name	Purpose	See:
<code>jbsmkumap</code>	Sets user mapping information in the common definition information at one time from a definition file.	(5)
<code>jbssetumap</code>	Adds or modifies user mapping information in the common definition information at one time from a definition file.	(6)
<code>jbsrmumap</code>	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 [8.1.6\(1\) Settings in the Password management area](#)

For details on the `jbspassmgr` command, see [jbspassmgr \(Windows only\)](#) in [15. 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 [15. 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 [16. 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 *15. 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 *15. 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 *16. 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 *15. 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 JPI-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 *16. Definition Files*. For details on the `jbssetumap` command, see *jbssetumap* in *15. 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 *15. Commands*.

8.1.8 Notes on user management setup

- 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.

You can change the password management information for JP1/Base from the User Mapping page of the JP1/Base Environment Settings dialog box, or by using the `jbsumappass` or `jbsrmumappass` commands.

- When you set user management in a cluster system, you must first set up the environment for a cluster system as described in *5. 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 **JP1_Base Setup**.
 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 *8.1 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\jplbase\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
```

8.2 Setup for user authentication linking with the directory server (Windows only)

User authentication through linking with a directory server has two methods. One is to use a DS user and the other is to use a linkage user. Use a DS user for the case where JP1 authentication information (JP1 user authentication information and JP1 operating permission) is managed by a directory server. Use a linkage user for the case where only JP1 user authentication information is managed by a directory server.

If user authentication is performed by linking with the directory server, both the JP1 administrator and directory server administrator need to perform setup tasks.

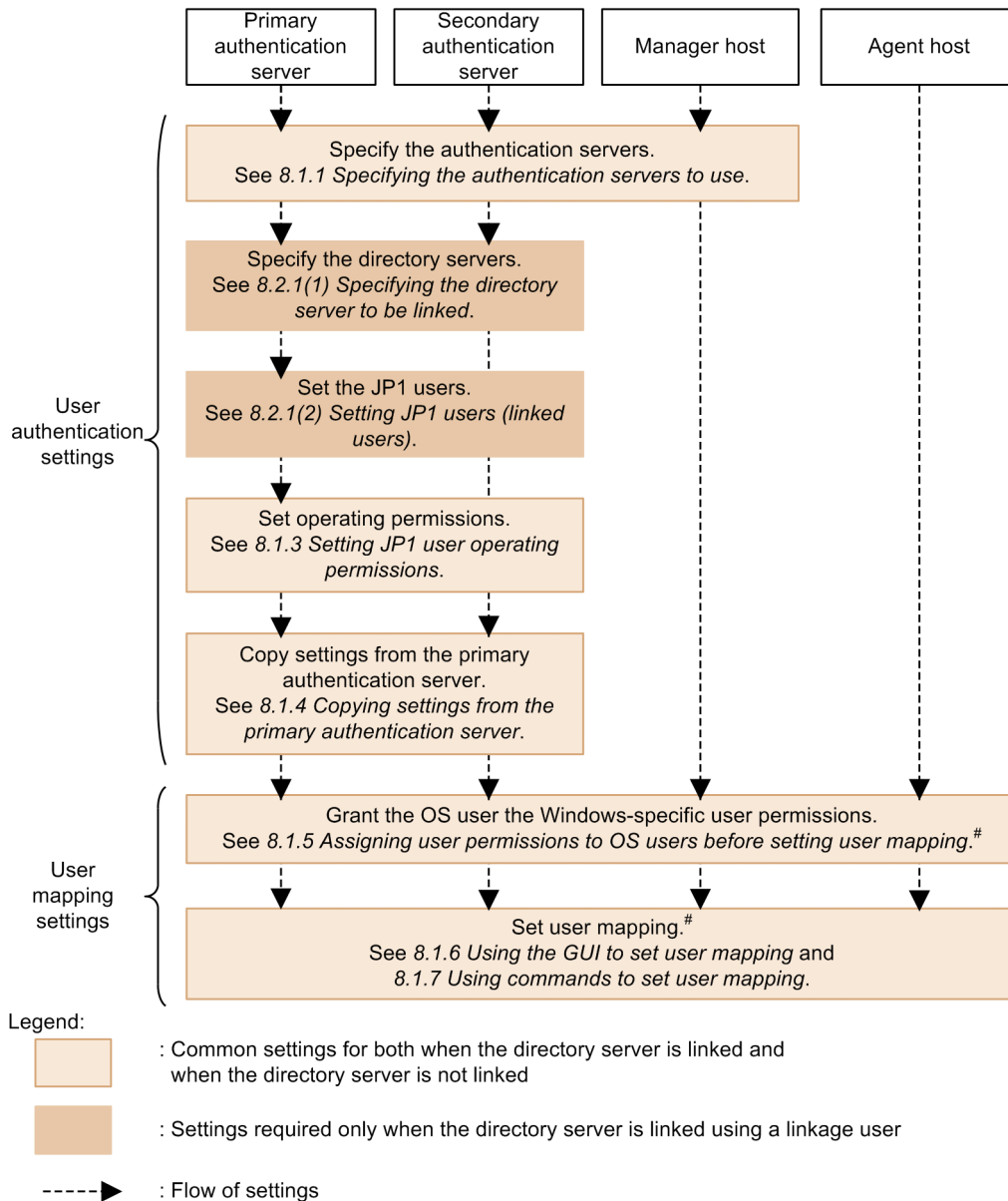
The following table shows the required setup tasks for the cases using a DS user or a linkage user respectively.

Table 8–4: Setup tasks for JP1 administrator and directory server administrator

JP1 user type	Setup tasks for JP1 administrator	Setup tasks for directory server administrator
Linkage user	Settings for directory server linkage on the authentication server <ul style="list-style-type: none">• Designation of a directory server• Setting of a JP1 user (linkage user)	Registration of a JP1 user (linkage user) to the directory server
DS user	Settings for directory server linkage on the authentication server <ul style="list-style-type: none">• Designation of a directory server Setting of operating permissions (when setting in JP1/Base)	In-advance setting of the Active Directory <ul style="list-style-type: none">• Extension of the schema to set operating permission• Creation and settings of a group Setting of operating permissions (when setting in Active Directory)

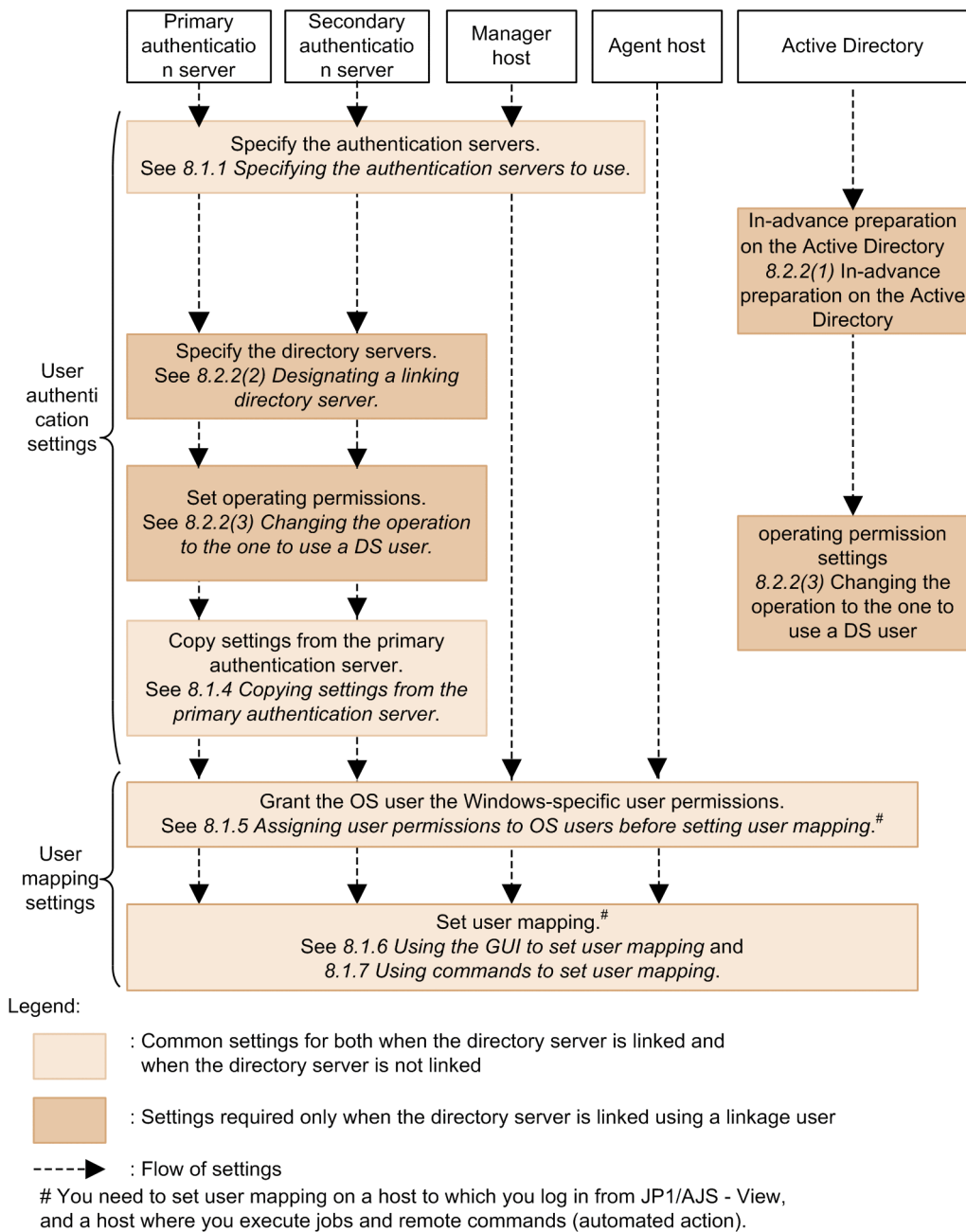
The following figure shows the setup procedure required on each host and the corresponding subsections in this manual when performing user authentication by linking with the directory server.

Figure 8–10: User management setup procedure (operation to use a linkage user)



[#] 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).

Figure 8–11: User management setup procedure (operation to use a DS user)



In the subsequent subsections, explanations will be given for settings required only for the cases performing user authentication through linking with a directory server. For details on other settings, see the location in this manual indicated in Figure 8-10 or Figure 8-11. 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 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
- `jp1hosts` information or `jp1hosts2` information cannot be used to resolve the name of the linked directory server to an IP address. Therefore, specify settings so that, for example, the OS `hosts` file can resolve the name.

8.2.1 Settings for the operation to use a linkage user

In case of operation to use a linkage user, perform JP1 user settings after finishing the settings for directory server linkage.

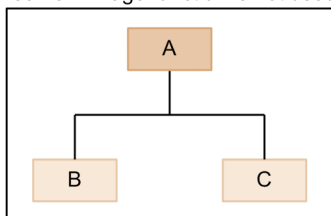
(1) Specifying the directory server to be linked

If you want to perform user authentication linking with the directory server, you must set up the common definition information from the authentication server. The directory server linkage function is inactive by default, and needs to be set up in the common definition before you can use it. If you use a secondary authentication server, set up the function on both the primary authentication server and secondary authentication server.

In JP1/Base version 10-10 or later, you can use the following extended functions by linking with the directory server:

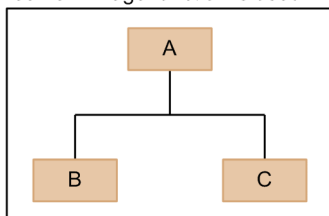
- All OUs under the specified OU can be linked to the directory server.

When the expanded directory server linkage function is not used



If OU _A is specified, only OU _A is linked to the directory server.

When the expanded directory server linkage function is used



If OU _A is specified, OU _A, and OU _B and OU _C (which are under OU _A) are linked to the directory server.

Legend:

: OUs linked to the directory server : OUs not linked to the directory server

- As the attribute name used for a JP1 user name, you can use an attribute other than CN.
You can specify CN, `sAMAccountName`, or `UserPrincipalName` as the attribute name used for a JP1 user name.

If you want to use these extended functions, you must set up an information-search user, which is used to search for users linked to the directory server on the directory server. For details, see (b) *Setting up the directory server linkage (when the expanded directory server linkage function is used)*.

(a) Setting up the directory server linkage (when the expanded directory server linkage function is not used)

The directory server administrator must register JP1 users in one container object when setting up the directory server. Note that a user linked to the directory server must have a CN (common name) attribute value that is the same as the corresponding JP1 user name.

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 16. *Definition Files*.
2. Execute the `jbssetcnf` command.

The settings are reflected in the common definition information. For details about the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

3. Execute the `jbschkds` command.

This command allows you to check the settings for directory server linkage.

For details on the `jbschkds` command, see *jbschkds (Windows only)* in 15. *Commands*.

(b) Setting up the directory server linkage (when the expanded directory server linkage function is used)

The directory server administrator must register JP1 users under the container object specified with the `BASE_DN` parameter in the directory server linkage definition file when setting up the directory server. Note that a user linked to the directory server must have the attribute value that is specified with the `ATTR_NAME` parameter in the directory server linkage definition file and that is the same as the corresponding JP1 user name.

1. Edit the directory server linkage definition file (`jp1bs_ds_setup.conf`).

Unlike when the expanded directory server linkage function is not used, the following settings are required:

`BASE_DN`

Specify the ID of the container object that the JP1 users belong to. Linkage to the JP1 users under the container object specified with this parameter will then be available.

`SEARCH_USER_DN`

Specify the ID of the information-search user used to access the directory server. The information-search user is a directory server user who has view permission for the search-origin container object and the underlying container objects.

`ATTR_NAME`

Specify the attribute name to be used as a JP1 user name from `CN`, `sAMAccountName`, and `UserPrincipalName`.

For details about the directory server linkage definition file, see *Directory server linkage definition file (Windows only)* in 16. *Definition Files*.

2. Execute the `jbssetcnf` command.

The settings are applied to the common definition information. For details about the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

3. Register the information-search user and the password in the authentication server host.

Register the information-search user and the password used to log in to the directory server as password management information in JP1/Base on the authentication server host. The password for the information-search user must be from 1 to 64 bytes. Use the `jbsmkpass` command, `jbspassmgr` command, or `jbsumappass` command for registration. Note that the user to be registered (information-search user) must be specified in the format of `aduser/information-search-user-name`. For example, specify `aduser/Groupcsearcher` when you specified `"CN=Groupcsearcher, OU=GroupC, DC=domain, DC=local"` in `SEARCH_USER_DN`.

For details about the individual commands, see *jbsmkpass (Windows only)*, *jbspassmgr (Windows only)*, or *jbsumappass (Windows only)* in 15. *Commands*.

4. Execute the `jbschkds` command.

Check the directory server linkage settings. For details about the `jbschkds` command, see *jbschkds (Windows only)* in 15. *Commands*.

Important

When the expanded directory server linkage function is used, if you change the password information managed by the OS, you must also change the password management information for the information-search user set in JP1/Base.

To change the password management information in JP1/Base, change it on the **User Mapping** tab in the JP1/Base Environment Settings dialog box or by executing the `jbsumappass` or `jbsrmumappass` command.

(c) Change the directory server to be linked

You can temporarily change the directory server to be linked if the specified directory server cannot be used for reasons such as system failure. To change the server temporarily, create a configuration file containing the required definition information, and then execute the `jbschgds` command. To cancel the change, execute the `jbschgds` command again.

For details on the `jbschkds` command, see *jbschkds (Windows only)* in *15.Commands*.

(2) Setting JP1 users (linked users)

This subsection describes how to set JP1 users (linked users) to use linked users. To set JP1 users, you can use the GUI or commands to register and delete JP1 users who use JP1/IM or JP1/AJS. The JP1 users you register here 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.

Set a JP1 user on both the primary authentication server and the secondary 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.

(a) 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.

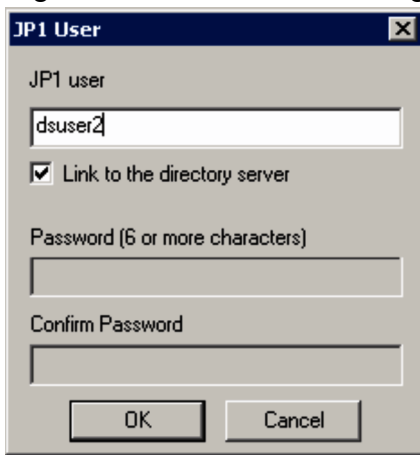
To set information in the **JP1 user** area, you must activate it first. To do this, select (highlight) an authentication server in the **Authentication Server** field in the **Order of authentication server** area. Note, however, that the **JP1 user** area remains dimmed if:

- 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 *8.4 Setup for handling the blocked status (using a secondary authentication server)*.

Click the **Add** button to display the JP1 User dialog box.

Figure 8–12: JP1 User dialog box



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 8–5: 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.

(b) 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 [15. 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 8-5 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
```

(c) 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:

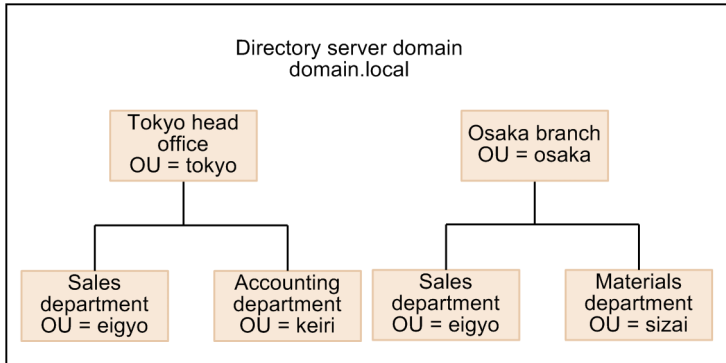
- Byte string (6 to 32 bytes)
- Prohibited characters: \ " : and spaces and tabs

If the number of bytes of a password registered on the directory server is not within the predefined range, or a prohibited character is used in the password, user authentication will fail.

(3) Changing the operation to one using the expanded directory server linkage function

This subsection describes the procedure for changing the operation from one not using the expanded directory server linkage function to one using that function.

This procedure is based on the directory server structure as shown in the figure below, assuming that both the primary and secondary authentication servers are used.



Legend:

 : OU

Directory server linkage settings before change:

The following is a part of the directory server linkage settings before the change:

```
[JP1_DEFAULT\JP1BASE\DIRSRV]
"SERVER"="host-A.domain.local"
"BASE_DN"="OU=eigyō,OU=osaka,DC=domain,DC=local"
"ATTR_NAME"="CN"
```

Change:

- Only the sales department of the Osaka branch was linked to the directory server before the change. Specify the settings so that the materials department of the Osaka branch will also be linked to the directory server.
- Change the attribute name used for a JP1 user name from CN to sAMAccountName.

To change the operation to one using the expanded directory server linkage function:

1. Change the settings for directory server linkage.

Add or change the following parameters in the directory server linkage definition file (`jp1bs_ds_setup.conf`).

Table 8–6: Definitions in the directory server linkage definition file

Parameter	Before the change	After the change
SEARCH_USER_DN	No settings	"CN=Osakaleader,OU=osaka,DC=domain,DC=local"
BASE_DN	"OU=eigyō,OU=osaka,DC=domain,DC=local"	"OU=osaka,DC=domain,DC=local"
ATTR_NAME	"CN"	"sAMAccountName"

Here, set the name of the directory server user (Osakaleader) who has view permission for the search-origin container object for the information-search user.

Change the settings for directory server linkage on both the primary and secondary authentication hosts.

2. Execute the `jbssetcnf` command.

The settings are applied to the common definition information. For details about the `jbssetcnf` command, see [jbssetcnf](#) in *15. Commands*.

3. Register the information-search user and the password in the authentication server host.

Register the information-search user and the password used to log in to the directory server as the password management information in JP1/Base on the authentication server host. Use the `jbsmkpass` command, `jbspassmgr` command, or `jbsumappass` command for registration.

Specify the information-search user to be registered in the format of `aduser/information-search-user-name`. In this procedure, user name `aduser/Osakaleader` and the password are registered as an example.

For details about individual commands, see [jbsmkpass \(Windows only\)](#), [jbspassmgr \(Windows only\)](#), or [jbsumappass \(Windows only\)](#) in *15. Commands*.

4. Add JP1 users.

After the settings are changed, the materials department of the Osaka branch will be also linked to the directory server. Therefore, register new JP1 users who will be linked to the directory server. For details, see [8.2.1\(2\) Setting JP1 users \(linked users\)](#).

Now, register JP1 user names with the same names as sAMAccountName of the users linked to the directory server. If CN and sAMAccountName are different for the users who were linked to the directory server in the sales department, JP1 users for those users must also be registered. After this registration, delete the JP1 users who were linked to the directory server before, because they are no longer required.

5. Copy the settings on the primary authentication server to the secondary authentication server.

Copy the settings on the primary authentication server to the secondary authentication server. For details, see [8.1.4 Copying settings from the primary authentication server](#).

6. Confirm the login.

On both the primary and secondary authentication server hosts, execute the `jbschkds` command to check the settings for directory server linkage and whether user authentication is available for the users linked to the directory server. Also check whether the users can log in to the primary and secondary authentication servers. For details about the `jbschkds` command, see *jbschkds (Windows only)* in 15. Commands.

8.2.2 Settings for the operation to use a DS user

In case of operation to use a DS user, perform directory server linkage settings after finishing the in-advance preparation on the Active Directory.

(1) Extending the schema of the Active Directory

To make Active Directory ready, the schema of Active Directory must be extended.

In order to perform integrated management of JP1 authentication information (JP1 user authentication information and JP1 operating permission) on the Active Directory, add an attribute to the Active Directory to allow the settings of JP1 operating permission. In accordance with the schema extension settings procedure shown below, add an attribute (JP1 operating permission) to the users and group objects on the Active Directory.

Specify a JP1 resource group and JP1 permission level to the value of the added attribute (JP1 operating permission).

The following explains the schema extension procedure to utilize an LDIF file. In order to enable system recovery in case the following schema extension procedure fails, back up the current system conditions (NTBACKUP) beforehand.

1. Copy the model file (`JP1_UserLevel_schema.ldf.model`) from an authentication server with an arbitrary LDIF file name.

The installation directory of the model file on the authentication server is as follows:

```
installation-folder\tools\schema\JP1_UserLevel_schema.ldf.model
```

2. Edit the copied LDIF file.

Change the domain name identification (DC) to follow the `dn :` in the copied file to the corresponding domain name.

The file contains entries [1] through [8], among which four entries, [1], [3], [5], and [7] need to be changed.

Example: Assume the domain name to be `domain.local`.

Before change:

```
dn: CN=hitachiJP1UserLevel,CN=Schema,CN=Configuration,DC=DomainName
```

After change:

```
dn: CN=hitachiJP1UserLevel,CN=Schema,CN=Configuration,DC=domain,DC=local
```

3. Execute the `ldifde` command to extend the schema through importing the LDIF file edited in step 2 above.

```
ldifde -i -f input-file-name -v -j log-file-output-folder-name
```

Because the `ldifde` command execution log is output on the log file, you can confirm the import information.

In case the `ldifde` command fails in an execution error, confirm and perform the following:

- If the execution error indicates `0000202B: RefErr`:

The cause of the domain name reference error (`RefErr`) could be the wrong domain name. Verify the domain names in the LDIF file. If one is incorrect, correct it. In order to avoid repeating the execution of successfully

processed entries, change the entries to comment (insert the # into the top column) before re-executing the `ldifde` command. If this error occurs during the execution of entry [3], for example, change all lines up to entry [2] to comment lines. If this error occurs during the execution of entry [1], no change to comment is needed.

- If the execution error indicates `00002071: UpdErrr`:
The cause of the update error (`UpdErrr`) could be because the schema had been extended and objects already exist. Verify whether the schema is already extended in a way shown in step 4 below. If the schema is already extended, step 3 (schema extension) is unnecessary.
- Other execution errors:
Take appropriate actions depending on the nature of the `ldifde` error.

4. Confirm that a JP1 operating permission attribute is added by schema extension through executing the `ldifde` command.

Confirmation of the default class (`User`):

Export the default class (`User`) to the LDIF file by executing the `ldifde` command. Specify the corresponding domain name for the domain name identification (DC) in the same manner as shown in step 2 above.

```
ldifde -f output-file-name -d CN=User,CN=Schema,CN=Configuration,DC=domain,DC=local
```

Confirm that the JP1 operating permission class (`hitachiJP1AccessLevel`) is specified as an auxiliary class (`auxiliaryClass`) in the exported LDIF file.

```
:  
auxiliaryClass: hitachiJP1AccessLevel  
:
```

Confirmation of the default class (`Group`):

Export the default class (`Group`) to the LDIF file by executing the `ldifde` command. Specify the corresponding domain name for the domain name identification (DC) in the same manner as shown in step 2 above.

```
ldifde -f output-file-name -d CN=Group,CN=Schema,CN=Configuration,DC=domain,DC=local
```

Confirm that the JP1 operating permission class (`hitachiJP1AccessLevel`) is specified as an auxiliary class (`auxiliaryClass`) in the exported LDIF file.

```
:  
auxiliaryClass: hitachiJP1AccessLevel  
:
```

(2) Designating a linking directory server

In order to perform user authentication through linking with a directory server, it is necessary to set the common definition information on the authentication server. Because the directory server linkage function is not set in the common definition at initial settings, it is necessary to change the settings. If a secondary authentication server is installed, change the settings for both the primary and secondary authentication servers.

(a) Directory server linkage setting procedure

It is necessary to set the directory server linkage definition file and to register an information-search user to use a DS user. After the setting up, confirm the connection with the directory server using the `jbschkds` command.

1. Edit the directory server linkage definition file (`jplbs_ds_setup.conf`).

The following explains the differences in editing the definition file in comparison with the operation to use a linkage user.

ENABLE

Specify whether to link with a directory server. Specify 00000002 for operation to use a DS user. Both a standard user and a DS user can be used.

BASE_DN

This parameter is used for specifying the identification name of the container object in which a JP1 user exists. The operation to use a DS user does not require the setting of this parameter.

SEARCH_USER_DN

Specify the identification name of the information-search user to access the directory server. You must specify this parameter for the operation to use a DS user.

For details about the directory server linkage definition file, see *Directory server linkage definition file (Windows only)* in 16. *Definition Files*.

2. Execute the `jbssetcnf` command.

Specified contents are applied to the common definition information. For details about the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

3. Register an information-search user and a password to the authentication server host.

Register an information-search user and a password to use when logging in to the directory server to the JP1/Base password management information of the authentication server host. The length of the information-search user's password must be 1 through 64 bytes. Use the `jbsmkpass` command, the `jbspassmgr` command, or the `jbsumappass` command for the registration. The registration format of a user (information-search user) shall be `aduser/information-search-user-name`. For example, specify `aduser/Groupcsearcher` when you specified "CN=Groupcsearcher,OU=GroupC,DC=domain,DC=local" in `SEARCH_USER_DN`.

It is necessary to register either of the following users because an information-search user needs to have permission to allow the collection of JP1 authentication information or the manipulation of JP1 operating permission attribute for the operation to use a DS user:

- A user to have write permission into the user or group's JP1 operating permission

For details about respective commands, see *jbsmkpass (Windows only)*, *jbspassmgr (Windows only)*, or *jbsumappass (Windows only)* in 15. *Commands*.

4. Execute the `jbschkds` command.

Confirm the settings of directory server linkage. For details about the `jbschkds` command, see *jbschkds (Windows only)* in 15. *Commands*.

(b) Changing the directory server to link

You can temporarily change the directory server to link when it becomes unusable due to failure. Create a file to define the information for a temporary change and execute the `jbschgds` command. Use the `jbschgds` command also to cancel a temporary change.

For details about the `jbschgds` command, see *jbschgds (Windows only)* in 15. *Commands*.

(3) Managing users (Setting operating permissions) when DS users are used

To manage users (set operating permissions) when DS users are used:

1. Create a user (DS user) or security group on the directory server (Active Directory).

Use the Active Directory Users and Computers management tool or Active Directory cmdlets in PowerShell to create a JP1 user (DS user) or security group on which you want to set operating permissions.

2. Set operating permissions.

Set operating permissions on the JP1 user (DS user) or security group that you created in step 1. You can use one of the following ways to grant JP1 operating permissions:

- Use Active Directory to set operating permissions.

On the directory server (Active Directory), use Attribute Editor[#] in the Active Directory Users and Computers management tool or Active Directory cmdlets in PowerShell to set operating permissions on the attribute `hitachiJP1UserLevel` of the JP1 user (DS user) or security group.

The setting format is as follows:

JP1-resource-group=JP1-permission-level:JP1-resource-group=JP1-permission-level:...

For details on definition, see *User permission definition file* in 16. *Definition Files*.

#: To use Attribute Editor, in the Active Directory Users and Computers management tool, select **View** and then **Advanced Features**.

- Use JP1/Base commands to set operating permissions.

On the authentication server (primary authentication server), use the JP1/Base `jbssetacl` command (with the `-ds` option) or the `jbsrmacl` command (with the `-ds` option) to set operating permissions on the JP1 user (DS user) or security group.

For details on how to set operating permissions, see 8.1.3(3) *Using a command to register operating permissions for individual JP1 users* and 8.1.3(4) *Using a command to delete operating permissions for individual JP1 users*.

3. Assign a security group on the directory server (Active Directory).

JP1 operating permissions can be granted through a security group. By using the Active Directory Users and Computers management tool or Active Directory cmdlets in PowerShell, add the JP1 user (DS user) to a security group to which JP1 operating permissions are granted, or set the group of the JP1 user (DS user) to a security group to which JP1 operating permissions are granted.

4. Apply JP1 operating permissions on the authentication server (primary authentication server).

Restart JP1/Base or use the `jbsaclreload` command (with the `-ds` option) to apply operating permissions set in step 2 to the authentication server.

For details on the `jbsaclreload` command, see *jbsaclreload* in 15. *Commands*.

When a secondary authentication server exists, you must also apply operating permissions to the secondary authentication server in the same way.

(4) Changing the operation to the one to use a DS user

The following explains the procedure to change the operation from the one to use a standard or linkage user to the one to use a DS user.

1. Set the Active Directory environment on the directory server.

Extend the schema of the Active Directory to add JP1 operating permission attribute. Perform this step only once to the Active Directory. For details, see 8.2.2(1) *Extending the schema of the Active Directory*.

2. Stop JP1/Base on the authentication server (primary authentication server).

Stop JP1/Base to allow the settings for DS user use.

3. Set JP1/Base environment on the authentication server (primary authentication server).

Modify the directory server linkage definition file to allow the use of DS users. For details, see [8.2.2\(2\)\(a\) Directory server linkage setting procedure](#).

4. Start JP1/Base on the authentication server (primary authentication server).

Start JP1/Base in order to set JP1 operating permission to the Active Directory by using an authentication command.

5. Set JP1 operating permission on the authentication server (primary authentication server).

Set JP1 operating permission to the Active Directory.

To change the operation from the one to use a standard user:

1. Copy the JP1_UserLevel file on the authentication server host with an arbitrary file name.
2. Change the standard user to a DS user name on the definition file.
3. Execute the jbssetacl command (-ds option specified) designating the definition file.
4. If the standard user is used in the user mapping, re-register the DS user together with a password.
5. Delete the standard user and the operating permission registered before the change on the authentication server host.

Use the jbsrmuser command to delete the standard user. Use the jbsrmac1 command to delete the operating permission.

To change the operation from the one to use a linkage user:

1. Copy the JP1_UserLevel file on the authentication server host with an arbitrary file name.
2. Execute the jbssetacl command (-ds option specified) designating the definition file of step 1 above.
3. Delete the linkage user and the operating permission registered before the change on the authentication server host.

Use the jbsrmuser command to delete the linkage user. Use the jbsrmac1 command to delete the operating permission.

6. Execute the jbsaclreload command on the authentication servers (primary and secondary authentication servers).

Execute the jbsaclreload command (-ds option specified) to reload JP1 authentication information with the newly set operating permission.

7. Verify JP1 authentication information on the authentication server (primary authentication server).

Verify JP1 authentication information by using the jbslistuser command or the jbslistacl command.

(5) Notes on the operation to use a DS user

- DS users and DS groups need to satisfy the following conditions:
 - User names or group names shall be unique on the Active Directory. They need to be unique with the attribute specified by the ATTR_NAME parameter on the directory server linkage definition file.
 - Their names shall satisfy the requirements defined in the following table.

Table 8–7: Character requirements for DS user and DS group names

Item	Number of bytes	Prohibited characters
DS user name [#]	1 through 31 bytes	* / \ " ' ^ [] { } () : ; = , + ? < > space, tab character, and non-ASCII characters
DS group name	1 through 256 bytes	* / \ " ' ^ [] { } () : ; = , + ? < > tab character, and non-ASCII characters

#: The character requirements for the DS user names are the same as those of JP1 user names.

- In an environment to use both standard and DS users, if a DS user whose name is identical to the name of a standard user appears, the standard user is given priority.
- In addition to the restrictions on passwords imposed by the directory server, the following restrictions must be observed to be able to use the passwords in JP1 products:

Password: Number of bytes: 6 to 32 bytes, Restrictions on character types: None

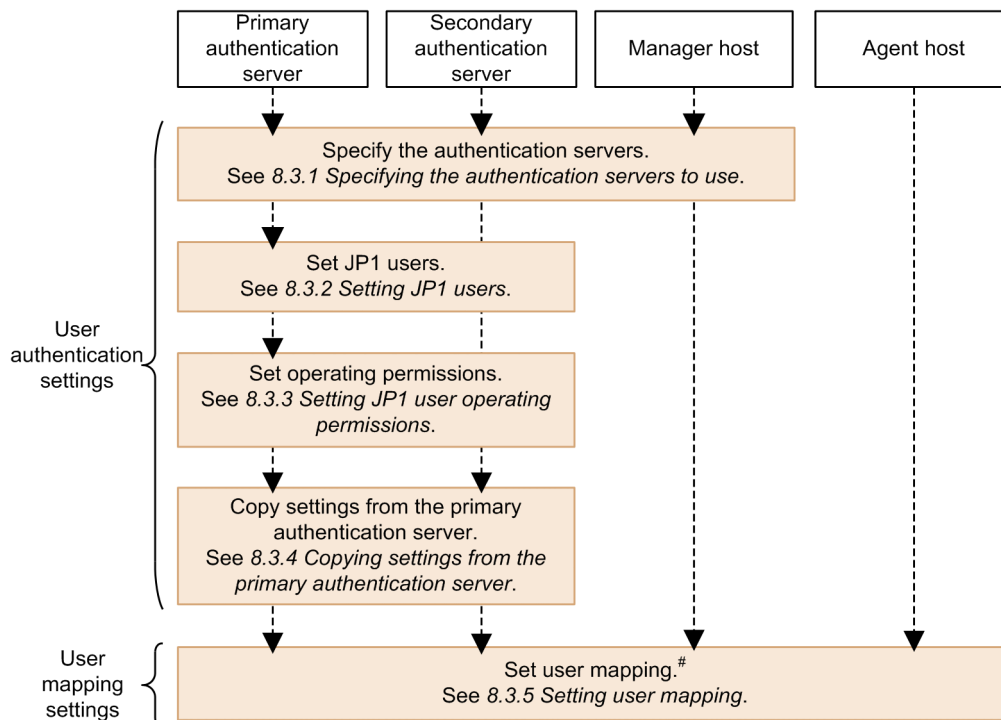
8.3 User management setup (in UNIX)

If you use automatic setup to install JP1/Base, JP1/Base is installed with the default settings. For details on the default settings that apply to an automatic setup, see [3.3.1 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 8–13: User management setup procedure (in UNIX)



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).

8.3.1 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)
- A host on which a product that utilizes JP1/Base user authentication, such as JP1/IM - Manager and JP1/AJS - Manager, is installed

A host specified as an authentication server manages JP1 users and the operating permissions for JP1 resource groups. If you want to use just one user authentication block for a system that contains two or more products that utilize JP1/Base user authentication, for example JP1/IM and JP1/AJS, specify the same authentication server on each host.

Note that if the communication encryption function (SSL communication) is enabled on an authentication server host, SSL communication must also be enabled on each host that connects to that authentication server. If hosts that do not use SSL communication must be authenticated, you need to install an authentication server that does not use SSL communication to separate the user authentication block. Also note that to use SSL communication, the version of JP1/Base on the authentication server host and the hosts connecting to the authentication server host must be 11-00 or later.

(1) Setting the authentication servers

Execute the following command:

```
jbssetusrsv primary-authentication-server [secondary-authentication-server]
```

For details on the `jbssetusrsv` command, see *jbssetusrsv (UNIX only)* in *15. 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 `jbssetusrsv` 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

Execute the following command:

```
jbslistsrv [-h logical-host-name]
```

For details on the `jbslistsrv` command, see *jbslistsrv* in *15. 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/jplbase/conf  
cp -p jplbs_spm�.conf.model jplbs_spm�.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.

8.3.2 Setting JP1 users

This section describes the JP1 users (standard users) for whom user authentication is performed from the authentication server. JP1 users must be set only from the hosts that are authentication servers (the primary authentication servers).

When an attempt is made to register a JP1 user or to change a JP1 user's password, the authentication server uses the password policy definitions to check the specified password. If the specified password is not compliant with the password policy, the authentication server outputs a warning message to the integrated trace log. By referring to the integrated trace log, you can identify the reason for non-compliance.

An error is output unless the specified password satisfies all the policy conditions set in the password policy definitions.

Important

When a password check based on the password policy definitions is enabled, entering a non-compliant password upon the execution of a command causes the KAVA5908-E message to be output.

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 [15. 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.

When a password check based on the password policy definitions is enabled, a check is performed to verify if a password set upon the registration of a JP1 user is compliant with the password policy.

Table 8–8: 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	When no password policy is defined: \ " : spaces and tabs When a password policy is defined: As per the setting specified in the password policy definition file

#

For details on how to enable a password check that is based on a password policy, see [2.1.1\(3\) Password policy-based management](#).

(2) Changing a JP1 user's password:

To change the password of a registered JP1 user, execute the following command:

```
jbschgpasswd JP1-user-name
```

When a password check based on the password policy definitions is enabled, a check is performed to verify if a password set during the process of changing a JP1 user's password is compliant with the password policy.

(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
```

8.3.3 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 [15. Commands](#). For details on the user permission level file, see [User permission level file](#) in [16. 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 16. *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 15. *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 15. *Commands*.

8.3.4 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.

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 *8.3.2 Setting JP1 users*. For details on how to set up user operation permissions, see *8.3.3 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 `jbsessionmgr`.

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/jplbase/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/jplbase/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 *15. 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_spm�.conf.session.model jp1bs_spm�.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.
- Ensure that the same password save format is set for the primary and secondary authentication servers. Because the default format has been changed from hash level 1 to hash level 2 in JP1/Base version 12-00 and later, the settings on the two authentication servers might not match. To check the password save format, check message KAVA1692-I, which appears when the authentication server host is started. For details on how to set the password save format, see [3.4.6 Setting the password save format](#).

8.3.5 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.

(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 [16. 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 [15. 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 (`jplBsUmap.conf`). For details on the format of the user mapping definition file, see *User mapping definition file* in *16. Definition Files*. For details on the `jbssetumap` command, see *jbssetumap* in *15. 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 JPl-user-name
```

For details on the `jbsrmumap` command, see *jbsrmumap* in *15. Commands*.

8.3.6 Notes on user management setup

When you set user management in a cluster system, you must first set up the environment for a cluster system as described in *5. Setting Up JPl/Base for Use in a Cluster System*. Then, set up user management as described in *8.3 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/jplbase/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/jplbase/conf/user_acl/
```

When not using a cluster system:

```
/etc/opt/jplbase/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
```

8.4 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.

8.4.1 Blocked status settings using the GUI (Windows only)

To use the GUI to work with the blocked status:

1. From the Windows **Start** menu, choose **Programs, JP1_Base**, and then **JP1_Base Setup**.
2. In the JP1/Base Environment Settings dialog box, 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

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.
In the Authentication Server dialog box, clear the **Set this authentication server in state of blockage** check box.
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

1. In the **Order of authentication server** area, select an authentication server that has nothing shown in **Status**.

2. Click the **Change** button.

In the Authentication Server dialog box, select the **Set this authentication server in state of blockage** check box.

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.

8.4.2 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

Execute the following command:

```
jbslistsrv
```

For details on the `jbslistsrv` command, see *jbslistsrv* in *15. Commands*.

(2) Releasing the blocked status

Execute the following command:

```
jbsunblockadesrv -s authentication-server
```

For details on the `jbsunblockadesrv` command, see *jbsunblockadesrv* in *15. Commands*.

(3) Placing an authentication server in the blocked status

Execute the following command:

```
jbsblockadesrv -s authentication-server
```

For details on the `jbsblockadesrv` command, see *jbsblockadesrv* in *15. Commands*.

9

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.

9.1 Setting the service start and stop sequences

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 *15. 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 *9.2 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 *9.3 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.

9.2 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.

9.2.1 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 `[FrontOtherServicexxx]` section of the startup sequence definition file (`JP1SVPRM.DAT`), where `xxx` represents a specific service.

2. JP1 services

Write the information in the `[Jp1xxx]` 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 `[OtherServicexxx]` 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).

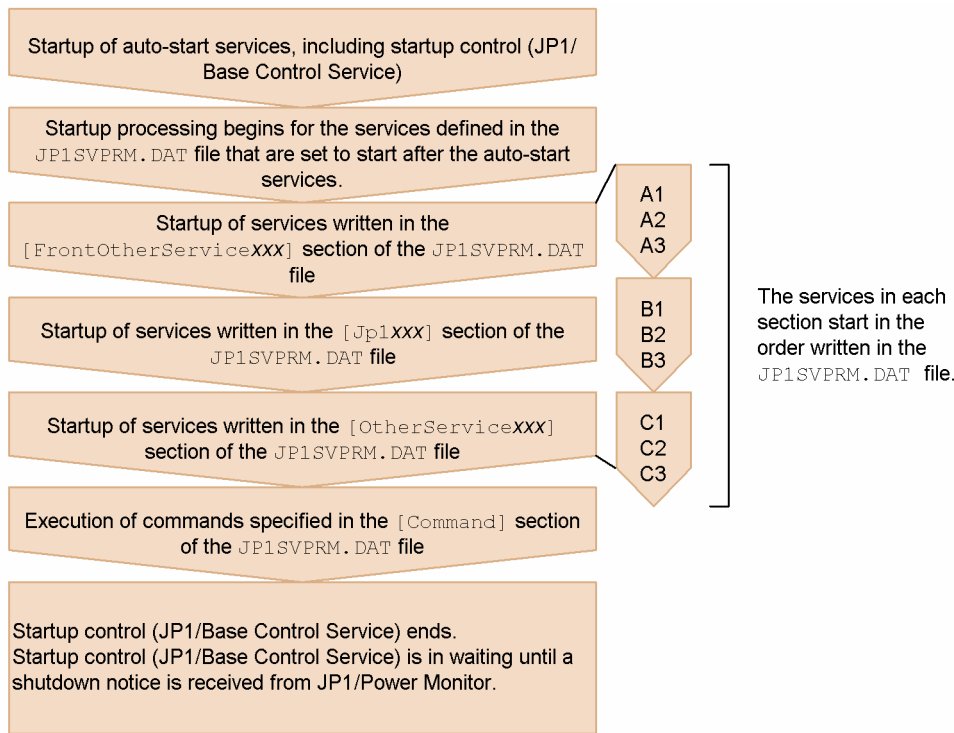
You can also control the startup sequence for the services that have been defined in the startup sequence definition file (`JP1SVPRM.DAT`) as follows:

- 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 *16. Definition Files*.

The following diagram shows the sequence in which services are activated at system startup.

Figure 9–1: Sequence for starting services when using the startup control



Legend:

- A1, A2, and A3: Services written in that order in [FrontOtherServiceXXX]
- B1, B2, and B3: Services written in that order in [Jp1xxx]
- C1, C2, and C3: Services written in that order in [OtherServiceXXX]

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).

9.2.2 Setting the service stop sequence

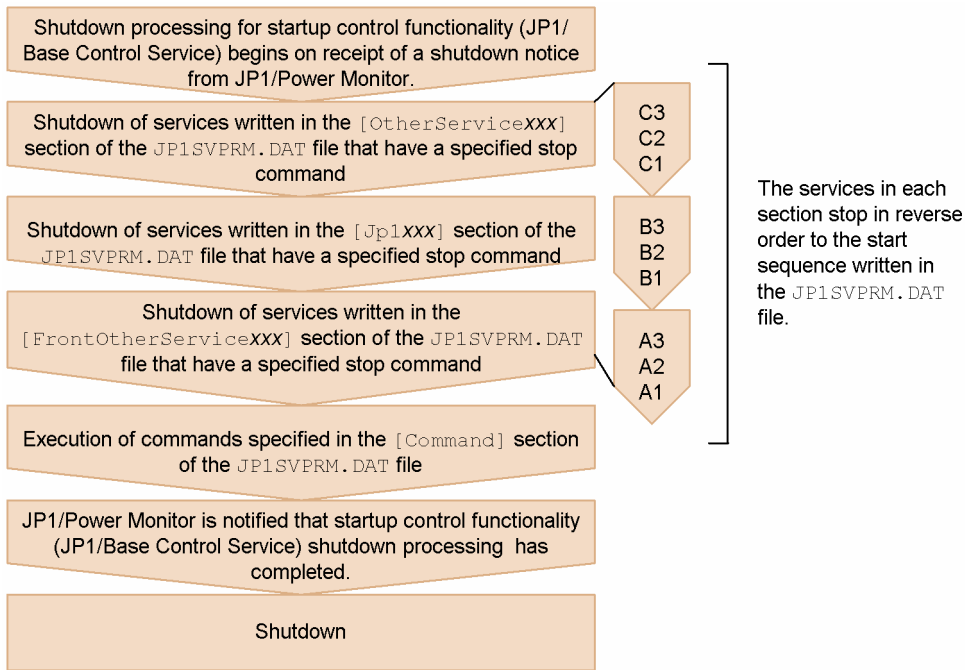
JP1/Power Monitor must be installed on the same host to control the sequence for stopping services. A stop command must be specified in the start sequence definition file (JP1SVPRM.DAT) file for each service that you want to control. The services that have a stop command specified in the file are shut 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 9–2: Sequence for stopping services when using the startup control



Legend:

- A1, A2, and A3: Services written in that order in [FrontOtherServiceXXX]
- B1, B2, and B3: Services written in that order in [Jp1xxx]
- C1, C2, and C3: Services written in that order in [OtherServiceXXX]

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 were started by the startup control function (JP1/Base Control Service) are stopped. Services that could not be started by the startup control function 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.

9.3 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 *16. 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.

9.4 Notes on using 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.

10

Setting up an Event Service Environment

This chapter explains how to set up the JP1/Base event service.

10.1 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

The default settings are as follows:

- 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/jplbase/sys/event/servers/
```

Initially, the maximum size of the event database is set to 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`, `Emergency`, or `Emergence` 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. You can configure JP1/Base to forward JP1 events to a remote host that is not defined in the configuration definition file by editing the forwarding settings file.

10.1.1 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.

By default, only important events are sent to a higher-level server as defined in the system configuration of JP1/IM - Manager. We recommend that you keep the default setting if your goal is to monitor the system for errors. If you do change this setting from the default, make sure that the system does not forward unnecessary JP1 events to higher-level servers.

- Consider JP1 events that are forwarded by default.

The following JP1 events are forwarded to every destination in the forwarding settings file (`forward`), even if the events do not match the event filter conditions. If you do not want JP1/Base to forward these events, define them in an exclusion condition or specify the `auto-forward-off` flag for the `options` parameter in the event server settings file (`conf`).

- Event reporting of JP1/Base startup (00004724)
- Event reporting of JP1/Base shutdown (00004725)
- Event reporting of a threshold-based suppression (00003D0B)
- Event reporting of a stop of a threshold-based suppression (00003D0C)

- Event reporting of a stop of all threshold-based suppressions (00003D0D)
 - Event reporting of the continuation of threshold-based suppressions (00003D0E)
- 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.

10.1.2 Determining if forwarding of a large numbers of events are suppressed

To prevent a large number of events from being forwarded, consider specifying a threshold to detect a large numbers of events, and automatically suppress event forwarding. To automatically suppress event forwarding, you must consider the condition for the suppression of event-forwarding, which represents the threshold for detecting a large numbers of events.

The conditions for the suppression of event-forwarding are specified in the forwarding settings file (`forward`).

The conditions for the suppression of event-forwarding includes unit time (time duration in which the threshold is evaluated), threshold (the number of JP1 events per unit time), and check count (the number of unit times used to determine the occurrence or convergence of large numbers of events).

For details on the conditions for the suppression of event-forwarding, see *Forwarding settings file* in *16. Definition Files*.

10.1.3 Setting up an 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 16. *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. By default, only important events are sent to a higher-level server as defined in the system configuration of JP1/IM - Manager. We recommend that you keep the default setting if your goal is to monitor the system for errors.

For details on the forwarding settings file, see *Forwarding settings file* in 16. *Definition Files*.

3. Enable the setting.

Start the event service to apply the settings.

In Windows:

By default, the event service is configured to start automatically when the system starts. For details on the startup control, see 9. *Setting the Service Start and Stop Sequences (Windows Only)*.

In UNIX:

Execute the `jevstart` command.

10.1.4 Modifying the event service operating environment

1. Edit the event server settings file (`conf`) or API settings file (`api`).

Edit the event server settings file (`conf`) or API settings file (`api`).

2. Edit the event server index file (`index`).

Stop the event service before editing the event server index file (`index`).

3. 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.

(1) 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 *16. Definition Files*.
2. Execute the `jevdbmkrep` command.
For details on the `jevdbmkrep` command, see *jevdbmkrep* in *15. Commands*.
3. Start the event server.

10.1.5 Modifying 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.

(1) 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 *12. Collecting and Distributing Event Service Definitions (JP1/IM Only)*.

(2) 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.

(3) 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 JPI/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 [jbsrt_distrib](#) in *15. Commands*.

10.1.6 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 *15. Commands*.

10.1.7 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 *15. Commands*.

10.1.8 Using a manager to suppress event forwarding of large numbers of events

This section describes how to use the `jevagtfw` command to start and stop event forwarding suppression and check the status of the event forwarding suppression. This section also describes how to stop a specific log file trap from the manager.

For details on how to use the `jevagtfw` command to suppress event forwarding and on how to stop a specific log file trap from the manager, see the *JPI/Integrated Management 3 - Manager Administration Guide*. In this manual, see the descriptions on suppressing forwarding of a large number of events.

(1) Using a manager to suppress event forwarding from an agent with large numbers of JP1 events

To suppress event forwarding from an agent on which large numbers of JP1 events are occurring, execute the following command from the manager:

```
jevagtfw -s host-name
```

For details on the `jevagtfw` command, see [jevagtfw](#) in *15. Commands*.

(2) Checking agent hosts whose event forwarding is suppressed

To display a list of agent hosts whose event forwarding has been suppressed by the `jevagtfw` command, execute the following command from the manager:

```
jevagtfw -l
```

For details on the `jevagtfw` command, see [jevagtfw](#) in *15. Commands*.

(3) Stopping event forwarding suppression from the manager

To stop forwarding suppression activated by the `jevagtfw` command, execute the following command from the manager:

```
jevagtfw -r host-name
```

For details on the `jevagtfw` command, see [jevagtfw](#) in *15. Commands*.

(4) Using a manager to stop a log file trap issuing large numbers of JP1 events

To selectively stop a log file trap from the manager, you can use the IM configuration management functionality. Stop the process of the log file trap to be suppressed from the Display/Edit Profiles window in IM configuration management - View.

10.1.9 Setting a threshold to suppress forwarding of large numbers of events

This section describes how to set up a threshold-based suppression of event-forwarding and how to check the forwarding status of each condition for the suppression of event-forwarding.

(1) Setting up the conditions for the suppression of event-forwarding

1. Edit the forwarding settings file (`forward`) on an agent whose event forwarding is to be automatically suppressed. Specify the conditions for the suppression of event-forwarding in the JP1/Base forwarding settings file (`forward`) on the agent.

Format:

```
suppress identifier unit-time threshold check-count [destination (optional
)]
event-filter
end-suppress
```

For details on the conditions for the suppression of event-forwarding, see [Forwarding settings file](#) in *16. Definition Files*.

2. Apply the modification in the forwarding settings file (`forward`).
Reload the forwarding settings file (`forward`), or restart the event service to apply the changes.

If the JP1 event occurrence status matches the condition for the suppression of event-forwarding, event forwarding is automatically suppressed. If the problem is solved and the JP1 event occurrence status matches the stop condition for the suppression of event-forwarding, event forwarding is automatically restarted.

(2) Checking the forwarding status of each condition for the suppression of event-forwarding

To check the forwarding suppression status of each condition for the suppression of event-forwarding, execute the following command from the manager:

```
jefwstat
```

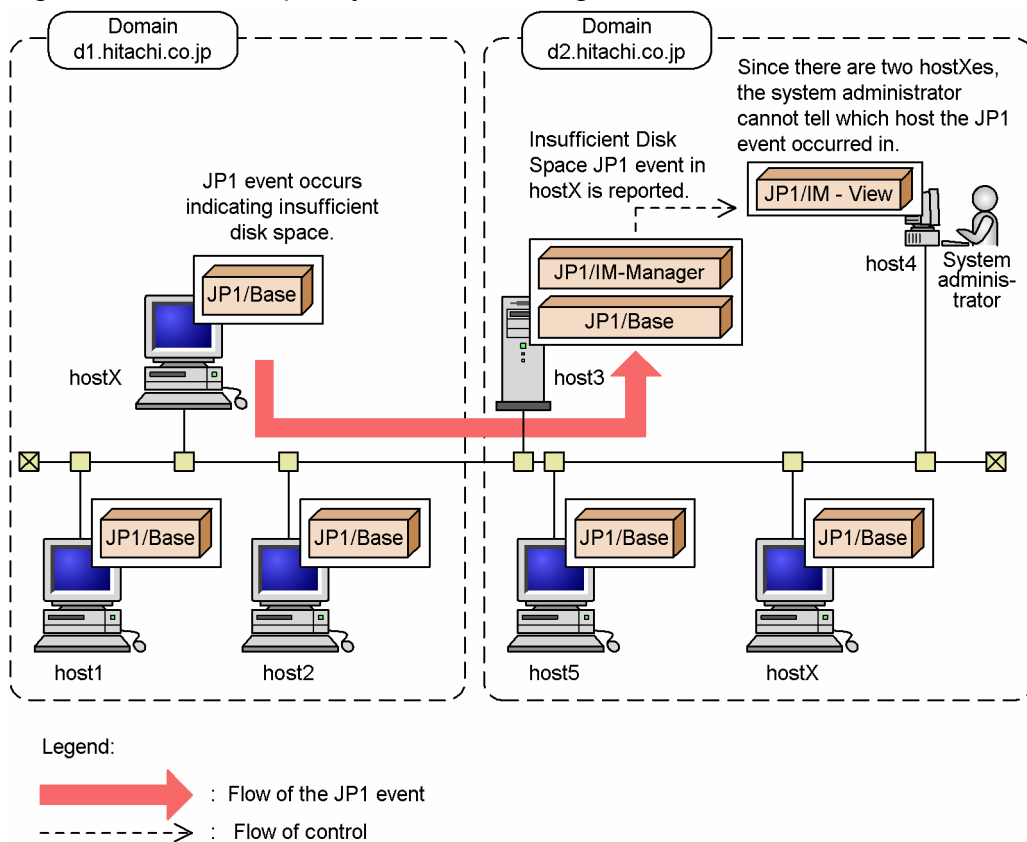
For details on the `jefwstat` command, see *jefwstat* in 15. *Commands*.

10.1.10 Setting up an event server in a system that uses DNS services

You might encounter a number of issues if you use an event server with the default settings 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 10–1: 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 this kind of problem in systems with multiple domains, configure an event server with a name in Fully Qualified Domain Name format (a FQDN-format event server).

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)

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 you have installed JP1/IM - Manager or JP1/AJS, there will be dependencies with the default services. When you configure an FQDN-format event server in Windows, remove any dependencies the default event service has with JP1/IM - Manager and JP1/AJS.

2. Open the event server index file (`index`) in an editor, and change the event server name in the `server` parameter from the default `*` to `@` or `hostX.d1.hitachi.co.jp`.

Change this to `@` to enable the collection and distribution of event service definitions. Change this to `hostX.d1.hitachi.co.jp` to disable the collection and distribution of event service definitions. Choose whichever setting suits your system.

3. Open the start sequence definition file (`JP1SVPRM.DAT`) in an editor, and edit the file so that the FQDN-format event server starts 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)

The specified event server here is assumed to be `hostX.d1.hitachi.co.jp`.

1. Open the event server index file (`index`) in an editor, and change the event server name in the `server` parameter from the default `*` to `@` or `hostX.d1.hitachi.co.jp`.

Change this to `@` to enable the collection and distribution of event service definitions. Change this to `hostX.d1.hitachi.co.jp` to disable the collection and distribution of event service definitions. 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 an editor, and 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
```

10.2 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.

10.2.1 Initializing an event database while the event service is active

If a JP1 event is being forwarded to another event server, refer to [10.2.2 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 *15. 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 *15. 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 [10.2.2 Initializing an event database while the event service is stopped](#).

10.2.2 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.

(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 *JP1/Integrated Management 3 - 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 *15. 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 *15. 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}
```

10.3 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 *15. Commands*. The output format of a CSV file is described below.

10.3.1 Output format of a CSV file

- 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.

10.3.2 Items output to the 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. To output these items in Japanese, specify an encoding in the code set attribute of the `-l` option. If you omit the `-l` option, the titles are output in English.

Table 10–1: 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
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.

Col.	Attribute name	Title name	Contents	Format	Remarks
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
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	SOURCESEQUENO	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
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	Character string	Extended attribute value 6

Col.	Attribute name	Title name	Contents	Format	Remarks
			range of values is the same as for OBJECT_TYPE.		
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
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	--
:	:	:	:	:	:
:	:	:	:	:	:
<i>m-1</i>	Program-specific extended attribute name <i>n</i>	Not output.	Program-specific extended attribute name	Character string	--
<i>m</i>	Program-specific extended	Not output.	Program-specific extended attribute value	Character string	--

Col.	Attribute name	Title name	Contents	Format	Remarks
	attribute value <i>n</i>				

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 10-1 Items output when the -k option is specified in the jevexport command](#). The title name is output when the `-a` option is specified. To output these items in Japanese, specify an encoding in the code set attribute of the `-l` option. If you omit the `-l` option, the titles are output in English.

Table 10-2: 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 <i>n</i>)
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	--
:	:	:	:	:	:
:	:	:	:	:	:
<i>m</i> -1	Program-specific extended attribute name <i>n</i>	Not output.	Program-specific extended attribute name	Character string	--
<i>m</i>	Program-specific extended attribute value <i>n</i>	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

10.4 Notes on 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 jplimevtapi
```

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 jplimevt jplimevtapi
```

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.

11

Setting Up the Event Converters

Windows event logs 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.

11.1 Converting application program log files

When you use log file trapping, the log messages to be converted to JP1 events differ for each user. For this reason, there is no default definition information 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.

11.1.1 Checking the format of application program log files

Check the format of the monitored log files, and specify the log file format in the action definition file for log file trapping. This subsection describes the flow of checking the log file format.

Log files are mainly divided into sequential files and wrap-around files, depending on the output format.

A sequential file is a file that does not shrink. When log data is output, the data is always added to the file. Among the various formats of sequential files, log file trapping can monitor the log files in SEQ, SEQ2, SEQ3, or UPD format.

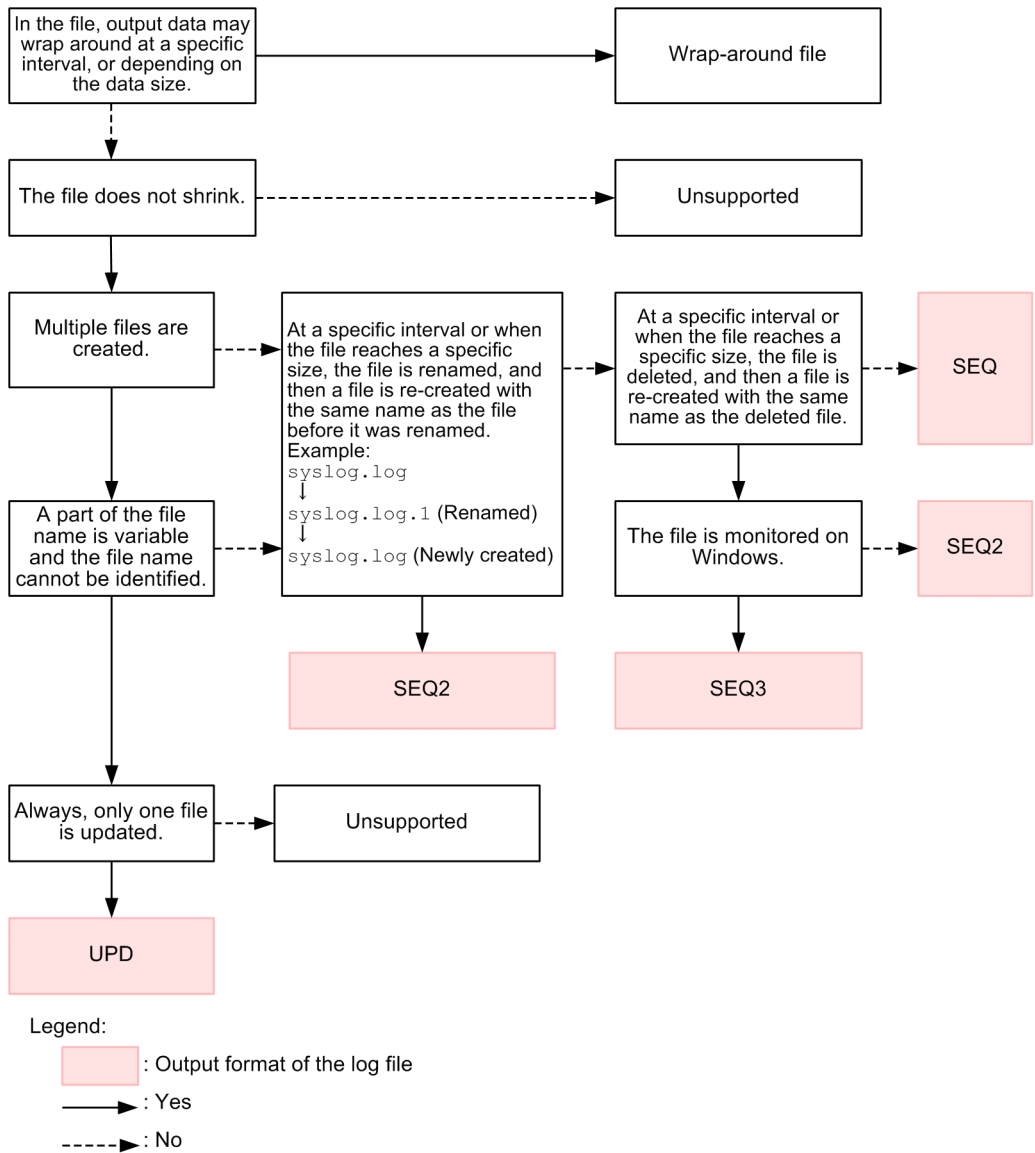
A wrap-around file is a file for which the output position of log data may return to the beginning of the file at a specific interval, or depending on the data size. Among the various formats of wrap-around files, log file trapping can monitor the log files in WRAP1, WRAP2, or HTRACE format.

For details about the format of log files that can be monitored, such as SEQ and WRAP1, see [2.4.4 Types of log files that can be monitored](#).

(1) Flow of checking the log file format (for a sequential file)

If the monitored log file is a sequential file, check the log file format according to the flow in the figure below. Note that the unsupported log files in the following figure cannot be monitored by log file trapping.

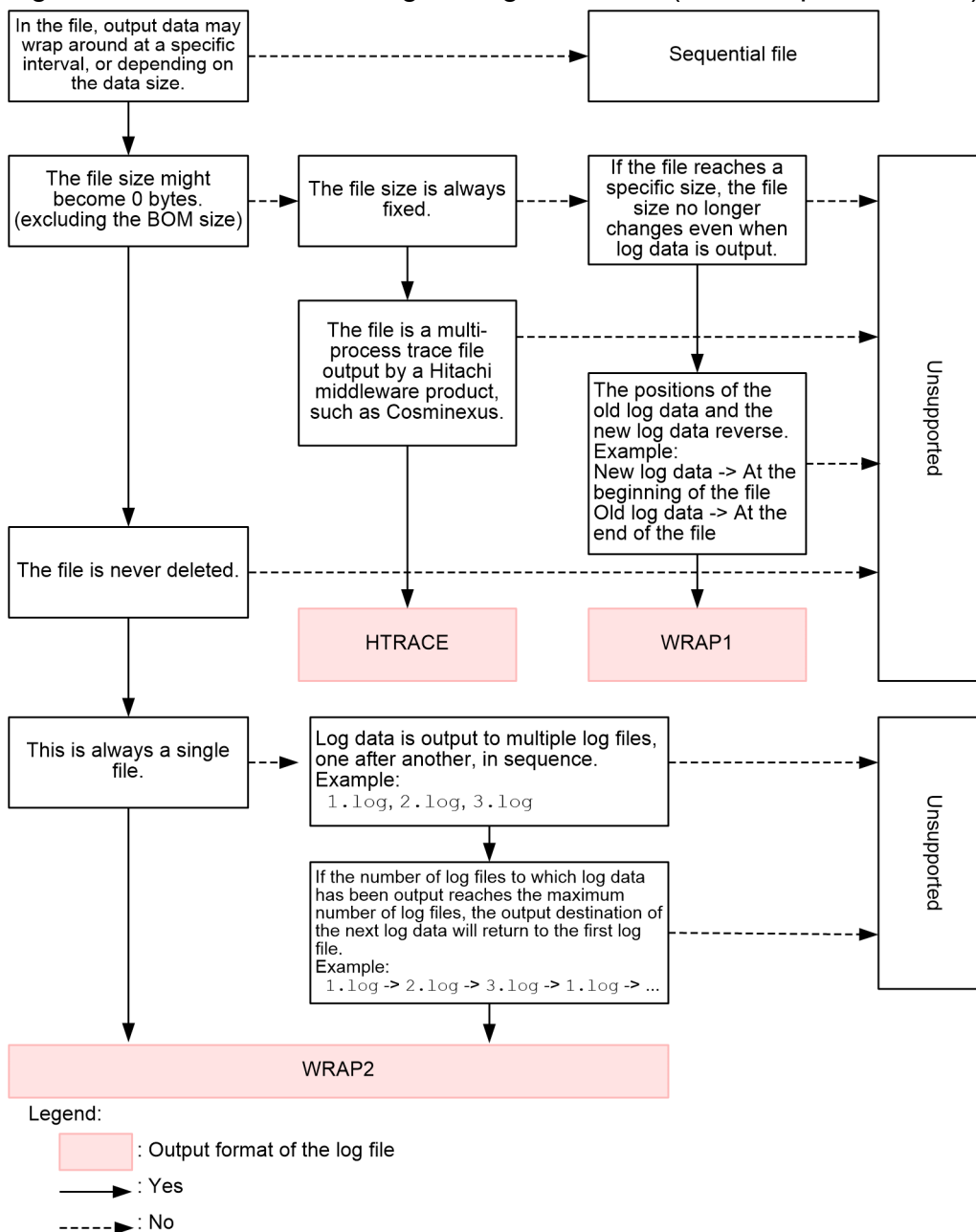
Figure 11–1: Flow of checking the log file format (for a sequential file)



(2) Flow of checking the log file format (for a wrap-around file)

If the monitored log file is a wrap-around file, check the log file format according to the flow in the figure below. Note that the unsupported log files in the following figure cannot be monitored by log file trapping.

Figure 11–2: Flow of checking the log file format (for a wrap-around file)



11.1.2 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. For details, see *Action definition file for log file trapping* in *16. Definition Files*.
- Log information definition file (`jevlogd.conf`)
Specify the maximum size and number of storable log files used for log file trapping. In most circumstances, you can use the default settings.
For details, see *Log information definition file* in *16. Definition Files*.

(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 *15. Commands*.

(2) Changing a setting

The following describes how to change settings in an action definition file for log file trapping and a 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 *15. Commands*.

For details on the `jevlogreload` command, see *jevlogreload* in *15. Commands*.

(b) Changing a setting in the log information definition file

1. Edit the log information definition file (`jevlogd.conf`).
2. Start the log-file trap management service (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 *15. 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 *15. 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 *15. 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:

- Use a log-file trap startup definition file (`jevlog_start.conf`).
In a log-file trap startup definition file, specify the log file traps that you want to start and the startup options for those log file traps. The log file traps you specify will start automatically when the log file trap management server (daemon) starts.
For details on the log-file trap startup definition file, see [Log-file trap startup definition file](#) in *16. Definition Files*.
If you use a log-file trap startup definition file, check whether the required log file traps have started by viewing the startup record (KAVA3661-I) and startup results (KAVA3662-I) output to the log-file trap startup execution results log.
- 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 *16. 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.

(7) Setting the language for log file traps (in UNIX)

You can set the language type for a log file trap by specifying the `LANG` environment variable when you start the trap. For details on the values that can be specified for the `LANG` environment variable, see [3.4.2 Setting the language \(for UNIX\)](#).

The following describes how to specify UTF-8 as the language for log file traps.

(a) Specifying LANG at jevlogstart command execution

You can monitor log information output in UTF-8 encoding by using the `jevlogstart` command to start a log file trap with UTF-8 specified in the `LANG` environment variable.

Example of using a script to start a log file trap

```
#!/bin/sh
LANG=ja_JP.utf8
export LANG
jevlogstart -a abc /home/hitachi/abc.log
```

(b) Specifying LANG in the log-file trap startup definition file

Specify UTF-8 as the startup `LANG` value in the `START_OPT` parameter (for the log file trap management daemon) and the `START_OPT_CLS` parameter (for a logical host) of the log-file trap startup definition file.

Format of log-file trap startup definition file

```
START_OPT=[<startup-LANG>] monitored-name:jevlogstart-command-options
START_OPT_CLS=[cluster-ID] [<startup-LANG>] monitored-name:jevlogstart-command-options
```

11.1.3 Notes on 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.

(1) Notes on monitoring the integrated trace log or syslog file

The event server settings file (`conf`) includes the `options` parameter with `KAJP1037-syslogoff` and `KAJP1037-hntroff` by default when JP1/Base V12 is newly installed. However, the parameter is not set properly in the following cases: you restore the definition file from another version where these flags are not set, you install JP1/Base by overwriting another version where these flags are not set, or you delete these flags. When `KAJP1037-syslogoff` and `KAJP1037-hntroff` are not specified and you use a log file trap to monitor the integrated trace log or `syslog` file, attempts to transfer 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 include settings like the following in the action definition file for log file traps in order to monitor the integrated trace log or `syslog` file, the transfer error message `KAJP1037-E` is converted to a JP1 event.

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"
```

In this case, if the forwarding settings file (`forward`) is used with initial settings in a system that links with IM Configuration Management of JP1/IM or that uses the JP1/Base configuration management functionality, transfer-failure JP1 events are also forwarded. This causes the event transfer to loop repeatedly.

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"
```

(2) Note on using JP1/AJS log file monitoring jobs

If you want to use a JP1/AJS log file monitoring job, you must first start the JP1/Base log-file trap management service (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 *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *JP1/Automatic Job Management System 3 Administration Guide*.

(3) Note on monitoring Unicode files in Windows

When you use a log file trap to monitor Unicode files in Windows, even if the log file trap is started successfully, the log files might not be monitored properly. These problems occur due to inappropriate action definition specification or erroneous monitoring target files.

When you monitor Unicode files in Windows, errors are not reported in the cases shown in the table below. Therefore, check the log file trap operation (whether filtering can be properly performed according to the condition) in advance.

Table 11–1: Cases where Unicode files cannot be monitored properly in Windows and associated prior checks

Case where monitoring cannot be performed properly	Prior check
Basic regular expression is used in the MARKSTR and ACTDEF parameters in the action definition file for log file trapping.	Specify the extended regular expressions used in the operation to the ACTDEF parameter in the action definition file for log file trapping, and check if proper filtering is performed according to the condition.

Case where monitoring cannot be performed properly	Prior check
A Unicode file is specified in the action definition file for log file trapping.	Specify a multi-byte character in the <code>ACTDEF</code> parameter in the action definition file for log file trapping, and check if proper filtering is performed according to the condition.
The monitoring target file is a Unicode file and the <code>-g</code> option is omitted when executing the <code>jevlogstart</code> command.	
You used the <code>jevlogstart</code> command with the <code>-g</code> option intending to monitor a Unicode file, but mistakenly specified a log file that is not Unicode.	

(4) Monitoring syslog files in SUSE Linux 15 or later

In SUSE Linux 15 or later, by default, log information is output to journals only, not to syslog.

To monitor syslog files by using log file traps, syslog output must be enabled. For details about how to enable syslog output, see [3.4.8 Syslog output when SUSE Linux 15 or later](#).

11.2 Converting Windows event logs

Use the event log trapping function to convert Windows event logs into JP1 events. By default, the event log trapping function converts the Error and Warning log entries output to the system log and application logs that are displayed as standard in the Windows event viewer.

The following describes how to set up an event log trap.

11.2.1 Procedures for setting up event log trapping

This section describes how to configure event log trapping to start and stop. 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 retry settings for when monitoring fails. For details, see *Action definition file for event log trapping (Windows only)* in *16. Definition Files*.

(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.
- By default, if an invalid log type or a malformed regular expression is specified in a filter in the action definition file for event log trapping (`ntevent.conf`), that filter is deemed invalid but the service will start and reload settings successfully. 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 *16. Definition Files*.
- Event log entries are monitored starting from the time the trapping service starts. Entries before the service starts cannot be monitored.
- When restarting the Windows event log service, also restart the event log trap service.

(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 `jeventreload` 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 (`nthevent.conf`).

```
jbsgetopinfo -o evttrap
```

For details on the `jbsgetopinfo` command, see *jbsgetopinfo* in 15. *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.

Notes

When the OS is shut down, the Windows event log service sometimes stops before the event log trapping function of JP1/Base. If this happens, conversion of the data received by the event log trapping function might fail, and the event log might either be converted to a JP1 event when it should not be, or not converted to a JP1 event when it should be. This problem does not occur if the event log trapping service is stopped before the OS is shut down.

(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 16. *Definition Files*.

11.2.2 Notes on event log trapping

(1) Notes on operation

The event server settings file (`conf`) includes the `options` parameter with `KAJP1037-syslogoff` and `KAJP1037-hntroff` by default when JP1/Base V12 is newly installed. However, the parameter is not set properly in the following cases: you restore the definition file from another version where these flags are not set, you install JP1/Base by overwriting another version where these flags are not set, or you delete these flags. This subsection describes notes and solutions for using the action definition file for event log trapping (`nthevent.conf`) and the forwarding setting file (`forward`) when `KAJP1037-syslogoff` and `KAJP1037-hntroff` are not specified.

Suppose that your system links with IM Configuration Management of JP1/IM or uses the configuration management functionality of JP1/Base, and the `nvent . conf` and `forward` files are used with their initial settings. If forwarding of a JP1 event fails, the error message KAJP1037-E is output to the event log and converted to a JP1 event. The converted JP1 event is then transferred again, and another transfer failure occurs. To prevent the event transfer from looping, change the setting in the action definition file for event log trapping (`nvent . conf`), so that the KAJP1037-E message will not be trapped. For details about settings example of `nvent . conf`, see *Action definition file for event log trapping (Windows only)* in 16. *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 (`nvent . 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 (`nvent . conf`). For details on Windows event log monitoring jobs, see the *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *JP1/Automatic Job Management System 3 Administration Guide*.

(3) Notes on event logs forwarded from remote hosts

An event log trap cannot properly convert an event log entry generated by a remote machine to a JP1 event. To convert event log entries generated on a remote host, use an event log trap on the machine that generated the entry.

(4) Other notes

- If the event log trapping functionality reads event log data that contains any of the 3rd or 4th level JIS characters, these characters are replaced with question marks ("?"), and registered as JP1 events.
- The attribute of a JP1 event converted using the event log trap function has a value that is almost equal to the value displayed in the General tab of Event Viewer. However, the opcode (extended attribute A9) may differ from that displayed in the General tab of Event Viewer.

12

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.

12.1 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 *JP1/Integrated Management 3 - 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 *16. Definition Files*.

12.2 Setting the system's hierarchical configuration

For details about the settings for managing the hierarchical configuration of a system that includes JP1/Base and JP1/IM, see the section on setting a system's hierarchical configuration using the IM configuration management functionality and the section on setting a system's hierarchical configuration without using the IM configuration management functionality in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

This section explains how to specify the method for distributing configuration definition information when you set the system's hierarchical configuration.

12.2.1 Specifying the method for distributing configuration definition information

This subsection explains how to specify the method for distributing configuration definition information. You can also specify the distribution method as an option of the `jbsrt_distrib` command. For details about the `jbsrt_distrib` command, see *jbsrt_distrib* in 15. *Commands*.

1. Copy the model file for the common definition settings file (configuration management functionality) (`jbsrt_setup.conf.model`), and save the copy under a file name of your choice.

2. Edit the copy of the common definition settings file (configuration management functionality).

To set the distribution method to the differential distribution method, specify 1 for the `JBSRT_DISTRIB_VERSION` parameter. To set the distribution method to the batch distribution method, specify 0 for the `JBSRT_DISTRIB_VERSION` parameter.

This definition example sets the distribution method to the differential distribution method:

```
[JP1_DEFAULT\JP1BASE\JBS_ROUTE]
"JBSRT_DISTRIB_VERSION"=dword:00000001
```

For details about the common definition settings file (configuration management functionality), see *Common definition settings file (configuration management functionality)* in 16. *Definition Files*.

3. Execute the `jbssetcnf` command.

Execute the `jbssetcnf` command, specifying the common definition settings file (configuration management functionality) that was edited in step 2.

```
jbssetcnf name-of-file-edited-in-step-2
```

The settings in the common definition settings file (configuration management functionality) are applied to the common definition information.

For details about the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

4. Execute the `jbs_spm�_reload` command or restart JP1/Base to apply the common definition information.

For details about the `jbs_spm�_reload` command, see *jbs_spm�_reload* in 15. *Commands*.

The configuration definition information will now be updated by using the method specified in step 2.

12.3 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 *15. 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. For details on the procedure for setting the language, see *3.4.2 Setting the language (for UNIX)*.

12.3.1 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.

12.3.2 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/NT_LOGTRAP
end-to

[SubHost_B]
to ManagerHost
```

```
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/NT_LOGTRAP
end-to
```

```
[SubHost_C]
to ManagerHost
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/NT_LOGTRAP
end-to
```

```
[JP1host_1]
to SubHost_A
E.SEVERITY IN Error Warning
OR
E.PRODUCT_NAME IN /HITACHI/JP1/NT_LOGTRAP
end-to
```

```
[JP1host_2]
to SubHost_A
E.SEVERITY IN Error Warning
OR
E.PRODUCT_NAME IN /HITACHI/JP1/NT_LOGTRAP
end-to
```

12.4 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 16. *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 15. *Commands*.

Notes

- If definitions are already set on a destination host, the `jevdef_distrib` command first deletes the existing definitions before distributing definitions.
- The messages returned from each destination host when you execute the `jevdef_distrib` command conform to the language type set on that host. For details on the procedure for setting the language, see 3.4.2 *Setting the language (for UNIX)*. When distributing definitions from a Japanese-language manager to Japanese-language agents, the encoding of the distribution definition file is automatically converted when the language type differs between the manager and agent.

13

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.

13.1 Setting a local action

13.1.1 Defining a local action

The procedure for defining a local action is described below:

1. Register local action definitions to the common definition information.

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 *15. Commands*.

For details on the common definition settings file (local action function), see *Common definition settings file (local action function)* in *16. Definition Files*. If the common definition settings file (local action function) contains an error, the setting with the error is invalidated and the system operates as if the setting were omitted from the common definition information.

2. Create and edit the local action execution definition file (`jbsslact.conf`).

You must define the following items in the local action execution definition file:

- Execution conditions of the local action
- JP1 user name
- Execution command

All other items are optional. For details on the local action execution definition file, see *Local action execution definition file* in *16. 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 *8.1 User management setup (in Windows)* or *8.3 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 *16. Definition Files*. If the local action environment variable file contains an error, the commands cannot be executed.

5. Enable the local action definition.

To apply the information, execute the `jbs_spmd_reload` command. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *15. Commands*.

13.1.2 Changing local action settings

To change the execution conditions or execution commands of local actions:

1. Edit the local action execution definition file (`jbsslact.conf`).

For details on the local action execution definition file, see *Local action execution definition file* in 16. *Definition Files*.

2. Enable the settings in 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 15. *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.

13.1.3 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 15. *Commands*.

13.1.4 Pausing a local action

Use the following procedure to pause a local action to conduct maintenance or other tasks.

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 16. *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 15. *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 15. *Commands*.

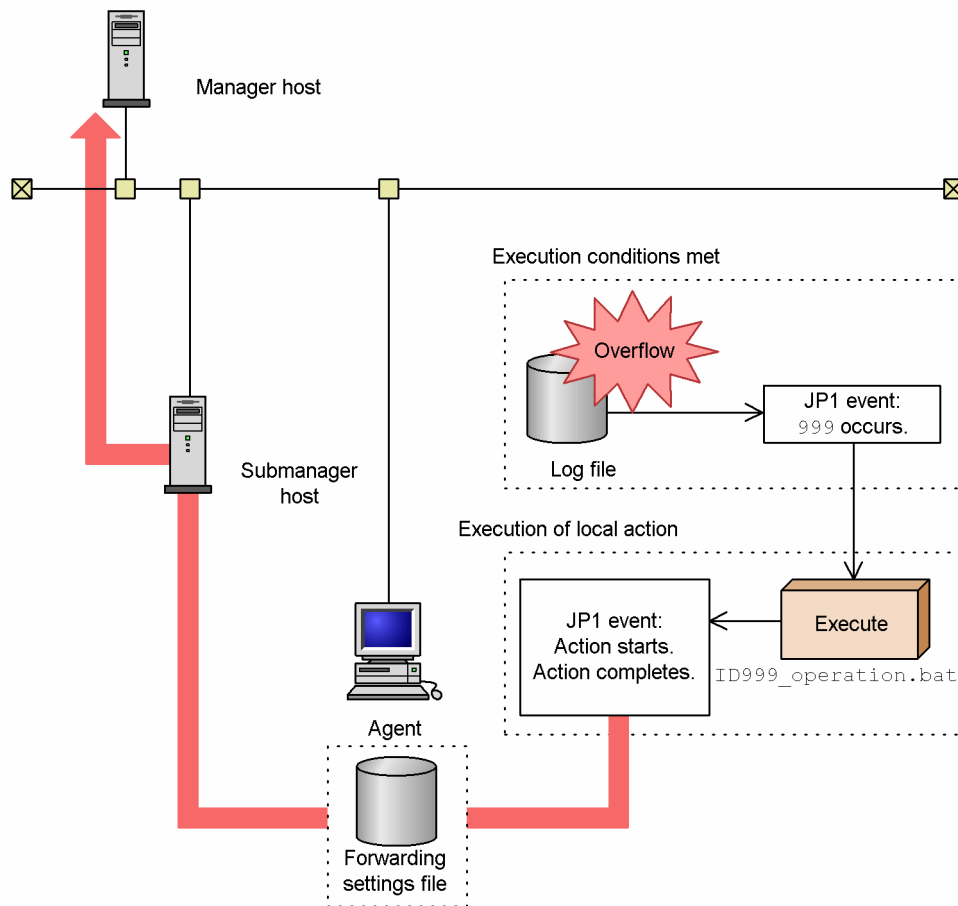
When a local action is paused, the local action remains in the state of having been started, and event acquisition stops. The actions in execution or in the queue are not canceled.

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 *16. Definition Files*.

13.2 Example of operating a local action

This section describes an example of a local action that executes a batch file (`ID999_operation.bat`) when a JP1 event (event ID: 999) indicating a log file overflow occurs. In this example, the file contains commands that initiate tasks such as backing up log files and starting the data collection tool. The example is based on the system configuration shown in the figure below.

Figure 13–1: Example of operating a local action



13.2.1 Setting the local action execution definition file

First of all, you need to set the local action execution definition 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 jpluser01
  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 [13.1.1 Defining a local action](#).

13.2.2 Setting the forwarding settings file

Use the following procedure to configure the forwarding settings file so that the action start event and action end event are forwarded to a higher-level manager host.

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 [10.1.3 Setting up an event service environment](#).

13.3 Notes on local actions

- Do not use perform the OS shutdown command (e.g. `shutdown` or `halt`) from a local action.
- The commands below cannot be executed as local action functions.
 - Commands requiring interactive operations
 - Commands that display a screen
 - Commands accompanied with escape sequences or control codes
 - Commands through which a daemon is not terminated
 - Commands requiring interaction with the desktop such as the Windows message mechanism or DDE (for Windows)
 - Commands for which data is input from the standard input
- The result of the command output to the KNAM3208-I message can be a maximum of 4095 bytes, including message text. Control characters are replaced with single-byte spaces when the characters appear in the output result.
- Only processes that were started by JP1/Base are forcibly terminated when an action that is running is canceled in Windows.
- Some commands executed by an action might remain if JP1/Base is stopped when the system load is high (e.g. when the CPU utilization is high or there are not enough user ports). To avoid such a situation, do the following when using a local action function:
 - Decrease the number of commands that can be simultaneously executed to reduce the load of the local action function.
 - Make sure actions do not establish further action conditions.
 - Avoid executing batch files where many commands are executed by one action.
- The service (`jbslcact` process) of a local action function connects to an event service during startup. A pause status is entered if the service cannot establish a connection. For operation using a cluster system, therefore, an event service must be started prior to the JP1/Base service.
- An event handled as a local action is an event registered after a local action function is started. An event registered during local action startup or a local action pause, or during a failover is not treated as an object.
- For local actions, execute the command using the following processing:
 - For Windows:
Execute `cmd.exe /c execution-command` from the local action.
 - For UNIX:
Using the OS user login shell, execute, for example, `/bin/sh -c execution-command` (if the login shell is `/bin/sh`) from the local action.
If `/sbin/false`, `/bin/false`, `/bin/true`, `/sbin/nologin`, or the like is set as the login shell, execution cannot be performed normally.
Furthermore, OS user passwords are not recognized, and therefore account locks and the like are not recognized.

14

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.

14.1 Modifying settings for JP1/Base

The following tables show when changes made to the JP1/Base settings during operation take effect. For details of how to modify settings, see the relevant section.

14.1.1 When changes take effect

(1) When JP1/Base troubleshooting settings take effect

No.	When settings are reflected	See:
1	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.	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.	4.

(2) When user management settings take effect

No.	When settings are reflected	See:
1	You can modify settings for the authentication server while JP1/Base is active provided that no JP1 products are using JP1/Base user authentication. The new settings take effect when you click the OK button in the GUI or when you execute the command.	In Windows: 8.1.1 In UNIX: 8.3.1
2	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.	In Windows: 8.1.2, 8.2.1(2) In UNIX: 8.3.2
3	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.	In Windows: 8.1.3 In UNIX: 8.3.3
4	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.	In Windows: 8.1.4 In UNIX: 8.3.4
5	You can modify the settings of user 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 (<code>jp1bs_ds_setup.conf</code>), the new settings will take effect after you execute the command.	8.2.1
6	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.	In Windows: 8.1.6, 8.1.7 In UNIX: 8.3.5

(3) When changes to service start and stop sequences take effect (Windows only)

No.	When settings are reflected	See:
1	If you modify the start sequence definition file (<code>JP1SVPRM.DAT</code>), the new settings take effect once you restart Windows.	<i>Start sequence definition file (Windows only)</i>

(4) When changes to the event service environment take effect

No.	When settings are reflected	See:
1	Changes are to be made to the event server index file (<code>index</code>) while the event service is stopped. When the event service is started up again after that, the settings are reflected.	<i>Event server index file</i>
2	If you modify settings in the event server settings file (<code>conf</code>), the new settings take effect once you restart the event service.	<i>Event server settings file</i>
3	If you modify settings in the forwarding settings file (<code>forward</code>), the new settings take effect once you execute the reload command.	<i>Forwarding settings file</i>
4	If you modify settings in the API settings file (<code>api</code>), the new settings take effect once you start or restart the event conversion functionality or a program (such as JP1/IM and JP1/AJS) that is linked with the event service.	<i>API settings file</i>

(5) When changes to event conversion settings take effect

No.	When settings are reflected	See:
1	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.	<i>Action definition file for log file trapping</i>
2	If you modify settings in the action definition file for event log trapping (<code>nthevent.conf</code>), the new settings take effect once you execute the reload command.	<i>Action definition file for event log trapping (Windows only)</i>

(6) When changes to the health check function take effect

No.	When settings are reflected	See:
1	If you modify settings in the health check definition file (<code>jbshc.conf</code>), the new settings take effect when you restart JP1/Base or execute the <code>jbs_spmd_reload</code> command.	<i>Health check definition file</i>

(7) When changes to Hitachi Network Objectplaza Trace Library (HNTRLib2) settings take effect

No.	When settings are reflected	See:
1	Settings take effect when you restart the Hitachi Network Objectplaza Trace Library (HNTRLib2).	<i>hntr2util (Windows only), hntr2util (UNIX only), hntr2utl2 (Windows only), hntr2utl2 (UNIX only), hntr2conf, hntr2getconf</i>

(8) When changes to communication settings take effect

No.	When settings are reflected	See:
1	If you modify <code>jp1hosts</code> information, the settings take effect once you execute the command and then restart JP1/Base.	6.5.2
2	If you modify <code>jp1hosts2</code> information, the settings take effect when you execute the command. However, when you change the following settings, the new setting will not take effect until you restart JP1/Base: <ul style="list-style-type: none">• The IP address allocated to the local host in the <code>jp1hosts2</code> information• The IP address in the <code>jp1hosts2</code> information for a host with which JP1/Base is communicating	6.6.2
3	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.	6.3
4	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.	6.5.3, 6.6.3

(9) When changes to local action function settings take effect

No.	When settings are reflected	See:
1	If you modify settings in the local action execution definition file, the new settings will take effect after you start or reload JP1/Base.	<i>Local action execution definition file</i>

(10) When changes to communication encryption function settings take effect

No.	When settings are reflected	See:
1	If you modify the settings of the communication encryption function, the new settings take effect after you execute the <code>jbsetcnf</code> command and restart JP1/Base, the products requiring JP1/Base (JP1/IM and JP1/AJS), and the programs that depend on JP1/Base.	6.13.4

14.2 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.

14.2.1 Effects and follow-up tasks when changing host names

(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 `jbssetusrsv` 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

For every agent host on which remote command execution is initiated from a manager, check the mapping definition file 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 *15. Commands*.

Note

For *server-host-name*, specify the host name displayed by the `hostname` command. However, if you are using domain names for DNS operation, add a host name definition in Fully Qualified Domain Name (FQDN) format.

(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 event server settings file (`conf`) and API settings file (`api`), you need to correct them completely. Only the host names set by users need to be corrected. You do not need to correct the default names. Since the event service does not automatically store default host names, you need not worry about correcting them.

If you use the `hostname` command to change the host name in UNIX, stop the event service first, and then change the name. If you change the host name while an event service is running, you will not be able to stop the event service.

When the stop processing of an event service is not completed due to a sudden power outage, the files listed below might remain. If any files remain, stop all event services running on the host and then delete the files. If you apply a JP1/Base patch while the files remain, KAJP1028-E and KAJP1049-E are issued. The patch is applied successfully even when KAJP1028-E and KAJP1049-E are issued.

In Windows

```
installation-folder\sys\tmp\event\process-ID.svr
```

```
installation-folder\sys\tmp\event\process-ID.lck
```

In UNIX

```
/var/opt/jp1base/sys/tmp/event/process-ID.svr
```

```
/var/opt/jp1base/sys/tmp/event/process-ID.lck
```

(4) When using JP1/IM - Manager

When you use **Read From Selected Event** in an event search, you need to set the `hosts` file 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.

With JP1/IM - Manager, the system is configured based on the contents of 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 *JP1/Integrated Management 3 - 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 how to delete a logical host name, see [5.7.1 Deleting logical hosts \(in Windows\)](#). For details on setting up a cluster system, see [5.4.3 Setup](#).

In UNIX:

For details on how to delete a logical host name, see [5.7.2 Deleting logical hosts \(in UNIX\)](#). For details on setting up a cluster system, see [5.5.3 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.

(7) jp1hosts definition file or jp1hosts2 definition file

If you are using a `jp1hosts` definition file or a `jp1hosts2` definition file, change the host name in the file.

14.2.2 Effects and follow-up tasks when changing IP addresses

To perform the required task:

1. Stop all products for which JP1/Base is a prerequisite program.
2. Stop JP1/Base.
3. Change the IP address.

Change the IP address in the `jp1hosts` definition file, `jp1hosts2` definition file, event server settings file, API settings file, and any other configuration files in which it appears. For details on when you need to set an IP address, and the files in which IP addresses are set, see [6.12 Situations that require communication settings](#).

4. Start JP1/Base.
5. Start all products for which JP1/Base is a prerequisite program.

14.2.3 Follow-up tasks when changing the system time

If you are using a NTP (Network Time Protocol) server or other method that never sets the system time to a time in the past, you do not need to follow the procedure below to synchronize the system clock. Also, you do not need to stop JP1/Base.

(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 *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and *JP1/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 *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and *JP1/Automatic Job Management System 3 Administration Guide*.

15

Commands

This chapter explains the syntax of JP1/Base 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.	<code>cpysvprm</code> (Windows only)	Yes	No	None

Command for checking the network setup

Functional overview	Command name	Windows	UNIX	Required execution permission
Checks network setup.	<code>jplping</code>	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 HNTRLlib2.	<code>hntr2mon</code> (UNIX only)	No	Yes	Superuser
Stops HNTRLlib2.	<code>hntr2kill</code> (UNIX only)	No	Yes	Superuser
Changes HNTRLlib2 settings.	<code>hntr2util</code> (Windows only)	Yes	No	Superuser
	<code>hntr2util</code> (UNIX only)	No	Yes	Superuser
	<code>hntr2utl2</code> (Windows only)	Yes	No	Superuser
	<code>hntr2utl2</code> (UNIX only)	No	Yes	Superuser
	<code>hntr2conf</code>	Yes	Yes	Superuser
Displays the HNTRLlib2 settings.	<code>hntr2getconf</code>	Yes	Yes	None
Outputs the names of program products that use HNTRLlib2.	<code>hntr2getname</code> (Windows only)	Yes	No	Superuser
Sets up JP1/Base.	<code>jplbase_setup</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
Starts JP1/Base including the event service.	<code>jbs_start</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
Stops JP1/Base including the event service.	<code>jbs_stop</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator

Functional overview	Command name	Windows	UNIX	Required execution permission
Starts JP1/Base processes other than the event service.	<code>jbs_spm�</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
Stops JP1/Base processes other than the event service.	<code>jbs_spm�_stop</code>	Yes	Yes	Superuser or JP1/Base administrator
Checks the status of JP1/Base processes other than the event service.	<code>jbs_spm�_status</code>	Yes	Yes	Superuser or JP1/Base administrator
Reloads JP1/Base processes other than the event service.	<code>jbs_spm�_reload</code>	Yes	Yes	Superuser or JP1/Base administrator
Sets up JP1/Base for use in a cluster system.	<code>jplbshasetup</code> (Windows only)	Yes	No	Superuser
	<code>jplbase_setup_cluster</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
	<code>jbs_setup_cluster</code> (Windows only)	Yes	No	Superuser
Starts JP1/Base in a cluster system.	<code>jbs_start.cluster</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
Stops JP1/Base in a cluster system.	<code>jbs_stop.cluster</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
Forcibly terminates all active JP1/Base processes in a cluster system.	<code>jbs_killall.cluster</code> (UNIX only)	No	Yes	Superuser
Starts the JP1/Base administrator console.	<code>jbsadmin</code> (Windows 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 or later.	<code>jcocmdconv</code>	Yes	Yes	Superuser

Commands for user management

Functional overview	Command name	Windows	UNIX	Required execution permission
Sets an authentication server.	<code>jbssetusrsv</code> (UNIX only)	No	Yes	Superuser or JP1/Base administrator
	<code>jbssetupsrv</code> (Windows only)	Yes	No	Superuser
Lists authentication servers.	<code>jbslistsrv</code>	Yes	Yes	Superuser or JP1/Base administrator
Blocks an authentication server.	<code>jbsblockadesrv</code>	Yes	Yes	Superuser or JP1/Base administrator
Unblocks an authentication server.	<code>jbsunblockadesrv</code>	Yes	Yes	Superuser or JP1/Base administrator

Functional overview	Command name	Windows	UNIX	Required execution permission
Registers a JP1 user.	<code>jbsadduser</code>	Yes	Yes	Superuser or JP1/ Base administrator
Deletes a JP1 user.	<code>jbsrmuser</code>	Yes	Yes	Superuser or JP1/ Base administrator
Lists registered JP1 users.	<code>jbslistuser</code>	Yes	Yes	Superuser or JP1/ Base administrator
Changes the password of a registered JP1 user.	<code>jbschgpasswd</code>	Yes	Yes	Superuser or JP1/ Base administrator
Registers JP1 user and DS group operating permissions.	<code>jbssetacl</code>	Yes	Yes	Superuser or JP1/ Base administrator
Deletes JP1 user or DS group operating permissions.	<code>jbsrmACL</code>	Yes	Yes	Superuser or JP1/ Base administrator
Displays registered JP1 user or DS group operating permissions.	<code>jbslistacl</code>	Yes	Yes	Superuser or JP1/ Base administrator
Registers JP1/Base administrators	<code>jbssetadmingrp</code> (UNIX only)	No	Yes	Superuser
Creates user mapping definitions and registers the information in the common definitions.	<code>jbsmkumap</code>	Yes	Yes	Superuser or JP1/ Base administrator [#]
Registers specific mapping information.	<code>jbssetumap</code>	Yes	Yes	Superuser or JP1/ Base administrator [#]
Deletes specific mapping information.	<code>jbsrmumap</code>	Yes	Yes	Superuser or JP1/ Base administrator
Lists registered mapping information.	<code>jbsgetumap</code>	Yes	Yes	Superuser or JP1/ Base administrator
Maintenance program for OS users' or information-search users' password management	<code>jbspasmgr</code> (Windows only)	Yes	No	Superuser
Registers an OS user or an information-search user, or changes the password of a registered OS user or information-search user.	<code>jbsumappass</code> (Windows only)	Yes	No	Superuser
Deletes an OS user or an information-search user.	<code>jbsrmumappass</code> (Windows only)	Yes	No	Superuser
Batch-registers password information of OS users or information-search users in the common definitions.	<code>jbsmkpass</code> (Windows only)	Yes	No	Superuser
Lists operating permission definitions registered on the authentication server.	<code>jbsacllint</code>	Yes	Yes	Superuser or JP1/ Base administrator
Reloads operating permission definitions to the authentication server.	<code>jbsaclreload</code>	Yes	Yes	Superuser or JP1/ Base administrator
Changes the directory server to be linked.	<code>jbschgds</code> (Windows only)	Yes	No	Superuser
Checks the settings of the directory server to be linked.	<code>jbschkds</code> (Windows only)	Yes	No	Superuser

[#]: You must have superuser permission to enter a superuser in the mapping information. An error occurs if you attempt to do so with JP1/Base administrator permission.

Commands for the event service

Functional overview	Command name	Windows	UNIX	Required execution permission
Reloads the forwarding settings file.	<code>jevreload</code>	Yes	Yes	Superuser or JP1/ Base administrator
Initializes the event database.	<code>jevdbinit</code>	Yes	Yes	Superuser or JP1/ Base administrator
Reorganizes a duplication prevention table	<code>jevdbmkrep</code>	Yes	Yes	Superuser or JP1/ Base administrator
Switches the event database.	<code>jevdbswitch</code>	Yes	Yes	Superuser or JP1/ Base administrator
Outputs the event database to a CSV file.	<code>jevexport</code>	Yes	Yes	None
Adds a service to the event server.	<code>jevregsvc</code> (Windows only)	Yes	No	Superuser
Manually starts the event service.	<code>jevstart</code> (UNIX only)	No	Yes	Superuser or JP1/ Base administrator
Manually stops the event service.	<code>jevstop</code> (UNIX only)	No	Yes	Superuser or JP1/ Base administrator
Checks the status of the event service.	<code>jevstat</code>	Yes	Yes	Superuser or JP1/ Base administrator
Registers a JP1 event on the event server.	<code>jevsend</code>	Yes	Yes	None
Registers a JP1 event in the event server and verifies its arrival at the destination server.	<code>jevsendd</code>	Yes	Yes	None
Reloads the action definition file for event log trapping.	<code>jeveltreload</code> (Windows only)	Yes	No	Superuser
Starts the log-file trap management daemon.	<code>jevlogdstart</code> (UNIX only)	No	Yes	Superuser or JP1/ Base administrator
Stops the log-file trap management daemon.	<code>jevlogdstop</code> (UNIX only)	No	Yes	Superuser or JP1/ Base administrator
Checks the status of the log-file trap management service (daemon).	<code>jevlogdstat</code>	Yes	Yes	Superuser or JP1/ Base administrator
Starts the log file trap.	<code>jevlogstart</code>	Yes	Yes	Superuser or JP1/ Base administrator
Stops the log file trap.	<code>jevlogstop</code>	Yes	Yes	Superuser or JP1/ Base administrator
Starts a log file trap (cluster environment only)	<code>jevlogstart</code> (cluster environment only)	Yes	Yes	Superuser or JP1/ Base administrator
Stops a log file trap (cluster environment only)	<code>jevlogstop</code> (cluster environment only)	Yes	Yes	Superuser or JP1/ Base administrator
Reloads the action definition file for log file trapping.	<code>jevlogreload</code>	Yes	Yes	Superuser or JP1/ Base administrator
Checks the operating status of the log file trap.	<code>jevlogstat</code>	Yes	Yes	Superuser or JP1/ Base administrator
Collects event service definitions.	<code>jevdef_get</code>	Yes	Yes	Superuser or JP1/ Base administrator

Functional overview	Command name	Windows	UNIX	Required execution permission
Distributes event service definitions.	<code>jevdef_distrib</code>	Yes	Yes	Superuser or JP1/ Base administrator
Suppresses event-forwarding, stops the event-forwarding suppression, and displays status of the event-forwarding suppression.	<code>jevagtfw</code>	Yes	Yes	Superuser or JP1/ Base administrator
Displays status of event-forwarding suppression for each suppression condition.	<code>jevfwstat</code>	Yes	Yes	Superuser or JP1/ Base administrator
Reloads an additional extended attribute settings file.	<code>jevextreload</code>	Yes	Yes	Superuser or JP1/ Base administrator
Changes the message IDs that are output to the Windows event log	<code>jevmessageid.bat</code> (Windows only)	Yes	No	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.	<code>Jiskeymnt</code>	Yes	Yes	Superuser or JP1/ Base administrator
Converts a file.	<code>Jisconv</code>	Yes	Yes	Superuser or JP1/ Base administrator
Checks a file.	<code>Jischk</code>	Yes	Yes	Superuser or JP1/ Base administrator
Extracts data from a file.	<code>Jisext</code>	Yes	Yes	Superuser or JP1/ Base administrator
Supports resource settings.	<code>Jislckreg</code> (UNIX only)	No	Yes	Superuser or JP1/ Base administrator
Displays records.	<code>Jisprt</code>	Yes	Yes	Superuser or JP1/ Base administrator
Deletes a resource.	<code>Jirsrdel</code> (UNIX only)	No	Yes	Superuser
Displays key definition information.	<code>Jisinfo</code>	Yes	Yes	Superuser or JP1/ Base administrator
Compresses files.	<code>Jiscond</code>	Yes	Yes	Superuser or JP1/ Base administrator
Extends the lock table.	<code>Jislckext</code>	Yes	Yes	Superuser
Displays lock table information.	<code>Jismlcktr</code> (Windows only)	Yes	No	Superuser
Deletes lock entry information.	<code>Jislckfree</code> (Windows only)	Yes	No	Superuser
Checks and releases file or record locks.	<code>Jislckclear</code> (Windows only)	Yes	No	Superuser
Copies files.	<code>Jiscpy</code>	Yes	Yes	Superuser or JP1/ Base administrator
Extracts records.	<code>Jisktod</code>	Yes	Yes	Superuser or JP1/ Base administrator

Commands for getting, setting, and deleting operating information and common definition

Functional overview	Command name	Windows	UNIX	Required execution permission
Collects operating information.	<code>jbsgetopinfo</code>	Yes	Yes	Superuser or JP1/ Base administrator
Collects common definition information.	<code>jbsgetcnf</code>	Yes	Yes	Superuser or JP1/ Base administrator
Registers common definition information.	<code>jbssetcnf</code>	Yes	Yes	Superuser or JP1/ Base administrator
Deletes common definition information.	<code>jbsunsetcnf</code>	Yes	Yes	Superuser or JP1/ Base administrator

Commands related to JP1-specific hosts information

Functional overview	Command name	Windows	UNIX	Required execution permission
Registers <code>jplhosts</code> information.	<code>jbshostsimport</code>	Yes	Yes	Superuser or JP1/ Base administrator
Registers <code>jplhosts2</code> information	<code>jbshosts2import</code>	Yes	Yes	Superuser or JP1/ Base administrator
Checks <code>jplhosts</code> information.	<code>jbshostsexport</code>	Yes	Yes	Superuser or JP1/ Base administrator
Checks <code>jplhosts2</code> information.	<code>jbshosts2export</code>	Yes	Yes	Superuser or JP1/ Base administrator

Commands for collecting JP1/Base setup information in a single operation and troubleshooting

Functional overview	Command name	Windows	UNIX	Required execution permission
Collects JP1/Base setup information in a single operation.	<code>jbsparamdump</code>	Yes	Yes	Superuser or JP1/ Base administrator
Collects data if an error occurs.	<code>jbs_log.bat</code> (Windows only)	Yes	No	Superuser
	<code>jbs_log.sh</code> (UNIX only)	No	Yes	Superuser or JP1/ Base administrator

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.	<code>jbsrt_distrib</code>	Yes	Yes	Superuser or JP1/ Base administrator
Collects the JP1/IM configuration definition information from the lower-level hosts, and then updates the information.	<code>jbsrt_sync</code>	Yes	Yes	Superuser or JP1/ Base administrator

Functional overview	Command name	Windows	UNIX	Required execution permission
Deletes the JP1/IM configuration definition information.	<code>jbsrt_del</code>	Yes	Yes	Superuser or JP1/Base administrator
Displays the JP1/IM configuration definition information.	<code>jbsrt_get</code>	Yes	Yes	Superuser or JP1/Base administrator

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.	<code>jbslistlcact</code>	Yes	Yes	Superuser or JP1/Base administrator
Cancels the waiting or running local actions.	<code>jbscancellcact</code>	Yes	Yes	Superuser or JP1/Base administrator
Configures the JP1/IM command execution environment.	<code>jcocmdef</code>	Yes	Yes	Superuser or JP1/Base administrator
Outputs the JP1/IM command execution logs.	<code>jcocmdlog</code>	Yes	Yes	None
Deletes the commands executed by JP1/IM - View or automated actions.	<code>jcocmdel</code>	Yes	Yes	Superuser or JP1/Base administrator
Checks the operating status of the commands executed by JP1/IM - View or automated actions.	<code>jcocmdshow</code>	Yes	Yes	Superuser or JP1/Base administrator

Command used for communication encryption

Functional overview	Command name	Windows	UNIX	Required execution permission
Command provided by OpenSSL	<code>openssl</code>	Yes	Yes	See the official website of OpenSSL.

In the following pages, the commands listed above are explained in alphabetical order.

JP1/Base administrator console (for Windows)

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.

Starting the administrator console

From the Windows **Start** menu, choose **Programs, JP1_Base**, and then **JP1_Base Console**.

Stopping the administrator console

Enter the `exit` command from the command prompt, or click the **Close** button (X).

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 contents of the profile batch program:

```
@echo off

rem #-----
rem # In this space you can set the profile information (such as an enviro
rem # nment variable)
rem # for the administrator console of JP1/Base.
rem #-----

echo JP1/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 enviro
rem # nment variable)
rem # for the administrator console of JP1/Base.
rem #-----

echo JP1/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 `hntr2utl2` 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]  
          [-t type-of-exclusive-control]  
          [-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:

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)
`system-drive\Program Files (x86)\Hitachi\HNTRLib2\bin\
HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)
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`. The initial setting is as follows:

For Windows:

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)
`system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2*.log
HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)
system-drive\Program Files\Hitachi\HNTRLib2\spool\hntr2*.log`

For UNIX:

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

-b log-file-size

Specify the size of the integrated trace logs (8 to 8,192 KB). The initial setting is 256 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. The initial setting is 4.

-s buffer-file-size

Specify the buffer file size (8 to 2,048 KB). The initial setting is 64 KB.

-w monitoring-period

Specify the period for monitoring the log file (1 to 300 seconds). The initial setting is 10 seconds.

-i monitoring-interval

Specify the interval for monitoring the log file (0 to 3,600 seconds). Do not change this value from the default.

-m number-of-messages

Specify the maximum number of messages output by the command (0 to 500). Do not change this value from the default.

-t type-of-exclusive-control

Specify the type of exclusive control for the integrated trace log. Specify 0 to disable exclusive control and specify 2 to enable exclusive control. If you omit this parameter, 0 is assumed.

-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 `hntr2uti2` 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 `hntr2uti2` command.
- If you when modify the buffer file size or the type of exclusive control, follow the procedure below to modify the settings.

In Windows:

1. Stop all the services that output log data to the integrated trace log.
2. Terminates the Hitachi Network Objectplaza Trace Library.
3. Modify the settings of the integrated trace log.
4. Starts the Hitachi Network Objectplaza Trace Library.
5. Start the service that outputs the integrated trace log stopped in 1.

In UNIX:

1. Stop all the services that output log data to the integrated trace log.
2. Terminates the Hitachi Network Objectplaza Trace Library.
3. Modify the settings of the integrated trace log.
4. Delete the memory-mapped file(/opt/hitachi/HNTRLib2/mmap/hntr2mmap.mm).
5. Starts the Hitachi Network Objectplaza Trace Library.
6. Start the service that outputs the integrated trace log stopped in 1.

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 <code>-f</code> option does not exist.
11	The log file size specified by the <code>-b</code> option is too small.
12	The buffer file size specified by the <code>-s</code> 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.

Format

```
hntr2getconf [-f]
              [-b]
              [-n]
              [-s]
              [-w]
              [-i]
              [-m]
              [-t]
              [-l command-log-file-name]
              [-h]
```

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)
system-drive\Program Files (x86)\Hitachi\HNTRLib2\bin\
HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)
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.

-t

Outputs the type of exclusive control.

-l *command-log-file-name*

Specify this option if you want to save the results read by the options to a log file.

-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):

```
> hnttr2getconf.exe -b
8
>
```

When multiple options are specified (in UNIX):

```
$ hnttr2getconf -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

Key name	Option name
MapSize	-s
WatchDog	-w
IntervalSec	-i
MaxMsgNum	-m
ShmLockType	-t

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

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)

system-drive\Program Files (x86)\Hitachi\HNTRLib2\bin\

HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)

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).

This command is for compatibility. Use the `hntr2utl2` command.

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: Size of a log file.
Specify the log file size (8 to 4,096 KB). The initial setting is 256 KB.
- 2: Number of log files.
Specify the number of log files (1 to 16). The initial setting is 4.
- 3: Size of buffer.
Specify the buffer file size (8 to 1,024 KB). The initial setting is 64 KB.
- 4: Watch dog time.
Specify the interval for monitoring the log file (1 to 300 seconds). The initial setting is 10 seconds.
- 5: Name of log files.
Enter the output path. The initial setting is `/var/opt/hitachi/HNTRLib2/spool/hntr2*.log`.

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.

JP1 Service

$7.5 \times \text{number-of-starts-and-stops-per-day}$ (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

$0.2 \times \text{number-of-logins-from-JP1/AJS - View} + 0.2 \times \text{number-of-command-executions}^\#$ (kilobytes)

#: Execute the command

`jbsadduser, jbsrmuser, jbschgpasswd, jbsacllint, jbsaclreload, jbslistuser, jbschkds, jbschgds, jbssetacl, jbsrmacl`

Log file trapping

$(0.5 + \text{length-of-action-definition-file-name-for-log-file-trapping} + \text{length-of-log-file-name}) \times \text{number-of-starts-per-day} + 0.2 \times \text{number-of-stops-per-day}$ (kilobytes)

JP1/IM

$(0.16 + \text{automated-action-command-length}) \times \text{number-of-times-automated-action-runs-per-day} + 0.4 \times \text{number-of-times-automated-action-is-changed-from-JP1/IM - View} + 0.16 \times \text{number-of-logins-from-JP1/IM - View-to-JP1/IM - Manager} + (0.16 + \text{command-length-on-command-execution-screen}) \times \text{number-of-command-executions-per-day}$ (kilobytes)

JP1/AJS

$\text{number-of-times-startup-conditions-are-satisfied} \times 0.2$ (kilobytes)

- If you modified the settings for the Hitachi Network Objectplaza Trace Library (HNTRLib2), you must restart it according to the following procedure:
 - Stop the integrated trace collection process by executing the following command:
`/opt/hitachi/HNTRLib2/bin/hntr2kill`
 - Start the integrated trace collection process by executing the following command:
`/opt/hitachi/HNTRLib2/bin/hntr2mon -d &`
- If you when modify the buffer file size, follow the procedure below to modify the settings.
 - Stop all the services that output log data to the integrated trace log.
 - Terminates the Hitachi Network Objectplaza Trace Library.
 - Modify the settings of the integrated trace log.
 - Delete the memory-mapped file(`/opt/hitachi/HNTRLib2/mmap/hntr2mmap.mm`).
 - Starts the Hitachi Network Objectplaza Trace Library.
 - Start the service that outputs the integrated trace log stopped in 1.
- If the log file size or buffer file size exceeds the upper limit that can be set using this command, the settings cannot be changed. Use the `hntr2utl2` command.

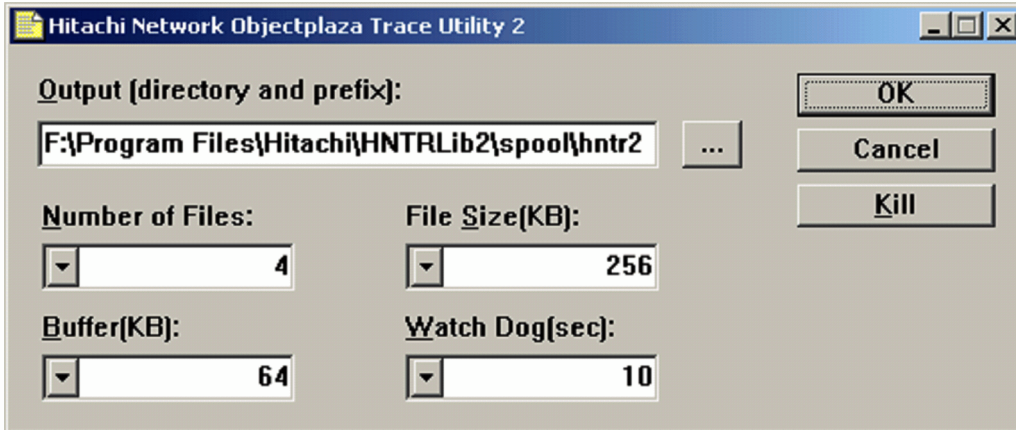
hntr2util (Windows only)

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).

This command is for compatibility. Use the `hntr2util2` command.

At command execution, the following dialog box appears.



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 following output destination is specified by default:

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)

```
system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2*.log
```

HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)

```
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)

Specify the buffer file size (8 to 1,024 KB). The initial setting is 64 KB.

Watch Dog (sec)

Specify the interval for monitoring the log file (1 to 300 seconds). The initial setting is 10 seconds.

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

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)

```
system-drive\Program Files (x86)\Hitachi\HNTRLib2\bin\
```

HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)

```
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.

JP1 Service

$7.5 \times \text{number-of-starts-and-stops-per-day}$ (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

$0.2 \times \text{number-of-logins-from-JP1/AJS - View} + 0.2 \times \text{number-of-command-executions}^\#$ (kilobytes)

#: Execute the command

```
jbsadduser, jbsrmuser, jbschgpasswd, jbsacllint, jbsaclreload, jbslistuser,  
jbschkds, jbschgds, jbssetacl, jbsrmacl
```

Log file trapping

$(0.5 + \text{length-of-action-definition-file-name-for-log-file-trapping} + \text{length-of-log-file-name}) \times$
 $\text{number-of-starts-per-day} + 0.2 \times \text{number-of-stops-per-day}$ (kilobytes)

JP1/IM

$(0.16 + \text{automated-action-command-length}) \times \text{number-of-times-automated-action-runs-per-day} +$
 $0.4 \times \text{number-of-times-automated-action-is-changed-from-JP1/IM - View} + 0.16 \times \text{number-of-logins-}$
 $\text{from-JP1/IM - View-to-JP1/IM - Manager} + (0.16 + \text{command-length-on-command-execution-screen}) \times$
 $\text{number-of-command-executions-per-day}$ (kilobytes)

JP1/AJS

$\text{number-of-times-startup-conditions-are-satisfied} \times 0.2$ (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**).

- If you when modify the buffer file size, follow the procedure below to modify the settings.
 1. Stop all the services that output log data to the integrated trace log.
 2. Terminates the Hitachi Network Objectplaza Trace Library.
 3. Modify the settings of the integrated trace log.
 4. Starts the Hitachi Network Objectplaza Trace Library.
 5. Start the service that outputs the integrated trace log stopped in 1.
- If the log file size or buffer file size exceeds the upper limit that can be set using this command, the settings cannot be changed. Use the `hntr2utl2` command.

hntr2utl2 (UNIX only)

Function

The `hntr2utl2` 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 2.0

Select the item you want to change. (Type 1-7 or e)

  [Log Files]
  1: Size of a log file.      256 KB
  2: Number of log files.    4
  3: Name of log files.      /var/opt/hitachi/HNTRLib2/spool/hntr2*.log

  [Monitor]
  4: Size of buffer.         64 KB
  5: Interval timer.         10 Sec

  [Logging Restriction]
  6: Lookout span.           0 Sec
  7: Max messages per span.  0

  e: Exit

Enter the number> 1
```

The menu has the following items.

- 1: Size of a log file.
Specify the log file size (8 to 8,192 KB). The initial setting is 256 KB.
- 2: Number of log files.
Specify the number of log files (1 to 16). The initial setting is 4.
- 3: Name of log files.
Enter the output path. The initial setting is `/var/opt/hitachi/HNTRLib2/spool/hntr2*.log`.
- 4: Size of buffer.
Specify the buffer file size (8 to 2,048 KB). The initial setting is 64 KB.
- 5: Interval timer.
Specify the interval for monitoring the log file (1 to 300 seconds). The initial setting is 10 seconds.
- 6: Lookout span.
Specify the interval for monitoring the log file (1 to 3,600 seconds). Do not change this from the initial setting.
- 7: Max message per span.
Specify the range (0 to 500) for the number of messages to be output by the command. Do not change this from the initial setting.

Format

```
hntr2utl2
```

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.

JP1 Service

$7.5 \times \text{number-of-starts-and-stops-per-day}$ (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

$0.2 \times \text{number-of-logins-from-JP1/AJS - View} + 0.2 \times \text{number-of-command-executions}^\#$ (kilobytes)

#: Execute the command

jbsadduser, jbsrmuser, jbschgpasswd, jbsacllint, jbsaclreload, jbslistuser, jbschkds, jbschgds, jbssetacl, jbsrmacl

Log file trapping

$(0.5 + \text{length-of-action-definition-file-name-for-log-file-trapping} + \text{length-of-log-file-name}) \times \text{number-of-starts-per-day} + 0.2 \times \text{number-of-stops-per-day}$ (kilobytes)

JP1/IM

$(0.16 + \text{automated-action-command-length}) \times \text{number-of-times-automated-action-runs-per-day} + 0.4 \times \text{number-of-times-automated-action-is-changed-from-JP1/IM - View} + 0.16 \times \text{number-of-logins-from-JP1/IM - View-to-JP1/IM - Manager} + (0.16 + \text{command-length-on-command-execution-screen}) \times \text{number-of-command-executions-per-day}$ (kilobytes)

JP1/AJS

$\text{number-of-times-startup-conditions-are-satisfied} \times 0.2$ (kilobytes)

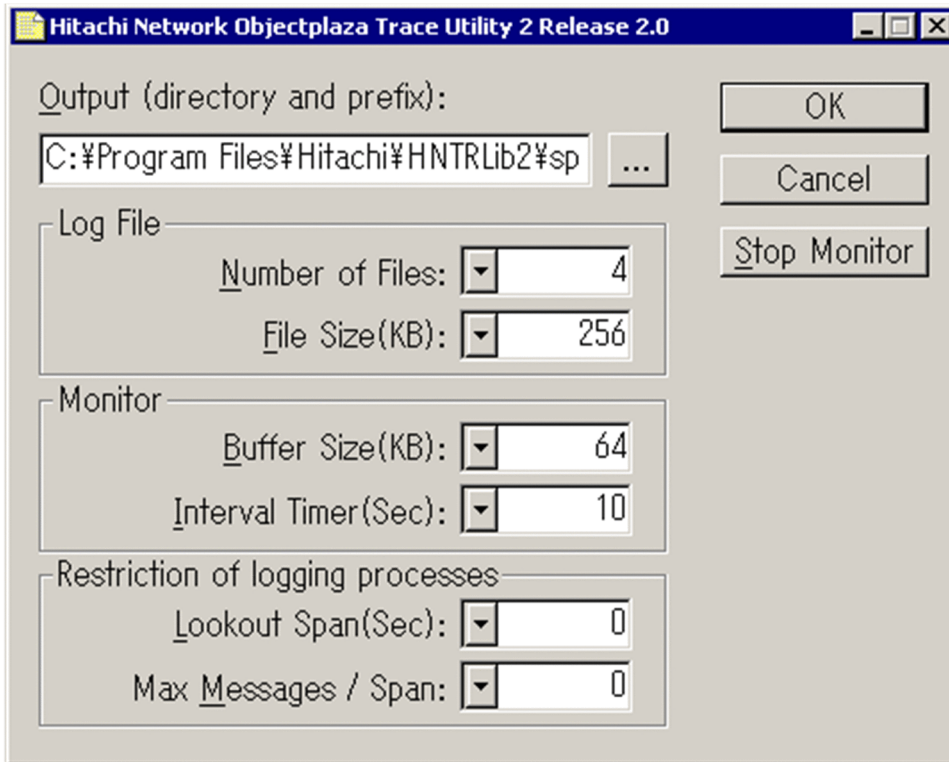
- If you modified the settings for the Hitachi Network Objectplaza Trace Library (HNTRLib2), you must restart it according to the following procedure:
 - Stop the integrated trace collection process by executing the following command:
`/opt/hitachi/HNTRLib2/bin/hntr2kill`
 - Start the integrated trace collection process by executing the following command:
`/opt/hitachi/HNTRLib2/bin/hntr2mon -d &`
- If you when modify the buffer file size, follow the procedure below to modify the settings.
 - Stop all the services that output log data to the integrated trace log.
 - Terminates the Hitachi Network Objectplaza Trace Library.
 - Modify the settings of the integrated trace log.
 - Delete the memory-mapped file(/opt/hitachi/HNTRLib2/mmap/hntr2mmap.mm).
 - Starts the Hitachi Network Objectplaza Trace Library.
 - Start the service that outputs the integrated trace log stopped in 1.

hntr2utl2 (Windows only)

Function

The `hntr2utl2` 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.



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 following output destination is specified by default:

HNTRLib2 for 32bit (If setting an integrated trace for 32-bit processes)

```
system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2*.log
```

HNTRLib2 for 64bit (If setting an integrated trace for 64-bit processes)

```
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 8,192 KB). The default is 256 KB.

Buffer (KB)

Specify the buffer file size (8 to 2,048 KB). The initial setting is 64 KB.

Interval Timer (Sec)

Specify the interval for monitoring the log file (1 to 300 seconds). The initial setting is 10 seconds.

Lookout Span(Sec)

Specify the interval for monitoring the log file (1 to 3,600 seconds). Do not change this from the initial setting.

Max Messages / Span

Specify the range (0 to 500) for the number of messages to be output by the command. Do not change this from the initial setting.

OK button

Applies the entered settings and closes the dialog box.

Cancel button

Closes the dialog box without applying the entered settings.

Stop Monitor button

Terminates the monitoring process currently executing. You can stop the HNTRLlib2 service (service name: **Hitachi Network Objectplaza Trace Monitor 2**) using the **Stop Monitor** button, but you should normally do this from the Services dialog box that opens from the Windows Control Panel.

Format

```
hntr2utl2
```

Required execution permission

Administrators

Command directory

HNTRLlib2 for 32bit (If setting an integrated trace for 32-bit processes)

```
system-drive\Program Files (x86)\Hitachi\HNTRLlib2\bin\
```

HNTRLlib2 for 64bit (If setting an integrated trace for 64-bit processes)

```
system-drive\Program Files\Hitachi\HNTRLlib2\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.

JP1 Service

$7.5 \times \text{number-of-starts-and-stops-per-day}$ (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

$0.2 \times \text{number-of-logins-from-JP1/AJS - View} + 0.2 \times \text{number-of-command-executions}^\#$ (kilobytes)

#: Execute the command

```
jbsadduser, jbsrmuser, jbschgpasswd, jbsacllint, jbsaclreload, jbslistuser,  
jbschkds, jbschgds, jbssetacl, jbsrmacl
```

Log file trapping

$(0.5 + \textit{length-of-action-definition-file-name-for-log-file-trapping} + \textit{length-of-log-file-name}) \times \textit{number-of-starts-per-day} + 0.2 \times \textit{number-of-stops-per-day}$ (kilobytes)

JP1/IM

$(0.16 + \textit{automated-action-command-length}) \times \textit{number-of-times-automated-action-runs-per-day} + 0.4 \times \textit{number-of-times-automated-action-is-changed-from-JP1/IM-View} + 0.16 \times \textit{number-of-logins-from-JP1/IM-View-to-JP1/IM-Manager} + (0.16 + \textit{command-length-on-command-execution-screen}) \times \textit{number-of-command-executions-per-day}$ (kilobytes)

JP1/AJS

$\textit{number-of-times-startup-conditions-are-satisfied} \times 0.2$ (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**).
- If you when modify the buffer file size, follow the procedure below to modify the settings.
 1. Stop all the services that output log data to the integrated trace log.
 2. Terminates the Hitachi Network Objectplaza Trace Library.
 3. Modify the settings of the integrated trace log.
 4. Delete the memory-mapped file(/opt/hitachi/HNTRLib2/mmap/hntr2mmap.mm).
 5. Starts the Hitachi Network Objectplaza Trace Library.
 6. Start the service that outputs the integrated trace log stopped in 1.

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/jplbase/`

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 32 bytes and forcibly terminates the associated process. You cannot kill a process for a logical host whose name exceeds 32 bytes. In this scenario, use the `ps` command to identify the process and then kill it using the `kill` command.
- 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 `jp1_default` folder in the specified data folder. If you specify the `-h` option, in addition to the `jp1_default` 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
<code>data-folder\jp1_default\base_1st\conf\</code>	Settings and definition files
<code>data-folder\jp1_default\base_1st\log\</code>	Log file
<code>data-folder\jp1_default\base_1st\allusers\jp1_default\JP1Base\log</code>	Log file
<code>data-folder\jp1_default\base_1st\allusers\logical-host-name\JP1Base\log</code>	Log file
<code>data-folder\jp1_default\base_1st\sys\</code>	OS system information
<code>data-folder\jp1_default\base_1st\sys\tmp\event\</code>	Event server settings
<code>data-folder\jp1_default\base_1st\sys\OPI</code>	Information on the operation of services
<code>data-folder\jp1_default\base_1st\default\</code>	Common definition information
<code>data-folder\jp1_default\base_1st\plugin\conf\</code>	Plug-in service settings file
<code>data-folder\jp1_default\base_1st\spool\</code>	Integrated trace logs (32bit)
<code>data-folder\jp1_default\base_1st\spoolx64\</code>	Integrated trace logs (64bit)
<code>data-folder\jp1_default\base_2nd\log\Command\</code>	Command execution log files
<code>data-folder\jp1_default\base_2nd\sys\</code>	Event database
<code>data-folder\logical-host-name\base_1st\conf\</code>	Settings and definition files for the logical host (if applicable)
<code>data-folder\logical-host-name\base_1st\log\</code>	Log data for the logical host (if applicable)
<code>data-folder\logical-host-name\base_1st\event\</code>	Event server settings for the logical host (if applicable)
<code>data-folder\logical-host-name\base_1st\sys\OPI</code>	Information on the operation of services for the logical host
<code>data-folder\logical-host-name\base_2nd\sys\</code>	Command execution log files for the logical host (if applicable)
<code>data-folder\logical-host-name\base_2nd\event\</code>	Event database for the logical host (if applicable)

For details on the types of data that you can collect with this tool, see [18.3 Data that must be collected when a problem 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.

You must specify the logical host name in this option if you use JP1/Base on a cluster system. You cannot use the environment variable JP1_HOSTNAME.

data-folder

Specify the folder to which you want to output the collected data, 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. Furthermore, do not specify a folder on a network drive.

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.

Notes

- When collecting data from the event server, if the names of the directories accessed by the event server are changed to full path in the event server index file, you cannot collect data from the altered event server directories. If an error occurs, in addition to gathering data, use the data collection tool to collect all the directories specified in the event server index file as information for investigating the problem.
- Do not run multiple data collection tools concurrently.
- The data collection tool may take 10 minutes or longer to run. Do not forcibly terminate the data collection tool if it does not end promptly.
- When a data collection tool is executed, the system information may not be collected even though the tool has completed execution. This problem occurs because the process that collects OS information internally had not ended when the data collection tool completed execution.
Open the Task Manager and in the Processes page make sure that `msinfo32.exe` has ended before you archive the data using a compression tool, or move, delete, or otherwise operate on the data.
- If the output directory for the integrated trace log is changed, you cannot collect data from the changed output directory for the integrated trace log. If an error occurs, in addition to collecting data, collect all the data from the changed output directory for the integrated trace log in order to investigate the problem.

Return values

0	Normal end
8	Abnormal end <ul style="list-style-type: none">• 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.

This tool archives the specified directories or files in the root directory using the `tar` command, and then compresses the archive using the `compress` command (or the `gzip` command in Linux). 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
<code>data-directory/jp1_default_base_1st/var/opt/jp1base/conf/</code>	Settings and definition files
<code>data-directory/jp1_default_base_1st/var/opt/jp1base/log/</code>	Log file
<code>data-directory/jp1_default_base_1st/var/opt/jp1base/log/sys/</code>	<ul style="list-style-type: none">OS system information<code>jbs_spmd_status</code> command execution results
<code>data-directory/jp1_default_base_1st/var/opt/jp1base/sys/tmp/event/</code>	Event server settings
<code>data-directory/jp1_default_base_1st/var/opt/jp1base/sys/OPI</code>	Information on the operation of services
<code>data-directory/jp1_default_base_1st/var/opt/jp1base/plugin/conf/</code>	Plug-in service settings file
<code>data-directory/jp1_default_base_1st/var/opt/hitachi/HNTRLib2/spool/</code>	Integrated trace logs
<code>data-directory/jp1_default_base_1st/opt/jp1/hcclibcnf/</code>	Common definition information
<code>data-directory/jp1_default_base_2nd/var/opt/jp1base/Command/</code>	Command execution log files
<code>data-directory/jp1_default_base_2nd/var/opt/jp1base/sys/event/</code>	Event database
<code>data-directory/jp1_default_base_2nd/usr/tmp/jp1_ses/</code>	Settings file for compatibility
<code>data-directory/jp1_default_base_2nd/usr/lib/jp1_ses/</code>	
<code>data-directory/jp1_default_base_2nd/usr/bin/jp1_ses/</code>	
<code>data-directory/jp1_default_base_2nd/tmp/</code>	
<code>data-directory/jp1_default_base_2nd/var/opt/jp1_ses/</code>	
<code>data-directory/logical-host-name_base_1st/etc/opt/jp1base/log/</code>	Log files for the logical host
<code>data-directory/logical-host-name_base_1st/etc/opt/jp1base/conf/</code>	Settings and definition files for the logical host (if applicable)
<code>data-directory/logical-host-name_base_1st/shared-directory/event/</code>	Event server settings for the logical host (if applicable)
<code>data-directory/logical-host-name_base_1st/shared-directory/jp1base/sys/OPI</code>	Information on the operation of services for the logical host
<code>data-directory/logical-host-name_base_2nd/shared-directory/event/</code>	Event database for the logical host (if applicable)

Command directory	Collected data
<i>data-directory/</i> 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 [18.3 Data that must be collected when a problem 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 permission or JP1/Base administrator permission

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:

OS other than Linux

/tmp/jp1base/jp1_default_base_1st.tar.Z

/tmp/jp1base/jp1_default_base_2nd.tar.Z

Linux

/tmp/jp1base/jp1_default_base_1st.tar.gz

/tmp/jp1base/jp1_default_base_2nd.tar.gz

For a logical host:

OS other than Linux

/tmp/jp1base/logical-host-name_base_1st.tar.Z

/tmp/jp1base/logical-host-name_base_2nd.tar.Z

Linux

/tmp/jp1base/*logical-host-name*_base_1st.tar.gz

/tmp/jp1base/*logical-host-name*_base_2nd.tar.gz

-k

Specify this option if you do not want to collect logs on compatibility settings file.

-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.

You must specify the logical host name in this option if you use JP1/Base on a cluster system. You cannot use the environment variable `JP1_HOSTNAME`.

Notes

- When the name of the directory used by an event server is changed to a full path name in the event server index file (`index`), the data collection tool does not collect data about the event server. If an error has occurred, collect the information on the directory changed by specifying the following option in the data collection tool:

```
jbbs_log.sh user-specified-option [directory-specified-in-the-index-file]
```

- For operation in an environment in which the core file name is changed, data cannot be collected using the data collection tool. Therefore, collect data separately during data collection.
- If the output directory for the integrated trace log is changed, you cannot collect data from the changed output directory for the integrated trace log. If an error occurs, collect the data from the changed integrated trace log directory by specifying the following option:

`jbs_log.sh user-specified-option [output-directory-for-the-integrated-trace-log]`

- In SUSE Linux Enterprise Server 12 SP2 or later, the specifications related to the core dump were changed, so the data collection tool can no longer be used to collect core dump files. For this reason, we might also ask you to collect core dump files separately. The output destination of core dump files is as follows:

`/var/lib/systemd/coredump/`

Return values

0	Normal end
8	<ul style="list-style-type: none">• 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 `jplbase_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]] | -r]
                    [-v]
```

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*\conf to the appropriate shared folder.

Folder	Files to be contained
<i>shared-folder</i> \jplbase\conf\	Definition files
<i>shared-folder</i> \jplbase\log\	Log file
<i>shared-folder</i> \jplbase\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.
- 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. 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 permission or JP1/Base administrator permission

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 JP1/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 permission or JP1/Base administrator permission

Command directory

In Windows:

```
installation-folder\bin\
```

In UNIX:

```
/opt/jplbase/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 you logged in from a viewer such as JP1/IM - View and the `jbs_spmd_reload` command is executed on the authentication server host, your authentication might be canceled. In this case, reattempt to log in.
- When the JP1 authentication information of DS users is reloaded from the directory server, some users might not be accepted as JP1 users, for example, because the user name conflicts with the name of a standard user or the length of the user name exceeds the maximum length of a JP1 user name. Use the `jbslistuser` and `jbslistacl`

commands to check whether the user names are acceptable. The information of users who were not accepted is recorded as warning messages in the integrated trace log of the authentication server.

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:

```
jbsessionmgr
jbsroute
jcocmd
jbsplugin
jbsbcd
jbsbchostd
jbsrvmgr
jbslact
jbscmd
```

If an authentication server has not been set:

```
jbsroute
jcocmd
jbsplugin
jbsbcd
jbsbchostd
jbsrvmgr
jbslact
jbscmd
```

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 permission or JP1/Base administrator permission

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 or JP1/Base administrator permission

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/jplbase
cp -p jbs_start.model jbs_start
```

Format

```
jbs_start
```

Required execution permission

Superuser or JP1/Base administrator permission

Command directory

/etc/opt/jplbase/

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_spmc_status` command.
- In Linux, the maximum size for core file dumps is sometimes set to 0 by default. In this case, the system will not output a core dump file. To avoid this issue, the `jbs_start` and `jbs_start.cluster` scripts contain the following standard setting:

```
if [ 'uname' = Linux ]; then
ulimit -c unlimited
fi
```

If this setting contravenes the security policy of the system on which the script is executed, comment it out by placing a hash mark (#) at the beginning of each line.

```
#if [ 'uname' = Linux ]; then
#ulimit -c unlimited
#fi
```

This invalidates the setting. However, it also means that the system will not create a core dump file when an event such as a segmentation fault or bus error that would usually trigger a core dump occurs in the JP1/Base process, denying you information that could be used to investigate the cause.

- 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 JP1/Base processes started.
- In the following cases, you must specify Japanese as the language of the `LANG` environment variable of the automatic start script:

- When Japanese is specified in the event filter of the forwarding settings file (`forward`).
- When Japanese is specified in the `lpSzFilter` parameter of the JP1 event acquisition function (`JevGetOpen`) in the user program.
- When Japanese is specified in various JP1/IM filters in JP1/IM[#].
#: For detailed conditions of servers that require language specification, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- The automatic start script (`jbs_start`) performs an unsetup of the locale settings of `LC_ALL`, `LC_COLLATE`, `LC_CTYPE`, `LC_MONETARY`, `LC_NUMERIC`, `LC_TIME`, and `LC_MESSAGES` by default.

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 or JP1/Base administrator permission

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.
- In Linux, the maximum size for core file dumps is sometimes set to 0 by default. In this case, the system will not output a core dump file. To avoid this issue, the `jbs_start` and `jbs_start.cluster` scripts contain the following standard setting:

```
if [ 'uname' = Linux ]; then
ulimit -c unlimited
fi
```

If this setting contravenes the security policy of the system on which the script is executed, comment it out by placing a hash mark (#) at the beginning of each line.

```
#if [ 'uname' = Linux ]; then
#ulimit -c unlimited
#fi
```

This invalidates the setting. However, it also means that the system will not create a core dump file when an event such as a segmentation fault or bus error that would usually trigger a core dump occurs in the JP1/Base process, denying you information that could be used to investigate the cause.

- When you execute the `jbs_start.cluster` command, a message might appear indicating that the log file trap management daemon is already running. You can prevent this message from appearing by modifying the `jbs_start.cluster` script. Note that you do not need to modify the script if you performed a new installation of JP1/Base version 10-00 or later.

The `jbs_start.cluster` script contains the following setting:

```
## Start services
echo "Please wait a minutes, now starting JP1/Base..."
if [ "$LHHOST" ]; then
    /opt/jplbase/bin/jevstart ${LHHOST}
    /opt/jplbase/bin/jevlogdstart
else
    /opt/jplbase/bin/jevstart
    /opt/jplbase/bin/jevlogdstart
fi
```

Change the script as follows:

```
## Start services
echo "Please wait a minutes, now starting JP1/Base..."
if [ "$LHHOST" ]; then
    /opt/jplbase/bin/jevstart ${LHHOST}
    /opt/jplbase/bin/jevlogdstat >/dev/null 2>/dev/null
    if [ $? -ne 0 ]; then
        /opt/jplbase/bin/jevlogdstart
    fi
else
    /opt/jplbase/bin/jevstart
    /opt/jplbase/bin/jevlogdstart
fi
```

- 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.
- In the following cases, you must specify Japanese as the language of the `LANG` environment variable in the automatic start script:
 - Japanese is specified in the event filter of the forwarding settings file (`forward`).
 - Japanese is specified in the `lpszFilter` parameter of the JP1 event acquisition function (`JevGetOpen`) in the user program.
 - Japanese is specified in various JP1/IM filters in JP1/IM[#].
#: For detailed conditions of servers that require language specification, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
 - The automatic start script for logical hosts (`jbs_start.cluster`) performs an unsetup of the locale settings of `LC_ALL`, `LC_COLLATE`, `LC_CTYPE`, `LC_MONETARY`, `LC_NUMERIC`, `LC_TIME`, and `LC_MESSAGES` by default.

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 or JP1/Base administrator permission

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 together with 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 or JP1/Base administrator permission

Command directory

`/etc/opt/jplbase/`

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 requires monitoring resource operations while a resource is being stopped, the stop command might fail and not be able to stop the resource normally. Therefore, a stop command is provided that can stop JP1/Base normally through a retry. Modify the command settings as follows:

```
cd /etc/opt/jplbase
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, and then outputs the information 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 or JP1/Base administrator permission

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
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. When the `-ds` option is not specified, the listed definitions are the access permission level (JP1_AccessLevel) file and user permission level (JP1_UserLevel) file. When the `-ds` option is specified, the listed definitions are the access permission level (JP1_AccessLevel) file and JP1 authentication information (managed in the directory server).

Format

```
jbsaclreload [-h logical-host-name]  
             [-s authentication-server-name]  
             [-ds#]
```

#:

The `-ds` option can be specified in Windows only.

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 or JP1/Base administrator permission

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.

-ds

This option can be specified in Windows only.

Specify this option for reloading the DS user's JP1 authentication information from a directory server.

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.
- When the JP1 authentication information of DS users is reloaded from the directory server, some users might not be accepted as JP1 users, for example, because the user name conflicts with the name of a standard user or the length of the user name exceeds the maximum length of a JP1 user name. Use the `jbslistuser` and `jbslistacl` commands to check whether the user names are acceptable. The information of users who were not accepted is recorded as warning messages in the integrated trace log of the authentication server.
- If this command ends abnormally, check error messages in the integrated trace log of the authentication server to eliminate failure causes.

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
12	An error occurred in the authentication server side when a DS user was used
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. 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 be specified in Windows only.

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 or JP1/Base administrator permission

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 be specified in Windows only.

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, the `-s` option and authentication server name, the `-p` option and password, and the `-ds` option and linked user, 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.
- This command cannot be used for DS users. Create a user on a directory server.
- The command prompt treats `\`, `*`, `&`, `?`, `^`, and `%any-character%` as special characters. Be aware that they may not be recognized as characters input as part of a password.

Return values

0	Normal end
1	The user has been already registered
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
24	Invalid password
32	An error occurred while initializing the communication functionality.
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbsadmin (Windows 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 or JP1/Base administrator permission

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
```

jbscancellact

Function

The `jbscancellact` 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

```
jbscancellact [-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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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 `jbslistlact` 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 16. *Definition Files*.

-d

Specify this option for canceling the temporary change of the directory server to be linked.

Notes

Restart of JP1/Base (authentication server) or execution of the reload command (`jbs_spmc_reload`) is required if you change a linked directory server during the startup of the authentication server for the operation to use a DS user.

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 or JP1/Base administrator permission

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, the `-s` option and authentication server name, the `-op` option and old password, and the `-np` option and new password, 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.
- The command prompt treats `\`, `*`, `&`, `?`, `^`, and `%any-character%` as special characters. Be aware that they may not be recognized as characters input as part of a password.

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
24	Invalid password
32	An error occurred while initializing the communication functionality.
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
- Information-search user ID
- ID (JP1 user)
- Result on connecting to the directory server
- Result of information-search user authentication
- Result of user authentication (JP1 user)

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.

Notes

The command prompt treats \, *, &, ?, ^, and %*any-character*% as special characters. Be aware that they may not be recognized as characters input as part of a password.

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 JP1 user is successfully authenticated (when the SEARCH_USER_DN parameter is enabled)

```
>jbschkds -u jpluser -p password
Directory server settings
  Directory server name host-A
  Port number 636
  SSL Use
  Information-search user distinguished name CN=Groupcsearcher,OU=GroupC,D
C=netmanage,DC=local
  Search-startpoint container object OU=GroupC,DC=netmanage,DC=local
  Authentication attribute sAMAccountName
The directory server is now connected.
The information-search user was successfully authenticated.
User authentication succeeded.
```

When the directory server linkage function is enabled and the JP1 user is successfully authenticated (when the SEARCH_USER_DN parameter is disabled)

```
>jbschkds -u jpluser -p password
Directory server settings
  Directory server name host-A
  Port number 636
  SSL Use
  Distinguished name CN=jpluser,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] [-c component-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 or JP1/Base administrator permission

Command directory

In Windows:

```
installation-folder\bin\
```

In UNIX:

```
/opt/jplbase/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. Note that the logical host name must be correctly specified with lower or upper case as specified when the logical host was set up. If you omit this option, the physical host name is assumed.

You must specify the logical host name in this option if you use JP1/Base on a cluster system. You cannot use the environment variable `JP1_HOSTNAME`.

If you specify an invalid argument other than this option, all the arguments from the invalid argument are ignored.

-c *component-name*

Specify the component from which you want to collect the definition information.

backup-file

Specify the name of the backup file in which to save the common definition information.

Note

When the common definition information is output, linefeed characters in each line are "CR,CR,LF" for Windows, "LF"(0x0A) for Unix.

Make sure to use appropriate linefeed characters when you edit or save the content of the file.

Return values

0	Normal end
-1	Abnormal end

Example

In this example, the command obtains the JP1/Base common definition information from a physical host:

```
jbsgetcnf -c JP1BASE > config.txt
```

In this example, the command obtains the JP1/Base common definition information from a logical host named `logical`:

```
jbsgetcnf -h logical -c JP1BASE > config.txt
```

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, the SSL communication settings, and event log traps can be collected as operating information.

Format

```
jbsgetopinfo [-h logical-host-name | event-service-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 or JP1/Base administrator permission

Command directory

In Windows:

`installation-folder\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

-h *logical-host-name*

Specify the name of the logical host name or event service name 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 *16. Definition Files*.
- `logtrap`
Outputs definitions in the action definition file for log file trapping in use among all log file traps started by the `jevlogstart` command and by JP1/AJS log file monitoring jobs. If you specify a logical host or an event service with the `-h` option, operating information of a physical host is collected. For details about the format of the action definition file for log file trapping, see [Action definition file for log file trapping](#) in *16. Definition Files*.

- `evttrap`

Outputs definitions in the action definition file for event log trapping in use. If you specify a logical host or an event service with the `-h` option, operating information of a physical host is collected. `evttrap` is only for Windows. For details on the format of an action definition file for event log trapping, see *Action definition file for event log trapping (Windows only)* in *16. Definition Files*.

- `SSL`

Outputs definitions in the SSL communication definition file in use. For details on the format of the SSL communication definition file, see *SSL communication definition file* in *16. 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.
- If SSL definitions are not set, specify `SSL` as the operating information name so that operating information of an event service or process 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

Output format

The following shows the output format of the setup information. Definitions are output in the order in which they appear in the SSL communication definition model file.

The operating information (SSL) is displayed for a physical host name, logical host name, or event service name.

```

<Process-name#1>
"ENABLE"#2="value-specified-for-ENABLE-label"
"SSLPROTOCOL"#3="value-specified-for-SSLPROTOCOL-label"
"CACERTIFICATEFILE"#3="value-specified-for-CACERTIFICATEFILE-label"
"CERTIFICATEFILE"#3="value-specified-for-CERTIFICATEFILE-label"
"PRIVATEKEYFILE"#3="value-specified-for-PRIVATEKEYFILE-label"
"SSLCIPHERS"#3="value-specified-for-SSLCIPHERS-label"
"BASESSL"#4="0" or "1"

```

#1

The names of the processes to be controlled are output. They are displayed in the following order:

<jbssessionmgr>: Authentication server

<jbsroute>: Configuration management

<jcocmd>: Command execution

<jbspplugind>: Plug-in service

<jbscomd>: Inter-process communication

<jevservice>: Event service

#2

This information is always output.

#3

This information is output only when both ENABLE and BASESSL are set to 1. When the name of the parameter is not defined, a null character is output.

#4

This information is output only when ENABLE is set to 1. dword:00000001 is output when SSL is enabled, and dword:00000000 is output when SSL is disabled.

Example

The following shows an example of output.

<pre> >jbsgetopinfo -o SSL Displays the operating information (SSL) of server1. <jbssessionmgr> "ENABLE"=dword:00000001 "SSLPROTOCOL"="TLSv1_2" "CACERTIFICATEFILE"="C:\CA\CAcert.pem" "CERTIFICATEFILE"="C:\CA\cert.pem" "PRIVATEKEYFILE"="C:\CA\certkey.pem" "SSLCIPHERS"="" "BASESSL"="1" <jbsroute> "ENABLE"=dword:00000001 "BASESSL"="0" </pre>	<p>— Outputs the process name.</p> <p>— Always output.</p> <p>— Outputs a null character when a parameter name is not defined.</p> <p>— When SSL is enabled.</p> <p>— Outputs only BASESSL when SSL is disabled.</p>
---	--

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 or JP1/Base administrator permission

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 or JP1/Base administrator permission

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

jbshosts2export

Function

The `jbshosts2export` command collects the `jp1hosts2` information registered for a host and outputs it to standard output.

Format

```
jbshosts2export [-h logical-host-name] > jp1hosts2-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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jp1base/bin/

Arguments

-h *logical-host-name*

Specify the name of the logical host whose `jp1hosts2` information you want to collect. If you omit this option, the host name set in the `JP1_HOSTNAME` environment variable is assumed. If `JP1_HOSTNAME` is not set, the physical host name is assumed.

To collect the `jp1hosts2` information for a logical host in a cluster system, execute the `jbshosts2export` command on the primary node.

jp1hosts2-definition-file-name

Specify the name of the file from which to collect the `jp1hosts2` information.

Return values

0	Normal end
1	Message processing error
2	Command argument error
3	Permission check error
4	Common definition error
5	File I/O error

jbshostsimport

Function

The `jbshostsimport` command registers the `jp1hosts` information into the common definition information.

Format

```
jbshostsimport { {-o|-r} jp1hosts-definition-file-name [-f] | -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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

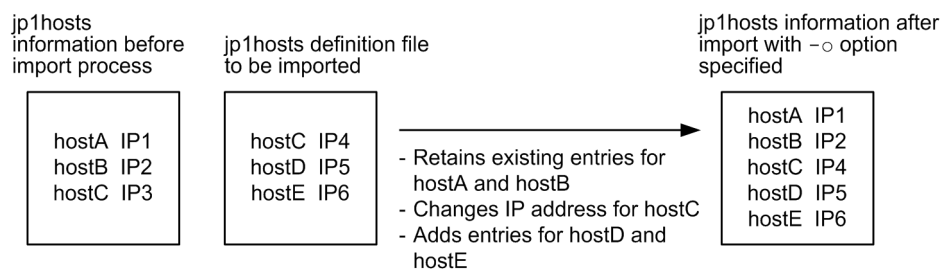
In UNIX:

/opt/jp1base/bin/

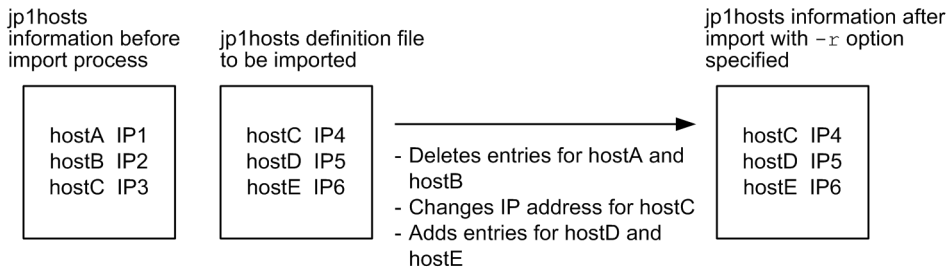
Arguments

{-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). The following figure shows what happens to the `jp1hosts` information when you specify the `-o` option.



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. The following figure shows what happens to the `jp1hosts` information when you specify the `-r` option.



For details about the format of `jp1hosts` definition file, see *jp1hosts definition file* in 16. *Definition Files*.

-f

If you specify this option, the `jp1hosts` data is forcibly registered in an environment where the `jp1hosts2` data is already defined.

-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.
- If you execute this command with the `-o` option or `-r` option in an environment where `jp1hosts2` information is set, the message KAVA0443-E is output and the command terminates with return value 8. However, if you specify the `-f` option along with the `-o` or `-r` option, the termination will not occur because the `jp1hosts` data is forcibly registered (also the message KAVA0443-E will not be output).

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
8	<code>jp1hosts</code> information could not be imported because <code>jp1hosts2</code> information has already been imported

Example

This example shows how to define the `jp1hosts` data in an environment where the `jp1hosts2` data is already defined:

Execute the `jbshostsimport` command with the `-f` option specified in an environment where the `jp1hosts2` data is defined.

```
>jbshostsimport -o jp1hosts-definition-file-name -f  
KAVA0436-I The processing was successful.
```

If you execute the `jbshostsimport` command without the `-f` option specified in an environment where `jp1hosts2` data is defined, an error will occur.

```
>jbshostsimport -o jp1hosts-definition-file-name  
KAVA0443-E The command cannot be executed because jp1hosts2 was already imp  
orted.
```

jbshosts2import

Function

The `jbshosts2import` command registers `jp1hosts2` information on a host.

Format

```
jbshosts2import { {-o|-r} [jp1hosts2-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 or JP1/Base administrator permission

Command directory

In Windows:

`installation-folder\bin\`

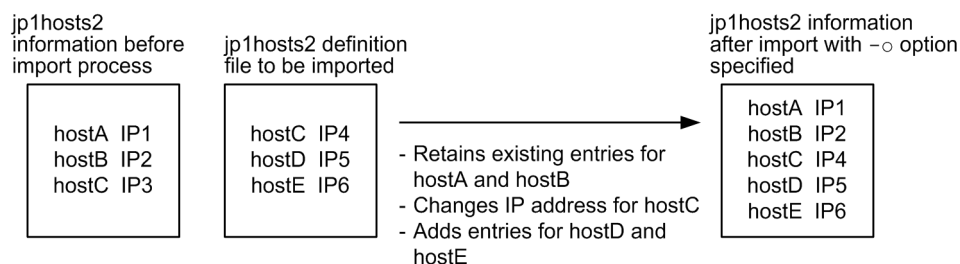
In UNIX:

`/opt/jp1base/bin/`

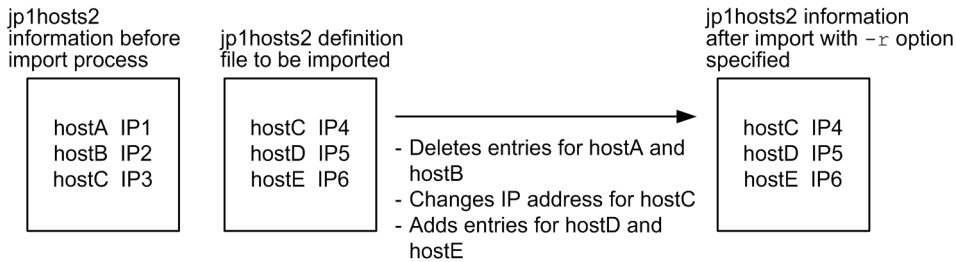
Arguments

`{-o|-r}` *jp1hosts2-definition-file-name*

Specify the name of the file that contains the `jp1hosts2` information you want to register with the host. If you specify the `-o` option, the command merges the new `jp1hosts2` information with the existing information (if the same host is already defined, the existing entry is overwritten). The following figure shows what happens to the `jp1hosts2` information when you specify the `-o` option.



If you specify the `-r` option, the `jbshosts2import` command deletes all of the existing `jp1hosts2` information before registering the new information. The following figure shows what happens to the `jp1hosts2` information when you specify the `-r` option.



If you specify the name of the `jp1hosts2` definition file by relative path, the path is interpreted relative to the current directory at command execution. If you do not specify a file name, the command imports the `jp1hosts2` definition file in the following directory:

In Windows:

```
installation-folder\conf\jp1hosts2.conf
shared-folder\jp1base\conf\jp1hosts2.conf (in a cluster environment)
```

In UNIX:

```
/etc/opt/jp1base/conf/jp1hosts2.conf
shared-directory/jp1base/conf/jp1hosts2.conf (in a cluster environment)
```

For details on the format of a `jp1hosts2` definition file, see *jp1hosts2 definition file* in *16. Definition Files*.

-d

Specify this option to delete the `jp1hosts2` information registered on the host.

-h *logical-host-name*

Specify the name of the logical host for which to register or delete `jp1hosts2` information. If you omit this option, the host name set in the `JP1_HOSTNAME` environment variable is assumed. If `JP1_HOSTNAME` is not set, the physical host name is assumed.

To register or delete `jp1hosts2` information on a logical host in a cluster system, execute the `jbshosts2import` command on the primary node.

Notes

- If executing the `jbshosts2import` command changes either of the following settings, you must restart JP1/Base, products for which JP1/Base is a prerequisite, and programs that have a dependency relationship with JP1/Base:
 - The IP address allocated to the local host
 - The IP address of a host with which JP1/Base is communicating
- If you execute this command in an environment where `jp1hosts` information is set but not `jp1hosts2` information, the confirmation message KAVA0455-I is output.
- When registering `jp1hosts2` information in an environment that uses `jp1hosts` information, first migrate the definitions in the `jp1hosts` information to `jp1hosts2` information. For details, see *6.4.5 Migrating from jp1hosts information to jp1hosts2 information*.
- In a cluster system environment, if you import `jp1hosts2` information to a physical host that contains a logical host with `jp1hosts` information, the `jp1hosts2` information you import is also applied to the logical host. When this happens, the `jp1hosts` information defined for the logical host becomes invalid.

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
7	Another <code>jbshosts2import</code> command is being executed

jbslistacl

Function

The `jbslistacl` command lists the operating permissions assigned to the registered JP1 users or DS group. The JP1 user can be a standard user, linkage user, or DS user.

Format

```
jbslistacl [-h logical-host-name]  
           [-s authentication-server-name]  
           [-ds#]
```

#:

The `-ds` option can be specified in Windows only.

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 or JP1/Base administrator permission

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 or DS group.

-s *authentication-server-name*

Specify an authentication server to list the operating permissions assigned to the JP1 users registered on that authentication server or DS group. When you set this option, the `-h` option is ignored.

-ds

This option can be specified in Windows only.

Specify this option to display DS users' operating permission. If operating permission is registered also to a DS group, the DS group's operating permission is displayed before that of DS users.

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 or DS group.

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
12	An error occurred in the authentication server side when a DS user was used
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

Output example

The following are examples of the `jbslistacl` command output.

No option specified:

```
>jbslistacl
UserLevel No.0
  Name      :user-001
  GroupName:*
  AccessLevel:JP1_AJS_Editor
UserLevel No.1
  Name      :user-admin
  GroupName:*
  AccessLevel:JP1_AJS_Admin
  AccessLevel:JP1_Console_Admin
```

-ds option specified:

```
>jbslistacl -ds
DSGroupLevel No.0
  DSGroupName:GRP-AJS
  GroupName:*
  AccessLevel:JP1_AJS_Editor
DSGroupLevel No.1
  DSGroupName:GRP-Adm
  GroupName:*
  AccessLevel:JP1_AJS_Admin
  AccessLevel:JP1_Console_Admin

UserLevel No.0
  Name      :user-001
  GroupName:*
  AccessLevel:JP1_AJS_Editor[GRP-AJS]
UserLevel No.1
  Name      :user-admin
```



```
GroupName:*  
AccessLevel:JP1_AJS_Admin[GRP-Adm]  
AccessLevel:JP1_Console_Admin[GRP-Adm]
```

jbslistlact

Function

The `jbslistlact` command lists the waiting or running local actions.

Format

```
jbslistlact [-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 or JP1/Base administrator permission

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 `jbslistlact` 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 or JP1/Base administrator permission

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 be specified in Windows only.

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 or JP1/Base administrator permission

Command directory

In Windows:

`installation-folder\bin\`

In UNIX:

`/opt/jplbase/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 JP1 users who were registered before upgrading to version 08-10, JP1 users who are initialized at the time of new installation, linkage users, and DS users 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 be specified in Windows only.

If this option is specified, only a linkage user or DS user is displayed. JP1 user to be displayed will change depending on the setting of the `ENABLE` parameter in the directory server linkage definition file.

- `"ENABLE"=dword:00000001`
Only linkage users among registered JP1 users are displayed.
- `"ENABLE"=dword:00000002`
Only DS users among registered JP1 users are displayed.

Note that no JP1 user will be displayed if `"ENABLE"=dword:00000000`.

If this option is not specified, all the registered JP1 users will be 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
32	An error occurred while initializing the communication functionality.
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 or DS user `testuser1` have been registered on the authentication server:

When no option is specified:

```
>jbslistuser
jpluser account[0]:jp1admin
jpluser account[1]:jp1admin2
jpluser account[2]:testuser1
Successful.
```

When the `-ld` option is specified:

```
>jbslistuser -ld

JP1User Name           Last Modified Time
-----/---/---  ---:---:---
jpladmin               2007/01/01 09:00:05
jpladmin2              2007/01/01 09:00:03
testuser1
Successful.

>
```

JP1 user name

Title line

Last updated date

When the `-ds` option is specified:

```
>jbslistuser -ds
Collected Time:2017/05/31 11:20:00#
jpluser account[0]:testuser1
Successful.
```

: When the DS user output is displayed, the timestamp to indicate the time of collecting JP1 authentication information from the Active Directory is shown on the top line.

The following shows an example of output where the standard users `jpladmin` and `jpladmin2` and no linked users or DS user have been registered on the authentication server:

When the `-ds` option is specified:

```
>jbslistuser -ds
Collected Time:2017/05/31 11:20:00
No jpluser 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 *16. 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 [8.1.5 Assigning user permissions to OS users before setting user mapping](#).

Return values

1	Normal end
0	Abnormal end

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 or JP1/Base administrator permission

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, the contents of the default user mapping definition file (`jp1BsUmap.conf`) are registered in the common definition information. For details on the format of the user mapping definition file, see [User mapping definition file](#) in *16. 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.
- When you register user mapping information by using a definition file that contains a large number of definitions, it might take a long time to apply the definition contents to the common definition information. While user mapping information is being updated, masked user functionality cannot be used, and therefore operations that require masked user functionality (such as JP1/AJS job execution and remote commands in JP1/IM - Manager) cannot be performed.

Therefore, if you intend to update a large amount of user mapping information at one time, execute the `jbsssetumap` command in a maintenance period not during operation. If you want to update a large amount of user mapping information during operation, consider splitting the definition contents before executing the `jbsssetumap` command. This minimizes the time required by the `jbsssetumap` command to apply the definition contents to the common definition information. For details on the `jbsssetumap` command, see [jbsssetumap](#).

Return values

1	Normal end
0	Abnormal end

Function

The `jbsparamdump` command collects the JP1/Base setup information in a single operation and outputs the information under the directory specified as the output destination.

If the collection target host is in logical host operation, this command outputs the setup information of the physical host and all the logical hosts.

When you execute the `jbsparamdump` command, a directory named `JP1Base` is created in a specified directory. Under that directory, setup information is output in the groups shown below. Note that if a file with the same name as the output file already exists, the file with the same name is overwritten.

- Setup information of a physical host (*physical-host-name*.prm)^{#1}
- Setup information of a logical host (*logical-host-name*.prm)^{#1}
- Setup information of an event server (*event-server-name*.prm)^{#1, #2}
- Contents of the files specified in the collection information file (`userconf.prm`)

#1: If the output file name (physical host name, logical host name, or event server name) is 129 bytes or more in length, the first 128 bytes becomes the file name.

#2: The setup information of an event server on a physical host is output to the *physical-host-name*.prm file. The setup information of an event server on a logical host is output to the *logical-host-name*.prm file. If an event server is set up on a host other than physical or logical hosts, the setup information of the event server is output to the *event-server-name*.prm file.

The following table lists setup information that can be collected.

Table 15–1: List of setup information that can be collected by the `jbsparamdump` command

Type of setup information	Setup information to be collected	Collection availability for each host type			
		Physical host	Logical host	Logical host (secondary node)	Event server
Host information	Host type (physical, logical, or event server)	Yes	Yes	Yes	Yes
	Physical host name, logical host name, or event server name	Yes	Yes	Yes	Yes
Product information	Company name ^{#1}	Yes	--	--	--
	Registered user name ^{#1}	Yes	--	--	--
	Version ID	Yes	--	--	--
	Product ID	Yes	--	--	--
	Product name	Yes	--	--	--
OS information	List of port numbers used by JP1/Base services	Yes	--	--	--
	<ul style="list-style-type: none"> • Startup settings of JP1/Base services (in Windows) • Whether automatic startup when starting the OS is set, and whether 	Yes	--	--	--

Type of setup information	Setup information to be collected	Collection availability for each host type			
		Physical host	Logical host	Logical host (secondary node)	Event server
	automatic termination when exiting the OS is set (in UNIX)				
JP1/Base setup information	Startup script file (physical host) ^{#2}	Yes	--	--	--
	Stop script file (physical host) ^{#2}	Yes	--	--	--
	Startup script file (logical host) ^{#2}	Yes	--	--	--
	Stop script file (logical host) ^{#2}	Yes	--	--	--
	Start sequence definition file ^{#1}	Yes	--	--	--
	Service startup delay time / timer monitoring period definition file ^{#1}	Yes	--	--	--
	Event server index file	Yes	--	--	--
	Event server settings file	Yes	Yes	No	Yes
	Forwarding settings file	Yes	Yes	No	Yes
	Forwarding settings file for event forwarding suppression ^{#3}	Yes	Yes	No	--
	API settings file	Yes	--	--	--
	Additional extended attribute settings file for transfer reception	Yes	Yes	No	Yes
	Additional extended attribute settings file for event registration	Yes	Yes	No	Yes
	Action definition file for log file trapping ^{#3}	Yes	--	--	--
	Log-file trap startup definition file	Yes	--	--	--
	Log information definition file	Yes	--	--	--
	Action definition file for event log trapping ^{#1}	Yes	--	--	--
	Distribution definition file (forwarding settings file) ^{#3}	Yes	Yes	No	--
	Distribution definition file (action definition file for log file trapping) ^{#3}	Yes	--	--	--
	Distribution definition file (log-file trap startup definition file) ^{#3}	Yes	--	--	--
	Distribution definition file (action definition file for event log trapping) ^{#1, #3}	Yes	--	--	--
	Authentication server name	Yes	Yes	No	--
	Authentication information (JP1 user name) ^{#4}	Yes	Yes	No	--
Authentication information (JP1 user permission) ^{#4}	Yes	Yes	No	--	
Password save format	Yes	Yes	Yes	--	

Type of setup information	Setup information to be collected	Collection availability for each host type			
		Physical host	Logical host	Logical host (secondary node)	Event server
	Directory server linkage definition ^{#1}	Yes	Yes	Yes	--
	User mapping information	Yes	Yes	No	--
	Health check setup information	Yes	Yes	Yes	--
	Health check definition file	Yes	Yes	No	--
	JP1/Base environment settings file (startup language type) ^{#2}	Yes	Yes	No	--
	JP1/Base parameter definition file	Yes	Yes	Yes	--
	Extended startup process definition file	Yes	Yes	No	--
	jp1hosts definition information	Yes	Yes	No	--
	jp1hosts2 definition information	Yes	Yes	No	--
	Configuration management functionality setup information	Yes	Yes	Yes	--
	Configuration definition file	Yes	Yes	No	--
	Configuration definition information	Yes	Yes	No	--
	Host access control definition file	Yes	Yes	No	--
	SSL communication definition information	Yes	Yes	Yes	--
	Local action setup information	Yes	Yes	Yes	--
	Local action execution definition file	Yes	Yes	No	--
	Extended regular expressions	Yes	Yes	Yes	--
	Operation log definition	Yes	Yes	Yes	--
	Controlling connections (configuration management and command execution)	Yes	Yes	Yes	--
	Controlling connections (operation requests from linkage products)	Yes	Yes	Yes	--
	Command execution environment	Yes	Yes	No	--
	JP1/Base administrator settings ^{#2#5}	Yes	--	--	--
	Communication protocol	Yes	Yes	Yes	--
	Operation language type	Yes	Yes	Yes	--
	Character code compatibility mode ^{#2}	Yes	Yes	Yes	--
User-specified information	Files specified in the collection information file (jbsparamdump.conf)	--	--	--	--

Legend:

Yes: Collected.

No: Not collected.

--: Not collected (setup information does not exist).

#1

Acquired only in Windows.

#2

Acquired only in UNIX.

#3

Acquired only when the default destination and file name are used.

#4

Acquired only when the command was executed with the `-s` option specified.

#5

Acquired only when the command was executed by a user with `root` permissions.

Note that the following setup information will not be collected:

- Password definition file
- JP1 user password information
- Local action environment variable file

Format

```
jbtparamdump [-s] -d output-destination-directory
```

Required execution permission

In Windows: Administrators privileges (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser or JP1/Base administrator privileges

Command directory

In Windows

installation-folder\bin\

In UNIX

/opt/jplbase/bin/

Arguments

`-s`

Specify this option to collect JP1 user names that are registered in the primary authentication server and operating permission information for JP1 users. An environment in which you can communicate with the authentication servers is required to specify this option.

`-d output-destination-directory`

Specify the directory name to which the collected setup information is output 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 (").

Notes

- This command can be executed no matter whether JP1/Base is running or stopped.
- The character code used in an environment in which you are executing this command must match the character code used in an environment in which JP1/Base is running. If the character codes do not match, multiple character codes might exist in a file.

- If you use the cluster system, execute this command on the primary node. If you execute the command on the secondary node, some setup information of a logical host cannot be collected.

Return values

0	Normal end
1	Setup information whose collection has failed exists.
4	A file whose output has failed exists.
10	Invalid arguments
11	Insufficient execution permission
12	Access error to the output destination directory
13	Failed to read the collection information file, or format error of the collection information file.
20	Insufficient memory
255	Other error

Output format

The following shows the output format of the setup information:

```
*****information-identifier<information-type>path-information#
Setup information
***End information-identifier(acquisition-result)
```

#: *Information-type* and *path-information* are output in setup information whose type is either *JPI/Base setup information* or *User-specified information* in Table 15-1.

The following table describes the meaning for each item.

Item	Description
<i>information-identifier</i>	A character string used for identifying the setup information
<i>information-type</i>	The type of information is shown in the following format: FILE Contents of the definition file CMD Result of the command execution CNF Common definition information
<i>path-information</i>	The path of the setup information is shown in the following format: If <i>information-type</i> is FILE: Full path of the definition file If <i>information-type</i> is CMD: Full path of the command and specified option(s) If <i>information-type</i> is CNF: Subkey of the common definition information
<i>acquisition-result</i>	Acquisition result of the setup information is shown in the following format:

Item	Description
	<p>If <i>information-type</i> is FILE or CNF: SUCCESS (Acquisition has succeeded), FAILURE (Acquisition has failed), or NONE (Information does not exist)</p> <p>If <i>information-type</i> is CMD: The return value of the command or FAILURE (Execution has failed)</p>

The following shows an output example of setup information of a physical host (*physical-host-name .prm*).

```

***JP1/Base Configurations(FileVersion=105000 TimeStamp=2013/09/10 16:53:12)

****Host Information
hosttype=Physical
hostname=hostA
***End Host Information(SUCCESS)

****Product Information
ExCurrentVersion=1050
ProductID=P-912C-6LA1
ProgramName=JP1/Base
***End Product Information(SUCCESS)

****Service Port Number List
jplimevt      20098/tcp
jplimevtapi   20099/tcp
(The rest is omitted.)
***End Service Port Number List(SUCCESS)

****Base Services Startup Information
jbs_start:available
jbs_stop:available
***End Base Services Startup Information(SUCCESS)

****Event service:conf<FILE>/etc/opt/jplbase/conf/event/server/default/conf
#-----
# JP1/Base - Event Server Setting
#-----
ports      <jplhosts2> jplimevt jplimevtapi
users      system *
eventids   *
db-size    10000000
include    ajs-conf
options    remote-receive v5-unused save-rep
forward-limit 3600
remote-server * close <jplhosts2>
***End Event service:conf(SUCCESS)

****User management:jbslistuser<CMD>/opt/jplbase/bin/jbslistuser
jpluser account[0]:jpladmin
Registered users were successfully listed.
***End User management:jbslistuser(0)

****Extending regular expressions<CNF>[JP1_DEFAULT\JP1BASE\]
[JP1_DEFAULT\JP1BASE\]
"REGEXP"="EXTENDED"
***End Extending regular expressions(SUCCESS)
(The rest is omitted.)

```

File header

Host information

Product information

List of port numbers used by JP1/Base services

Whether automatic startup when starting the OS is set, and whether automatic termination when the existing OS is set

Contents of the definition file: Event server settings file

Result of the command execution: Authentication information (JP1 user name)

Common definition information
Extended regular expressions

The table below shows the correspondence between the information identifiers and setup information that are output. For items that output a specific parameter, such as common definition information, the Parameter column below gives the parameter name. For items that output the contents of a definition file or command execution result, the Parameter column shows --, indicating that there is no applicable entry.

Information identifier	Parameter	Description
Host Information	hosttype	Host type Physical (physical host), Logical (logical host), or Event (event server)
	hostname	Physical host name, logical host name, or event server name
Product Information	RegisteredOrganization	Company name
	RegisteredOwner	Registered user name
	ExCurrentVersion	Version ID
	ProductID	Product ID
	ProgramName	Product name
Service Port Number List	jplimevt jplimevtapi jplimrt jplimcmnda jplimcmcdc jplbsuser jplbsplugin jplbscom JPlAutoJob jesrd	List of port numbers used by JP1/Base services
Base Services Startup Information	--	<ul style="list-style-type: none"> Startup settings of JP1/Base services (in Windows) Whether automatic startup when starting the OS is set, and whether automatic termination when existing the OS is set (in UNIX)
Starting and stopping:jbs_start	--	Startup script file (physical host)
Starting and stopping:jbs_stop	--	Stop script file (physical host)
Starting and stopping:jbs_start.cluster	--	Startup script file (logical host)
Starting and stopping:jbs_stop.cluster	--	Stop script file (logical host)
Startup control:JP1SVPRM.DAT	--	Start sequence definition file
Startup control:Jplsvprm_wait.dat	--	Service startup delay time / timer monitoring period definition file
Event service:index	--	Event server index file
Event service:conf	--	Event server settings file
Event service:forward	--	Forwarding settings file
Event service:forward_suppress	--	Forwarding settings file for event forwarding suppression
Event service:api	--	API settings file
Event service:recv_add_extattr	--	Additional extended attribute settings file for transfer reception

Information identifier	Parameter	Description
Event service:send_add_extattr	--	Additional extended attribute settings file for event registration
Event conversion:jevlog.conf	--	Action definition file for log file trapping
Event conversion:jevlog_start.conf	--	Log-file trap startup definition file
Event conversion:jevlogd.conf	--	Log information definition file
Event conversion:ntevent.conf	--	Action definition file for event log trapping
Distribution definition file:jev_forward.conf	--	Distribution definition file (forwarding settings file)
Distribution definition file:jev_logtrap.conf	--	Distribution definition file (action definition file for log file trapping)
Distribution definition file:jev_logstart.conf	--	Distribution definition file (log-file trap startup definition file)
Distribution definition file:jev_ntevent.conf	--	Distribution definition file (action definition file for event log trapping)
User management:jbslistsrv	--	Authentication server name
User management:jbslistuser	--	Authentication information (JP1 user name)
User management:jbslistacl	--	Authentication information (JP1 user permission)
User management:HASH_LEVEL	HASH_LEVEL	Password save format
User management:ds_setup	ENABLE SERVER PORT SEARCH_USER_DN BASE_DN ATTR_NAME SSL	Directory server linkage definition
User management:jbsgetumap	--	User mapping information
Health check:setup	ENABLE FAILOVER	Health check setup information
Health check:jbshc.conf	--	Health check definition file
Process management:jplbs_env.conf	--	JP1/Base environment settings file (startup language type)
Process management:jplbs_param_v7.conf	SEND_PROCESS_TERMINATED_AB NORMALLY_EVENT SEND_PROCESS_RESTART_EVENT SEND_AUTHSRV_EVENT	JP1/Base parameter definition file
Process management:jplbs_service_0700.conf	--	Extended startup process definition file
jplhosts:jbshostsexport	--	jplhosts definition information
jplhosts:jbshosts2export	--	jplhosts2 definition information
SSL communication definition:setup	ENABLE CERTIFICATEFILE	SSL communication definition information

Information identifier	Parameter	Description
	CACERTIFICATEFILE PRIVATEKEYFILE SSLPROTOCOL SSLCIPHERS BASESSL	
Configuration definition:setup	JBSRT_DISTRIB_VERSION JBSROUTE_COM_TIMEOUT	Configuration management functionality setup information
Configuration definition:jbs_route.conf	--	Configuration definition file
Configuration definition:jbsrt_get	--	Configuration definition information
Configuration definition:jbsdfts_srv.conf	--	Host access control definition file
Local action:setup	LOGSIZE LOGFILENUM PAUSE CODECONV	Local action setup information
Local action:jbslact.conf	--	Local action execution definition file
Extending regular expressions	REGEXP	Extended regular expressions
Operation log:setup	ENABLE LOGFILEDIR LOGSIZE LOGFILENUM LOGCHANGEOPT	Operation log definition
unintended hosts:ROUTE	UPPER_ONLY ALT_CLIENT_HOSTS	Controlling connections (configuration management and command execution)
unintended hosts:RECEIVE	CLIENT_HOSTS	Controlling connections (operation requests from linkage products)
Command execution:jcocmdef	--	Command execution environment
JP1Base administrator:jbssetadmingrp	--	JP1/Base administrator settings
Base common definition:setup	JP1_COM_VERSION JP1_BIND_ADDR JP1_CLIENT_BIND_ADDR JP1_ANY_BIND	Communication protocol
	LANG	Operation language type
	LANG_MODE	Character code compatibility mode

Legend:

--: Not applicable.

For details on the output format of files specified in the collection information file (`jbsparamdump.conf`), see *Collection information file* in *16. Definition Files*.

jbspasmgr (Windows only)

Function

The `jbspasmgr` 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 OS users or information-search users.

Format

```
jbspasmgr
```

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 [8.1.5 Assigning user permissions to OS users before setting user mapping](#).
- Before you delete an OS user, make sure that the user is not mapped to any JP1 user. You can check the user mapping information by using either of the following:
 - List of OS users to be mapped in the **User mapping** tab of JP1/Base Environment Settings
 - `jbsgetumap` command

jbsrmacl

Function

The `jbsrmacl` command deletes all the operating permissions assigned to a specified JP1 user or DS group. The JP1 user can be a standard user, linkage user, or DS user.

Format

```
jbsrmacl [-h logical-host-name]  
         [-s authentication-server-name]  
         {-u JP1-user-name | -g DS-group-name}  
         [-i]  
         [-ds#]
```

#:

The `-ds` option can be specified in Windows only.

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 or JP1/Base administrator permission

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 or DS group. 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* | -g *DS-group-name*

-u *JP1-user-name*

Specify the JP1 user name for which you want to delete operating permissions.

-g *DS-group-name*

Specify the security group name of the directory server from which you want to delete operating permission. Specify also the `-ds` option at the same time.

If the group name contains a space, enclose it with double quotation marks (").

The permissible number of characters is 1 through 256 (bytes). Permissible DS group name characters are limited only to ASCII characters except * / \ " ' ^ [] { } () : ; | = , + ? < >, and tab characters.

-i

When you specify this option, a confirmation message appears before the operating permissions for the specified JP1 user or DS group are deleted. The deletion processing is executed only if you type `y` or `Y` in response to the message.

-ds

This option can be specified in Windows only.

Specify this option to delete operating permission from a DS user or DS group. If this option is specified, the value of the JP1 operating permission attribute of the DS user or DS group registered in the directory server becomes a null character.

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.
- When the `-ds` option is specified, the reload command (`jbsaclreload`) must be executed.

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
12	An error occurred in the authentication server side when a DS user was used
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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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 or an information-search user registered in the JP1/Base password management information.

Format

```
jbsrmumappass [-h logical-host-name]  
               -u { OS-user-name | information-search-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* | *information-search-user-name* }

Specify the OS user name or information-search user name you want to delete from the password management information.

Note

Before you delete an OS user, make sure that the user is not mapped to any JP1 user. You can check the user mapping information by using either of the following:

- List of OS users to be mapped in the **User mapping** tab of JP1/Base Environment Settings
- `jbsgetumap` command

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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.

- This command cannot be used for DS users. Delete the user on the directory server.

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 [-f] [-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 or JP1/Base administrator permission

Command directory

In Windows:

```
installation-folder\bin\
```

In UNIX:

```
/opt/jp1base/bin/
```

Arguments

-f

Specify this argument if you do not want a message confirming command execution (a message asking you to enter Y or N) to be output. If you specify this option, the message confirming command execution is omitted, the value Y is assumed, and processing continues. If you omit this option, a message confirming command execution will be displayed.

-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.

Environment variables

JBSRT_CMDRCD_EXTEND

This environment variable expands the set of values that can be returned by the command. To use the expanded set of return values, specify 1. To use the original (unexpanded) set of return values, specify 0. If you omit this environment variable, the command will return a value from the original set of return values.

Notes

If your JP1/IM - Manager version is 11-01 or earlier, do not set the `JBSRT_CMDRCD_EXTEND` environment variable as a system environment variable or a user environment variable. If you do, you might not be able to use IM

Configuration Management to configure the system hierarchy. Instead, use the command prompt or a batch file to set the JBSRT_CMDRCD_EXTEND environment variable.

Return values (original set)

0	Normal end
1	Abnormal end

Return values (expanded set)

0	Normal end
10	Invalid argument
11	Permission error
12	No configuration definition information
13	Configuration definition information access error
20	Insufficient memory
128	Other error

Example

The examples below show the command with the `-f` option specified and the command with the `-f` option omitted.

With the `-f` specified:

```
# jbsrt_del -f
KAVB3115-I The definition information was deleted.
```

With the `-f` option omitted:

```
# jbsrt_del
Do you want to delete the definition information? [Y/N] y
KAVB3115-I The definition information was deleted.
```

The following example shows how to expand the set of values returned by the command:

```
# set JBSRT_CMDRCD_EXTEND=1
# jbsrt_del
```

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.

The two methods for distributing configuration definition information are the batch distribution method and the differential distribution method.

When this command is executed, JP1/Base must be running on all hosts to which the configuration definition is to be distributed (on the hosts whose configuration definition is to be changed and all of their higher hosts when a differential distribution method is used). 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 information to a host to which the definition could not be distributed, start JP1/Base on the host, and then re-execute the `jbsrt_distrib` command to distribute the definition. If you are using the batch distribution method, enter `N` when a message asking you to delete configuration information is displayed. 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\jplbase\conf\route\jbs_route.conf` (when the `-h` option is specified)

In UNIX:

`/etc/opt/jplbase/conf/route/jbs_route.conf`

`shared-directory/jplbase/conf/route/jbs_route.conf` (when the `-h` option is specified)

For details on the format of the configuration definition file, see [Configuration definition file](#) in *16. Definition Files*.

Format

Common definition (JBSRT_DISTRIB_VERSION=0):

```
jbsrt_distrib [{-D [-f] | -L}]
               [-h logical-host-name]
```

Common definition (JBSRT_DISTRIB_VERSION=1):

```
jbsrt_distrib [{-D [-f] | -L | -f}]
               [-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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/bin/

Arguments

-D

Specify this argument to distribute the configuration definition information by using the differential distribution method. This method deletes configuration definition information from or distributes configuration definition information to only hosts for which changes have been made in the configuration definition. If you omit this option, the value set for `JBSRT_DISTRIB_VERSION` in the common definition information takes effect.

-L

Specify this argument to distribute the configuration definition information by using the batch distribution method. This method deletes configuration definition information from or distributes configuration definition information to all hosts in the configuration definition information. If you omit this option, the value set for `JBSRT_DISTRIB_VERSION` in the common definition information takes effect.

-f

Specify this argument if you do not want a message confirming command execution (a message asking you to enter Y or N) to be output. If you specify this option, the message confirming command execution is omitted, the value Y is assumed, and processing continues. If you omit this option, a message confirming command execution will be displayed.

-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.

Environment variables

JBSRT_CMDRCD_EXTEND

This environment variable expands the set of values that can be returned by the command. To use the expanded set of return values, specify 1. To use the original (unexpanded) set of return values, specify 0. If you omit this environment variable, the command will return a value from the original set of return values.

Note

- When you execute this command to delete configuration definition information, the configuration definition information after a host with an asterisk (*), if any, in the configuration definition file will not be deleted. If you want to delete the existing configuration definition information, confirm that there is no asterisk (*) in the configuration definition file.
- If you are using the IM configuration management and execute this command, configuration definition information will be different in the IM configuration management and in JP1/Base. Therefore, if you are using the IM configuration management, we recommend that you do not execute this command, and instead use the IM configuration management to perform integrated configuration management. For details, see the chapter that

explains management of hierarchical structure of a system using the IM configuration management in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

- If the batch distribution method is used to distribute configuration definition information and configuration information is deleted while the system is running, the following problems might occur between the time when the information was deleted and the time when distribution finishes:
 - An event transfer might fail.
 - Command execution might fail.
 - Automatic action execution might fail.

When a management-target host is added but no hosts are deleted, follow the procedure below to distribute the configuration files without deleting any configuration information. The following procedure allows you to change the system configuration without affecting the existing configuration information.

1. If the message Delete the current configuration definition? is output, enter N.
 2. If the message Distribute the configuration definition? is output, enter Y.
- If your JP1/IM - Manager version is 11-01 or earlier, do not set the `JBSRT_CMDRCD_EXTEND` environment variable as a system environment variable or a user environment variable. If you do, you might not be able to use IM Configuration Management to configure the system hierarchy. Instead, use the command prompt or a batch file to set the `JBSRT_CMDRCD_EXTEND` environment variable.
 - When distributing configuration definition to many hosts (roughly 1,000 or more hosts) at a time, it may take a long time to complete the command execution if many errors occur during the distribution process. We recommend, therefore, that you use the differential distribution method to distribute it to a group of several hundred to 500 hosts at a time.
 - When operating under a system hierarchical configuration with three or more levels, the processes of hosts under a submanager may take too much time and fail to properly return a response. Hence, the `jbsrt_distrib` command may result in timeout. For details, see [2.6.3 \(5\) Reviewing the communication timeout value](#).

Return values (original set)

0	Normal end
1	Abnormal end

Return values (expanded set)

0	Normal end
1	Distribution or deletion of the configuration definition information failed on some hosts.
2	Configuration management server processing is being performed.
3	The command timed out.
10	Invalid argument
11	Permission error
13	A configuration definition information access error occurred, or the configuration definition information is corrupted.
14	Definition file access error
15	Definition file format error
16	An error occurred during communication with the configuration management server.
20	Insufficient memory

Example

The examples below show the command with the `-f` option specified and the command with the `-f` option omitted.

With the `-f` option specified:

```
# jbsrt_distrib -D -f
Sending the configuration definition...
KAVB3109-I The definition distribution command terminated normally.
```

With the `-f` option omitted:

```
# jbsrt_distrib -D
All hosts to which the configuration definition is to be distributed must
be running.
Do you want to distribute the configuration definition? [Y/N] y
Sending the configuration definition...
KAVB3109-I The definition distribution command terminated normally.
```

The following example shows how to expand the set of values returned by the command:

```
# set JBSRT_CMDRCD_EXTEND=1
# jbsrt_distrib
```

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 or JP1/Base administrator permission

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 [-f] [-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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/bin/

Arguments

-f

Specify this argument if you do not want a message confirming command execution (a message asking you to enter Y or N) to be output. If you specify this option, the message confirming command execution is omitted, the value Y is assumed, and processing continues. If you omit this option, a message confirming command execution will be displayed.

-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.

Environment variables

JBSRT_CMDRCD_EXTEND

This environment variable expands the set of values that can be returned by the command. To use the expanded set of return values, specify 1. To use the original (unexpanded) set of return values, specify 0. If you omit this environment variable, the command will return a value from the original set of return values.

Notes

If your JP1/IM - Manager version is 11-01 or earlier, do not set the `JBSRT_CMDRCD_EXTEND` environment variable as a system environment variable or a user environment variable. If you do, you might not be able to use IM

Configuration Management to configure the system hierarchy. Instead, use the command prompt or a batch file to set the `JBSRT_CMDRCD_EXTEND` environment variable.

- When operating under a system hierarchical configuration with three or more levels, the processes of hosts under a submanager may take too much time and fail to properly return a response. Hence, the `jbsrt_sync` command may result in timeout. For details, see [2.6.3 \(5\) Reviewing the communication timeout value](#).

Return values (original set)

0	Normal end
1	Abnormal end

Return values (expanded set)

0	Normal end
1	Synchronization of configuration definition information failed on some hosts.
2	Configuration management server processing is being performed.
3	The command timed out.
10	Invalid argument
11	Permission error
12	There is no configuration definition information.
13	A configuration definition information access error occurred, or the configuration definition information is corrupted.
16	An error occurred during communication with the configuration management server.
20	Insufficient memory
128	Other error

Example

The examples below show the command with the `-f` option specified and the command with the `-f` option omitted.

With the `-f` is specified:

```
# jbsrt_sync -f
Sending the synchronization request...
KAVB3112-I The synchronization command terminated normally.
```

With the `-f` option is omitted:

```
# jbsrt_sync
Do you want to execute the synchronous command? [Y/N] y
Sending the synchronization request...
KAVB3112-I The synchronization command terminated normally.
```

The following example shows how to expand the set of values returned by the command:

```
# set JBSRT_CMDRCD_EXTEND=1
# jbsrt_sync
```

jbssetacl

Function

The `jbssetacl` command registers operating permissions for individual JP1 users and DS group. The JP1 user can be a standard user, linkage user, or DS user.

Format

```
jbssetacl [-h logical-host-name]  
          [-s authentication-server-name]  
          -f definition-file-name  
          [-no]  
          [-ds#]
```

#:

The `-ds` option can be specified in Windows only.

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 or JP1/Base administrator permission

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 and DS group operating permissions. When you specify this option, the `-h` option is ignored, even if it is specified.

-f *definition-file*

Specify the name of the user permission definition file containing JP1 user and DS group operating permissions. The file format is the same as that of the user permission level file (`JP1_UserLevel`). You can give the user permission definition file any name and store it in any location. For details about the user permission definition file, see [User permission definition file](#) in *16. Definition Files*.

-no

When this option is specified, if operating permission is already given to the specified JP1 user and DS group, an error is returned and the operating permission for the JP1 user and DS group is not registered.

-ds

This option can be specified in Windows only.

Specify this option to register operating permission to a DS user or DS group. The operating permission to register is the one defined in the JP1 operating permission attribute value for the DS user or DS group registered in the directory server.

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.
- When the `-ds` option is specified, the reload command (`jbsaclreload`) must be executed.
- Duplicate registrations of operating permissions are not allowed.

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
12	An error occurred in the authentication server side when a DS user was used
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

jbssetadmingrp (UNIX only)

Function

The `jbssetadmingrp` command sets up an environment in which users with JP1/Base administrator permission can use JP1/Base. It also checks whether users in the JP1/Base administrator role are able to use JP1/Base.

Format

```
jbssetadmingrp {-s JP1-administrators-group [-f] | -v}
```

Required execution permission

Superuser permission

Command directory

/opt/jplbase/bin/

Arguments

-s *JP1-administrators-group*

Allows users in the JP1/Base administrator role to operate JP1/Base. When you specify this option, access permission for the files and directories provided by JP1/Base is assigned to the JP1 administrators group, allowing JP1/Base administrators to use JP1/Base. If you specify this option in an environment where use by JP1/Base administrator is already enabled, the existing JP1 administrators group is replaced with the one specified in this option.

Specify the JP1 administrator group as a character string of no more than 256 bytes.

To stop operation by JP1/Base administrators and temporarily allow only system administrators to use JP1/Base, specify the value below as the JP1 administrators group. You can restore the ability of the JP1 administrators group to use JP1/Base by executing the command again with the group name specified.

In SUSE Linux 15 or later: `root`

In Linux other than the above: `sys`

In AIX: `system`

-f

Specify this option to suppress the confirmation message displayed when you allow JP1/Base administrators to use JP1/Base. If you omit this option, the confirmation message is displayed.

-v

Specify this option to output messages related to the status of the JP1/Base administrators.

Notes

- Shut down JP1/Base before using this command with any option other than `-v`.
- Do not change the ID assigned to the JP1 administrators group after you use this command to allow JP1/Base administrators to use JP1/Base.

Return values

0	Normal end
1	Access permission change error
2	Invalid argument
3	Command executed while JP1/Base is running
4	Insufficient system resource such as memory
5	Invalid setting
6	Execution permission error
127	Internal error other than insufficient resources

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 or JP1/Base administrator permission

Command directory

In Windows:

```
installation-folder\bin\
```

In UNIX:

```
/opt/jplbase/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.

Note

- If you want to change the JP1/AJS common definition information, we recommend that you use the `jaajs_config` command. The `jaajs_config` command checks environment setting parameter names and definitions, thus preventing incorrect data from being registered. For details on the `jaajs_config` command, see the manual *JP1/Automatic Job Management System 3 Command Reference*.
- The end of each line in definition file must have linefeed character "CR,LF"(0x0D,0x0A) for Windows, "LF"(0x0A) for Unix).

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 or JP1/Base administrator permission

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 *16. 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 `jbssgetumap` command.
- When you register user mapping information by using a definition file that contains a large number of definitions, it might take a long time to apply the definition contents to the common definition information. While user mapping information is being updated, masked user functionality cannot be used, and therefore operations that require masked user functionality (such as JP1/AJS job execution and remote commands in JP1/IM - Manager) cannot be performed. Therefore, if you intend to update a large amount of user mapping information at one time, execute the `jbsssetumap` command in a maintenance period not during operation. If you want to update a large amount of user mapping information during operation, consider splitting the definition contents before executing the `jbsssetumap` command. This minimizes the time required by the `jbsssetumap` command to apply the definition contents to the common definition information.

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

jbsssetupsrv (Windows only)

Function

The `jbsssetupsrv` 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

```
jbsssetupsrv [-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

jbssetusrsv (UNIX only)

Function

The `jbssetusrsv` command specifies the authentication server (primary authentication server and secondary authentication server).

Execute this command on the following hosts:

- Host used as an authentication server
- Host on which a product that utilizes JP1/Base user authentication, such as JP1/IM - Manager and JP1/AJS - Manager, is installed

Format

```
jbssetusrsv [-h logical-host-name]  
             primary-authentication-server  
             [secondary-authentication-server]
```

Required execution permission

Superuser or JP1/Base administrator permission

Command directory

/opt/jplbase/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 `jbsumappass` command registers an OS user or an information-search user in the JP1/Base password management information. This command also enables you to change the registered OS user's or information-search user's password.

Format

```
jbsumappass [-h logical-host-name]  
            -u { OS-user-name | information-search-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* | *information-search-user-name* }

Specify the OS user name or information-search user name that you want to register or change in the password management information.

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.

To register an information-search user, type it in the format of `aduser/OS-user-name-used-as-the-information-search-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 [8.1.5 Assigning user permissions to OS users 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 or JP1/Base administrator permission

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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 or later 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 or later 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 <code>jcocmdconv</code> 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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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`, `-queueenum`, `-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 default is 196,600 records.

The number of records to be used in one command execution is $(\textit{number-of-command-output-rows} + 3)$ 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 *JP1/Integrated Management 3 - 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 host group definition file, see *Host group definition file* in *16. Definition Files*.

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-commands-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 15–2: 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 15–3: 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.
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 version of JP1/Base on the command-executing host is 07-51 or earlier, the default is `OFF` (not suppressed).

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 version of JP1/Base on the command-executing host is 07-51 or earlier, the default is OFF (not suppressed).

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 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 15–1: `jcocmddef` command output format

Response time: <u>60</u>	●	Response monitoring time (specified in <code>-rsptime</code>)
Record size: <u>20000</u>	●	Number of records (specified in <code>-record</code>)
LoadUserProfile: <u>OFF</u>	●	Whether user profiles can be loaded (specified in <code>-loaduserprofile</code>)
Queuing num: <u>1024</u>	●	Number of commands in queue (specified in <code>-queuenum</code>)
Execution num: <u>1</u>	●	Number of commands to be executed concurrently (specified in <code>-execnum</code>)
Record open: <u>OFF</u>	●	Whether the command execution log files can always be opened (specified in <code>-open</code>)
Record flush: <u>OFF</u>	●	Whether command execution logs can be written for each row (specified in <code>-flush</code>)
Action Event Level: <u>0</u>	●	Level for issuing an action status notification event (specified in <code>-actevent</code>)
Command Event Level: <u>0</u>	●	Level for issuing an a command execution operation event (specified in <code>-cmdevent</code>)
Action Result: <u>ON</u>	●	Whether automated action execution results are saved (specified in <code>-actresult</code>)
Running Event Interval: <u>600</u>	●	Interval of issuing the elapsed time notification event (specified in <code>-runeinterval</code>)
Action Result Limit: <u>1000</u>	●	Transferred data amount of automated action execution results (specified in <code>-actlimit</code>)
Window Result Limit: <u>1000</u>	●	Transferred data amount of command execution results (specified in <code>-cmdlimit</code>)
Queuing Threshold: <u>10</u>	●	Threshold for number of commands in queue (specified in <code>-queuethreshold</code>)
Groupname:groupim01	●	Host group name Host names belonging to the host group } Contents of the host group definitions file specified in <code>-group</code>
Host:hostA,HostB	●	

Legend:

 (underscore): Indicates the default value.

Return values

0	Normal end
-1	Abnormal end

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

```
jcocmdel [-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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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.

```
jcocmd del -s host01 1234
```

Output example

```
jcocmd del -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 c
ontrol.
```


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/jplbase/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, and when output suppression has been disabled by the `jcocmddef` command (with the `-actresult ON` option).

-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, execute  
d-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 or JP1/Base administrator permission

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 `joccmdshow` command, specify this option.

If you omit this option, the information items output by the `joccmdshow` 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   jpladmin 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     :jpladmin
STIME    :Feb 13 18:55:29
ETIME    :000:01:05
COMMAND  : "C:\WINNT\system32\notepad.exe"
```

Function

The `jevagtfw` command is executed on the manager host (host on which JP1/IM - Manager is installed).

This command is used to suppress events from being forwarded from an agent and stop event forwarding suppression. This command is also used to display a list of event forwarding suppression statuses. A maximum of 10,000 agents can be subject to this event-forwarding suppression.

Note that JP1/Base version of the agent host to be suppressed must be 08-00 or later.

Format

```
jevagtfw {-s [forwarding-suppression-definition-file-name] [-o {dispose | suppress | all}] [-n] host-name |  
         -r [-f | -m] host-name |  
         -l}  
         [-h logical-host-name]
```

Required execution permission

In Windows: Administrators privileges (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser or JP1/Base administrator privileges

Command directory

In Windows

`installation-folder\bin\`

In UNIX

`/opt/jp1base/bin/`

Arguments

`-s [forwarding-suppression-definition-file-name] [-o {dispose | suppress | all}] [-n] host-name`

Specify the host name of an agent whose event forwarding is suppressed. You can also specify a host not managed by the configuration definition. Specify the host name as a case-insensitive character string of no more than 128 bytes. The `-n` option is required if you specify the local host for *host-name*.

`forwarding-suppression-definition-file-name`

Specify the name of the user-specified event-forwarding suppression definition file. You cannot specify a path as the file name. If you omit this option, the `forward_suppress` file is assumed.

Note that the forwarding suppression definition file has the same format as the forwarding settings file.

`-o {dispose | suppress | all}`

Specify whether the manager discards the received events and whether the agent suppresses event forwarding. If you omit this option, `all` is assumed.

`dispose`

Suppression is set up only on the manager (received events are discarded).

`suppress`

Suppression is set up only on the agent (event forwarding is suppressed).

`all`

After suppression is set up on the manager to discard received events, event forwarding suppression is set up also on the agent.

`-n`

Specify this option if you want to suppress event forwarding on the local host.

`-r [-f | -m] host-name`

Specify the host name of an agent whose event forwarding suppression is stopped. Specify the host name as a case-insensitive character string of no more than 128 bytes.

`-f`

Event forwarding suppression is forcibly stopped even if the forwarding settings file (`forward`) on the agent has been changed during the event forwarding suppression (the forwarding settings will revert back to the settings before the event forwarding suppression).

`-m`

Event forwarding suppression (discarding the received events) is stopped only on the manager.

`-l`

Outputs the suppressed status for agents whose event forwarding is currently suppressed.

`-h logical-host-name`

Specify the event server name of the local host from which you are executing the command. Specify the event server name as a character string of no more than 128 bytes.

If you omit this option, the event server name is assumed as a host name in the following order of priority:

1. The logical host name specified in the `JP1_HOSTNAME` environment variable
2. The local host name, if an asterisk (*) or the local host name (physical host name returned by the `hostname` command) has priority in the `server` parameter of the event server index file (`index`)
3. The FQDN name, if an at mark (@) or FQDN name has priority in the `server` parameter of the event server index file (`index`)
4. The local host name (physical host name returned by the `hostname` command)

Note

During execution of the `jevagtfw` command with the `-s` option specified, if an error occurs after the setting to discard received events is successfully specified, suppression is set on the manager, but not on the agent. To resolve this condition, execute the `jevagtfw` command with the `-r -m` option specified to change the suppression status on the manager only.

When you want to include a Japanese filter condition in the forwarding setting file for event forwarding suppression, you must use an encoding supported by the language of the environment where the `jevagtfw` command is executed. The encoding of the forwarding setting file for event forwarding suppression is automatically converted when the language differs from a language set on the Japanese-language agent. For details on how to set the language, see [3.4.2 Setting the language \(for UNIX\)](#).

Return values

0	Normal end
1	Argument error

2	Cannot connect to the agent (plug-in service).
10	Event forwarding suppression cannot be stopped because the forwarding settings file (<code>forward</code>) on the agent has been changed.
255	Other error

Example

The following shows an example of the output when the `-s` option is specified:

```
# jevagtfw -s Agent01
KAJP1422-I The events received from AGENT01 will be discarded.
KAJP1430-I The events received from AGENT01 are now being discarded.
KAJP1419-I Event-forwarding from AGENT01 will be suppressed.
KAJP1401-I The forward file of AGENT01 is being backed up.
KAJP1404-I The forward file of AGENT01 was backed up. (file = /etc/opt/jplbase/conf/event/servers/default/suppress/Agent01/forward_backup)
KAJP1405-I The forward file for suppressing event-forwarding will be sent to AGENT01.
KAJP1408-I The forward file for suppressing event-forwarding was applied to AGENT01.
KAJP1410-I Event-forwarding from AGENT01 is now being suppressed.
#
```

The following shows an example of the output when the `-r` option is specified:

```
# jevagtfw -r Agent01
KAJP1427-I Discarding of events received from AGENT01 will be stopped.
KAJP1424-I Discarding of events received from AGENT01 was stopped.
KAJP1420-I The suppression of event-forwarding from AGENT01 will be stopped.
KAJP1414-I The contents of the forward file of AGENT01 will be checked.
KAJP1416-I An applicable forward file for suppressing event-forwarding is specified for AGENT01.
KAJP1417-I The backed-up forward file will be sent to AGENT01.
KAJP1418-I The backed-up forward file was applied to AGENT01.
KAJP1421-I The suppression of event-forwarding from AGENT01 was stopped.
#
```

The following shows an example of the output when the `-l` option is specified:

```
# jevagtfw -l
KAJP1413-I Manager is now suppressing event-forwarding from the following hosts:
Host                Suppressed-date      Dispose    Suppress
-----
AGENT01             2013/12/31 10:15:36 Yes        Yes
AGENT05             2013/11/29 05:21:03 Yes        Yes
AGENT11             2014/01/07 03:11:45 Yes        Yes
#
```

The following table describes meaning of the headers.

Header	Description
Host	Name of the host on which the event server whose event forwarding is currently suppressed is running.
Suppressed-date	Time when the event forwarding suppression is started.
Dispose	<p>Indicates whether received events are set to be discarded.</p> <p>Yes Received events are discarded.</p> <p>No Received events are not discarded.</p>
Suppress	<p>Indicates whether event forwarding is set to be suppressed.</p> <p>Yes Event forwarding is suppressed.</p> <p>No Event forwarding is set not suppressed.</p>

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 [10.2 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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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
<code>IMEvent{0 1}.idx</code>	<code>0IMEvent{0 1}.idx</code>
<code>IMEvent{0 1}.dat</code>	<code>0IMEvent{0 1}.dat</code>
<code>IMEvent{0 1}.fwd</code>	<code>0IMEvent{0 1}.fwd</code>

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.
- If you modified the serial number of the event database by using the `jevdbinit` command with the `-s` option specified on the host with JP1/IM - Manager installed, you need to set up the integrated monitoring database again. You also need to re-create the command execution log in JP1/IM - Manager. See the chapter on JP1/IM system maintenance in the *JP1/Integrated Management 3 - Manager Administration Guide*.

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 [2.3.2 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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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).
- The maximum value for the source event database serial number is not cleared in the case where the duplication prevention table is re-created by the `jevdbmkrep` command when no JP1 events have been received from the source event server since a JP1 event for clearing the duplication prevention table was issued by the target event server. After you have executed the `jevdbmkrep` command, issue a JP1 event for clearing the duplication prevention table again.

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 [10.2 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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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-name1] |  
               -e [distribution-definition-file-name2] |  
               -l [distribution-definition-file-name3] |  
               -s [distribution-definition-file-name4] }  
               [-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 or JP1/Base administrator permission

Command directory

In Windows:

`installation-folder\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

-f [*distribution-definition-file-name1*]

Specify the `-f` option to distribute definitions in the forwarding settings file (`forward`). If you create a distribution definition file with the name `jev_forward.conf`, you do not need to specify 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. You cannot use the `\`, `/`, `:`, `,`, `;`, `*`, `?`, `"`, `<`, `>`, `|`, tab, or space characters when specifying the file name. Create a distribution definition file for each forwarding settings file in the appropriate location, as described in *Distribution definition file* in *16. 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-name2*]

Specify the `-e` option to distribute definitions in the action definition file for event log trapping (`nthevent.conf`). If you created a distribution definition file with the name `jev_nthevent.conf`, you do not need to specify 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. You cannot use the `\`, `/`, `:`, `,`, `;`, `*`, `?`, `"`, `<`, `>`, `|`, tab, or space characters when specifying the file

name. Create a distribution definition file for each forwarding settings file in the appropriate location, as described in *Distribution definition file* in 16. *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-name3]

Specify the `-l` option to distribute definitions in the action definition file for log file trapping. If you created a distribution definition file with the name `jev_logtrap.conf`, you do not need to specify the file name. If you have prepared a distribution definition file with another name, specify that file name. You cannot specify a directory name as the file name. You cannot use the `\`, `/`, `:`, `,`, `;`, `*`, `?`, `"`, `<`, `>`, `|`, `tab`, or space characters when specifying the file name. Create a distribution definition file for each forwarding settings file in the appropriate location, as described in *Distribution definition file* in 16. *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.

-s [distribution-definition-file-name4]

Specify the `-s` option to distribute definitions in a log-file trap startup definition file (`jevlog_start.conf`). The definitions in the log-file trap startup definition file are not reloaded into the log-file trap management service (daemon). The definitions will be enabled next time the log-file trap management service starts.

If you created a distribution definition file with the name `jev_logstart.conf`, you do not need to specify the file name. If you gave the file another name, specify the name of the file. You cannot specify a directory name. You cannot use the `\`, `/`, `:`, `,`, `;`, `*`, `?`, `"`, `<`, `>`, `|`, `tab`, or space characters when specifying the file name. Create each distribution definition file in the appropriate location, as described in *Distribution definition file* in 16. *Definition Files*. To distribute a log-file trap startup definition file, the distribution source and destination hosts must both be running JP1/Base version 10-00 or later.

-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] |  
-s}  
          [-r host-name[,host-name...]]  
          [-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 or JP1/Base administrator permission

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-for-log-file-trapping*]

This argument enables you to collect definitions from an action definition file for log file trapping. For the log file trap definition file name, specify a file name or relative path of your choice. The definition information is distributed to the specified file or relative path under the following folder on the target host:

- In Windows: *installation-folder*\conf\
- In UNIX: /etc/opt/jp1base/conf/

Specify a file name so that the length of the full path, including the above folder, does not exceed 256 bytes.

Note that you cannot use tabs, spaces, or the following symbols when specifying the distribution definition file: :, ,, ;, *, ?, ", <, >, or |. Furthermore, you cannot use ". ." in the file name to indicate a higher-level directory.

If you omit the log file trap definition file name, `jevlog.conf` is assumed.

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.

-s

Specify the `-s` option to collect definitions in the log-file trap startup definition file (`jevlog_start.conf`). The command only collects these definition if the source and destination hosts are running JP1/Base version 10-00 or later.

-r *host-name* [, *host-name* . . .]

Specify the `-r` option to collect definitions from specific hosts. If you omit this option, information is collected from all hosts. Use commas to separate multiple host names.

-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

jeventreload (Windows only)

Function

The `jeventreload` command reloads the action definition file for event log trapping (`nthevent.conf`).

Format

```
jeventreload
```

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 or `unicode-trap` parameter, you must restart the event-log trapping service. If you execute this command without restarting the service, an error occurs (the message KAVA3009-E is output) 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}]  
          [-l encoding-name]  
          [-k items-file-name]  
          [-a]
```

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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 (extension: `dat`) 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 *16. 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`.

-l encoding-name

When converting data to CSV format, the `jevexport` command converts character strings in the event database to the encoding specified in this option. If you omit this option, the converted data retains the encoding of the event database. You can specify the following encodings:

- SJIS
- EUCJIS
- ISO2022JP
- UTF-8

-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.

To output these items in Japanese, specify an encoding in the encoding name attribute of the `-l` option. If you omit the `-l` option, the titles are output in English.

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 settings 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 *16. Definition Files*.
- If you implement character code conversion using the `-l` option, machine-dependent characters will not be converted correctly.
- 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 an 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.
- The maximum size of the CSV file that can be output using the `evexport` command is 2 GB. The CSV file will easily reach 2 GB if a command is executed without specifying a filter and the `db-size` parameter in the event server environment settings file (`conf`) is set to 1 GB or more. In such a case, a command error might occur. To prevent this command error from occurring, filter the events to be output by using the `-f` option or output the events for each file by using the `-i` option.

Return values

0	Normal end
1	Invalid argument
2	CSV output was interrupted because the event database was switched during command processing
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
```

jevextreload

Function

The `jevextreload` command reloads an additional extended attribute settings file (`recv_add_extattr` and `send_add_extattr`).

Format

```
jevextreload [-h event-server-name] { -recv | -send }
```

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 or JP1/Base administrator permission

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 an additional extended attribute settings file. You can specify a character string that is no more than 255 bytes long.

If this option is not specified, the command determines the event server name in the following order:

1. If the logical host name is specified in the `JP1_HOSTNAME` environment variable, that logical host name is used.
2. If an asterisk (*) or the local host name (physical host name returned by the `hostname` command) is preferentially specified for the `server` parameter in the event server index file (`index`), the local host name is used.
3. If an at mark (@) or FQDN name is preferentially specified for the `server` parameter in the event server index file (`index`), the FQDN name is used.
4. The local host name (physical host name returned by the `hostname` command) is used.

{ `-recv` | `-send` }

Specify the type of the additional extended attribute settings file that you want to reload (file for transfer reception or event registration).

`-recv`

Specify this argument to reload the additional extended attribute settings file for transfer reception (`recv_add_extattr`). If the `recv_add_extattr` file does not exist in the command directory, the command terminates normally, disabling the relevant additional extended attribute settings.

-send

Specify this argument to reload the additional extended attribute settings file for event registration (`send_add_extattr`). If the `send_add_extattr` file does not exist in the command directory, the command terminates normally, disabling the relevant additional extended attribute settings.

Return values

0	Normal end
1	Invalid argument
2	The specified event server has not started.
3	The additional extended attribute settings file contains an error.
255	Other error

Example

The following shows an example of use.

In this example, the command reloads the additional extended attribute settings file for transfer reception on the `evserver1` event server:

```
jevextreload -h evserver1 -recv
```

jevlogdstart (UNIX only)

Function

The `jevlogdstart` command starts the log-file trap management daemon. Before you use JP1/AJS log file monitoring jobs, execute this command to start the log-file trap management daemon.

Format

```
jevlogdstart
```

Required execution permission

Superuser or JP1/Base administrator permission

Command directory

`/opt/jp1base/bin/`

Return values

0	Normal end
255	Abnormal end

jevfwstat

Function

The `jevfwstat` command displays JP1 event forwarding suppression status for each condition for the suppression of event-forwarding (`suppress`).

Format

```
jevfwstat [-h event-server-name]
```

Required execution permission

In Windows: Administrators privileges (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser or JP1/Base administrator privileges

Command directory

In Windows

installation-folder\bin\

In UNIX

/opt/jp1base/bin/

Argument

-h *event-server-name*

Specify an event server name on which you want to check the JP1 event forwarding status. Specify the event server name as a character string of no more than 128 bytes.

If you omit this option, the event server name is assumed as a host name in the following order of priority:

1. The logical host name specified in the `JP1_HOSTNAME` environment variable
2. The local host name, if an asterisk (*) or the local host name (physical host name returned by the `hostname` command) has priority in the `server` parameter of the event server index file (`index`)
3. The FQDN name, if an at mark (@) or FQDN name has priority in the `server` parameter of the event server index file (`index`)
4. The local host name (physical host name returned by the `hostname` command)

Note

You cannot execute multiple instances of the `jevfwstat` command at the same time. If you attempt to execute the `jevfwstat` command when another user is executing the same command, the message KAJP1352-E is output and the command execution fails.

Return values

0	Normal end
1	Argument error
2	Event server is not running.

3	Another user is executing the command.
255	Other error

Example

The following shows an example of the output:

```
KAJP1350-I The status of the threshold-based suppression of event-forwarding
for agent01 will be checked.
ID          C  Forwarded Suppressed LastModified      BaseTime Detection
-----
log1        F      8          0 None             11:37:10      0/1
log2        S     136       1274 2014/05/22 11:33:42 11:37:02      1/2
log3        F     309       520 2014/05/22 11:33:12 11:37:12      2/3
```

The following table describes meaning of the headers.

Header	Description
ID	Identifier specified for the condition for the suppression of event-forwarding (<code>suppress</code>)
C	S is output when event forwarding is in suppressed status, and F is output when in forwarded status (suppression-stopped status).
Forwarded#	The number of JP1 events that were forwarded.
Suppressed#	The number of JP1 events that were suppressed from being forwarded.
LastModified	The most recent time at when the suppression status has changed.
BaseTime	The time used as the base for the current unit time.
Detection	Output differs depending on whether event forwarding is in suppressed status (the C value is S) or forwarded status (the C value is F). Suppressed status (the C value is S): n/m <i>n</i> : The number of unit times in which the threshold was not exceeded <i>m</i> : The number of unit times that the system determines that the large numbers of events have converged Forwarded status (the C value is F): n/m <i>n</i> : The number of unit times in which the threshold was exceeded <i>m</i> : The number of unit times that the system determines that a large number of events has occurred

#

If you reload the event service (by executing the `jevreload` command) or restart the system, each value will default to 0.

jevlogdstat

Function

The `jevlogdstat` command shows the operating status of the log-file trap management service (daemon). The operating status of the log-file trap management service (daemon) can be identified from the messages and return values of this command.

Format

```
jevlogdstat
```

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jp1base/bin/

Return values

0	The log-file trap management service (daemon) is active.
1	Invalid argument
2	The log-file trap management service (daemon) is inactive.
4	The log-file trap management service (daemon) is starting.
7	Insufficient memory
8	Permission error
9	Communication error
255	Other error

jevlogdstop (UNIX only)

Function

The `jevlogdstop` command stops the log-file trap management daemon.

Format

```
jevlogdstop
```

Required execution permission

Superuser or JP1/Base administrator permission

Command directory

`/opt/jp1base/bin/`

Note

The log-file trap management daemon runs on both the logical and physical hosts. Executing the `jevlogdstop` command stops all the running log file traps, including any JP1/AJS log file monitoring jobs. Then, you can no longer use log file traps and JP1/AJS log file monitoring jobs. When you execute the `jevlogdstop` command, make sure that log file traps and JP1/AJS log file monitoring jobs are not being used on either the logical or 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 or JP1/Base administrator permission

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 and by JP1/AJS log file monitoring jobs. However, do not modify the action definition file for log file trapping started by JP1/AJS log file monitoring jobs. If you modify and then reload the action definition file, you might no longer be able to perform monitoring correctly.

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	The event server is inactive.
7	Insufficient system resource such as memory
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.

The locale information (language specified for `LANG` or other settings) in the environment in which this command was executed is used for monitoring logs and registering JP1 events. Therefore, you must set the same language for the action definition file for log file trapping and for the monitored log files.

For details about the languages of log files that can be monitored in UNIX, see [3.4.2 Setting the language \(for UNIX\)](#). In Windows, the languages of log files that can be monitored are MS932, Unicode (UTF-8, UTF-16), and C. To monitor Unicode files, create an action definition file for log file trapping in the language of the OS, not in Unicode.

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.

After you execute this command and a log file trap starts successfully, the ID of the log file trap is output to the standard output. This ID is a thread ID in Windows, or a process ID in UNIX. This ID is used by the following commands:

- `jbsgetopinfo` command (Collect operating information)
- `jevlogstat` command (Check the operating status)
- `jevlogstop` command (Stop the log file trap)
- `jevlogreload` command (Reload)

For details on the command used to collectively start the log file traps specified in a log-file trap startup definition file when a failover occurs in a cluster system, see [jevlogstart \(cluster environment only\)](#).

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]  
            [{-g UTF-8 | -g [UTF-16] [-b { LE | BE }]}] (Windows only)  
            [-x]  
            { log-file-name1[...log-file-name32(100)] |  
              log-file-name (when monitoring UPD log files) }
```

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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.

Note that you cannot specify the action definition file for log file trapping under one of the following conditions:

- The folder name, directory name, or file name contains an environment-dependent character.
- In UNIX, the file name contains a space character.
- In Windows, the file is a Unicode file.

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/jplbase/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:

$log\text{-file-size (bytes)} \times number\text{-of-log-files} > output\text{-size-per-second (bytes)} \times monitoring\text{-interval (seconds)}$

-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 without this option after the program that outputs log data 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. You cannot include a space character in the display command name. If you omit this option, *log-file-name1* is assumed as the display command name.

-p *log-data-source-program-name*

Specify the name of the program that outputs the log data. Specify the program name in no more than 256 bytes. You cannot include a space character in the program name.

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 monitoring UPD type log files, the log file trapping function checks for monitoring targets at the interval specified in the `-t` option, until it detects a log file whose file name matches the name (and wildcard pattern) specified when the log file trap was started.

When monitoring log files on a shared disk, configure the log file trap to start and stop when the logical host starts and stops. Use the `-r` option when you want to monitor log files that are created after the log file trap starts.

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. Destination server names are case sensitive.

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.

-g UTF-8 | -g [UTF-16] [-b { LE | BE }]

This option can be specified in Windows only.

If you specify this option, the log file trap monitors the log files as Unicode files. Also, JP1 events are registered in the UTF-8 code set. As the regular expressions used, extended regular expressions are applied to the conditions in the action definition file.

If you omit this option, the log file trap monitors the log files as non-Unicode files.

-g UTF-8

The log file trap monitors the log files as UTF-8 Unicode files.

-g [UTF-16]

The log file trap monitors the log files as UTF-16 Unicode files. You can omit the specification value, `UTF-16`.

Note that this argument cannot be specified if `HTRACE` is specified for the `FILETYPE` parameter in the log file trap definition file.

The following UTF-16 Unicode types are supported for monitoring:

- UTF-16: UTF-16 with BOM (Byte Order Mark)
- UTF-16LE: Little-endian UTF-16 without BOM
- UTF-16BE: Big-endian UTF-16 without BOM

When monitoring Unicode files with BOM:

The byte order (Little-endian or Big-endian) is determined by the BOM value.

When monitoring Unicode files without BOM:

You can use the `-b { LE | BE }` option to specify the byte order of the Unicode files. If you omit the `-b { LE | BE }` option, the byte order is determined depending on the processor architecture. In Windows, log files are monitored as Little-endian Unicode files (UTF-16LE format).

-b { LE | BE }

You can use this option to explicitly specify the byte order of Unicode files. This option must be specified following the `-g [UTF-16]` option.

When monitoring Unicode files with BOM:

This option is ignored and the byte order is determined by the BOM value.

When monitoring Unicode files without BOM:

Log files are monitored as Unicode files with the specified format. You can specify either of the following values:

`LE`

Log files are monitored as Little-endian Unicode files (UTF-16LE format).

BE

Log files are monitored as Big-endian Unicode files (UTF-16BE format).

-x

Specify this option to set the output source host in the `JP1_SOURCEHOST` extended attribute of log file data converted to JP1 events.

log-file-name1 [. . . log-file-name32 (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. Specify the log file names after the final option.

Do not specify the following log file names:

- A file name that begins with a hyphen (-).
- A folder name, directory name, or file name that contains an environment-dependent character
- In UNIX, a directory name or file name that contains a space character

You can specify 32 log file names in Windows, and 100 in 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.

Note that when you specify a single log file for one execution of the `jevlogstart` command, the output order of log data matches the registration order of JP1 events. Conversely, when you specify multiple log files for one execution of the `jevlogstart` command, each log file is monitored independently. At this time, log data might be output over multiple log files during an interval between monitoring operations. In such a case, the output order of log data might not match the registration order of JP1 events because each log file is monitored in parallel.

Therefore, the `ps` command lists the command names in the form `log-file-name.child`.

log-file-name (when monitoring UPD log files)

Specify the log file name to use when monitoring UPD type files in no more than 256 bytes. Use this argument when you specify UPD in the `FILETYPE` parameter of the action definition file for log file trapping.

Specify a log file name using wildcards (* or ?). An asterisk represents a character string of zero or more characters, and a question mark represents any one character. You can use wildcards in the file name, but not the path. For UNIX, refer to the following examples to prevent the shell from evaluating wildcards:

Example:

- Enclose the file name with double quotation marks ("").

```
"/home/log*.log"
```

- Escape the wildcard with a backslash (\).

```
/home/log\*.log
```

For both Windows and UNIX, you can specify only one file name.

You can specify only one file name in Windows and UNIX.

If you specify a relative path, make sure that the full path with the directory names added will not exceed 256 bytes. The path is interpreted relative to the current directory at command execution. Specify the log file name after the final option. Log file names are case sensitive.

Do not specify the following log file names:

- A file name that begins with a hyphen (-).
- A folder name, directory name, or file name that contains an environment-dependent character
- In UNIX, a directory name or file name that contains a space character

Notes

- Some types of log files cannot be monitored. For details on the formats of log files that can or cannot be monitored, see [2.4.4 Types of log files that can be monitored](#) and [2.4.5 Types of log files that cannot be monitored](#).
- 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.
- When monitoring UPD log files, if you start a log file trap that monitors a log file name specified using several wildcards (*), the log file trapping function might take a long time to search for monitoring targets. For this reason, use wildcards only where necessary.
- When monitoring UPD log files, the log file trapping function will not monitor files with file names longer than 256 bytes, even if the file matches the wildcard pattern.
- When monitoring UPD log files, the log file trapping function might monitor a non-log file created in the target directory if it happens to match the wildcard pattern. Do not use the monitoring-target directory as a destination for backup files or other data.
- If the message KAVA3667-E or KAVA3672-E is output when you monitor UPD log files, there might be more than one log file with the most recent update time (within one second). Change the file names so that only one of these files matches the wildcard pattern, and then restart the log file trap.
- If you executing the `jevlogstart` command with the `-g` option specified to monitor Unicode files, JP1 events are registered in the UTF-8 code set. Upgrade the JP1/Base on the host (to which those JP1 events are forwarded) to version 8 or later.
- If you specify the `-h` option and a large log file is monitored, loading of the log data that was output after log file trapping started might be delayed or many events might occur. If a loading delay or the occurrence of many events adversely affects operation, stop the log file trapping and then restart it without specifying the `-h` option.

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 <code>-a</code> 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 6 applies to monitoring UPD log files.

Example 1

Search for and read data from log file `c:\log\logfile1.log`. This example omits all arguments except the log file name. In this case, the log-file trap startup definition file is `jevlog.conf` in the JP1/Base conf folder, the monitoring interval is 10 seconds, and the maximum 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 the UTF-8 Unicode file `logfile_uni.log` in `c:\log`, using the action definition file for log file trapping `c:\conf\configfile.conf`.

```
jevlogstart -f c:\conf\configfile.conf -g UTF-8 c:\log\logfile_uni.log
```

Example 4

Search for and read data from the UTF-16BE-format Unicode file `logfile_uni_be.log` in `c:\log`, using the action definition file for log file trapping `c:\conf\configfile.conf`.

```
jevlogstart -f c:\conf\configfile.conf -g UTF-16 -b BE c:\log\logfile_uni_be.log
```

Example 5

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
```

Example 6

Search for and read data from a file in the `c:\log` folder whose name begins with `logfile.`, using the action definition file for log file trapping `c:\conf\configfile.conf`.

```
jevlogstart -f c:\conf\configfile.conf c:\log\logfile.*
```

jevlogstart (cluster environment only)

Function

The `jevlogstart` command starts the log file traps specified in the `START_OPT_CLS` parameter of a log-file trap startup definition file. By registering this command with the cluster software, you can automatically start log file traps on the server that takes over as the primary node when a failover occurs.

Format

```
jevlogstart -cluster [cluster-ID]
```

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jp1base/bin/

Arguments

-cluster [*cluster-ID*]

Specify this option to start those log file traps specified in the `START_OPT_CLS` parameter of the log-file trap startup definition file that match the specified cluster ID. The cluster ID can be a value from 0 to 99. If you do not specify a cluster ID, 0 is assumed.

Note

If there are several log file traps to be started, the `jevlogstart` command might not have finished starting all the log file traps by the time the KAVA3652-I message is output. Wait a while before making sure all the log file traps have started.

Return values

0	Normal end
1	Invalid argument
2	The log-file trap management service or daemon is inactive.
255	Other error

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/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 started by the `jevlogstart` command and by JP1/AJS log file monitoring jobs. 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.

For details on the command you can use to stop all of the log file traps that were started by the `jevlogstart` command when a failover occurs in a cluster environment, see *jevlogstop (cluster environment only)*.

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

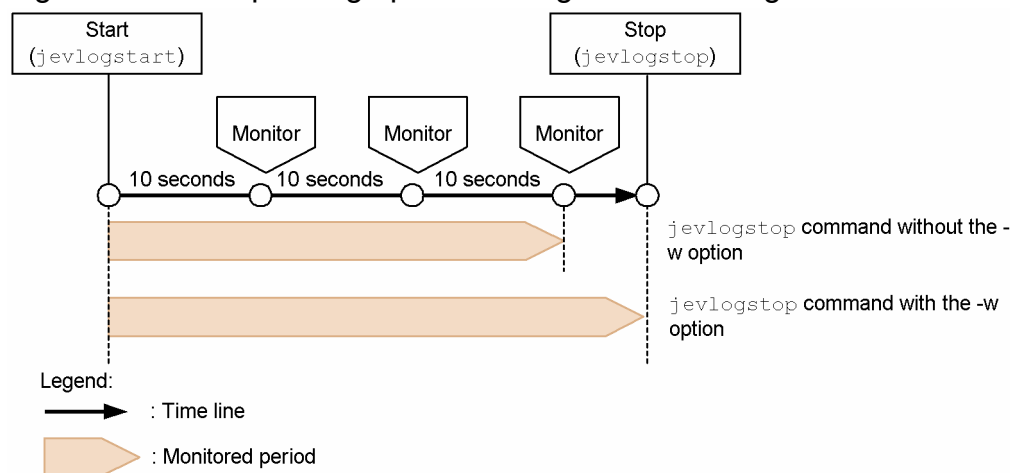
/opt/jp1base/bin/

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 15–2: 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 and by JP1/AJS log file monitoring jobs.

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

jevlogstop (cluster environment only)

Function

The `jevlogstop` command stops log file traps started earlier by the `jevlogstart` command. By registering this command with the cluster software, you can automatically stop log file traps on the failed host before failover takes place.

Format

```
jevlogstop -cluster [cluster-ID]
```

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/bin/

Arguments

-cluster [*cluster-ID*]

Specify this option to stop log file traps that were started by the `jevlogstart` command specifying a particular cluster ID. The cluster ID can be a value from 0 to 99. If you do not specify a cluster ID, 0 is assumed.

Return values

0	Normal end
1	Invalid argument
2	The log-file trap management service or daemon is inactive.
3	The log file traps do not exist (the traps have already stopped).
255	Other error

jevmessageid.bat (Windows only)

Function

The `jevmessageid.bat` command changes the setting for whether message IDs are to be assigned to the messages of the event service that are output to the event log.

This command is a batch file. It cannot be customized by the user.

Format

```
jevmessageid.bat { -r | -u }
```

Required execution permission

Administrators permission (if the Windows UAC function is enabled, execute this command from the administrator console.)

Command directory

installation-folder\bin\

Arguments

-r

Changes the setting so that message IDs will be assigned to the messages that are output to the event log by the event service.

-u

Changes the setting so that message IDs will not be assigned to the messages that are output to the event log by the event service.

Notes

- If Event Viewer is being used to display messages, this change is also applied to the messages that were output to the event log before the change was made. If Event Viewer is running, this change is applied after the Event Viewer is restarted.
- If events are converted to JP1 events by event log trapping, this change is applied only to the event logs that are output after this change has been made.
- The same setting must be used for the physical host messages and the logical host messages.

Return values

0	Normal end
1	Invalid argument
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
- When an event server for audit log data only is set in JP1/Audit

#:

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 or JP1/Base administrator permission

Command directory

In Windows:

installation-folder\bin\

In UNIX:

/opt/jplbase/bin/

Arguments

-h *event-server-name*

Specify the name of the event server on which you want to reload the forwarding settings file (`forward`). Specify the event server name as a character string of no more than 255 bytes.

If you omit this option, the event server name is determined in the following order of priority:

1. The logical host name specified in the `JP1_HOSTNAME` environment variable.
2. The local host name, if an asterisk (*) or the local host name (the physical host name returned by the `hostname` command) has priority in the `server` parameter of the event server index file (`index`).
3. The FQDN name, if an at mark (@) or FQDN name has priority in the `server` parameter of the event server index file (`index`).
4. The local host name (the physical host name returned by the `hostname` command).

Notes

Executing the `jevreload` command also reloads the conditions for suppression of event-forwarding (`suppress`) that are used for threshold-based suppression of event forwarding. Reloading the conditions for suppression of event-forwarding (`suppress`) affects event forwarding suppression status as follows:

- Stops the event forwarding suppression status.
- Clears the total number of JP1 events that correspond to each condition for suppression of event-forwarding.
- Clears the unit time and check count for each condition for suppression of event-forwarding.

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/jplbase/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 [17.1.2 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.
- Do not specify any event server names that are specified for `-s` (or ones that are assumed when the option is omitted). Specifying the same event server name for `-s` and this option causes unnecessary event forwarding, which increases the risk that JP1 events cannot be registered due to forwarding errors.

-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.
- In a UNIX system, if a message or extended attribute contains non-ASCII Japanese characters, make sure the correct encoding is specified in the `LANG` environment variable.

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/jplbase/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 [17.1.2 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.
- Do not specify any event server names that are specified for `-s` (or ones that are assumed when the option is omitted). Specifying the same event server name for `-s` and this option causes unnecessary event forwarding, which increases the risk that JP1 events cannot be registered due to forwarding errors.

-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 6.

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.
- In a UNIX system, if a message or extended attribute contains non-ASCII Japanese characters, make sure the correct encoding is specified in the LANG environment variable.
- This command does not return control until the arrival is verified or an error is detected.

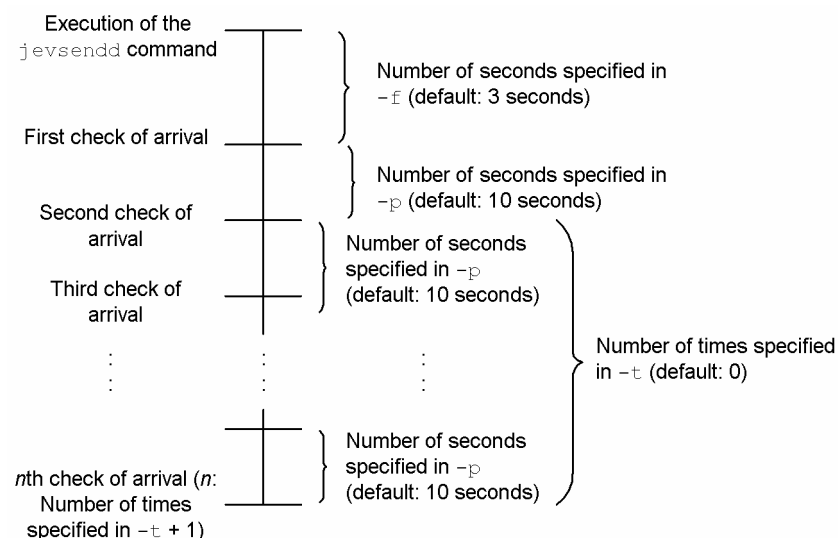
Return values

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 15–3: Behavior when the `-f`, `-p`, and `-t` options are specified



You can use the following expression to obtain the maximum time for waiting for arrival:

$$\text{Maximum-time-for-waiting-for-arrival} = (\text{number-of-seconds-specified-in-}\text{-f}\text{-option}) + (\text{number-of-seconds-specified-in-}\text{-p}\text{-option}) \times (\text{number-of-times-specified-in-}\text{-t}\text{-option})$$

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 or JP1/Base administrator permission

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.

Note

If you manually start an event server instead of automatically starting it, locale information used when the event service is started (for example, the `LANG` environment variable) must match the language specified in `jp1bs_env.conf`.

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 or JP1/Base administrator permission

Command directory

In Windows:

`installation-folder\bin\`

In UNIX:

`/opt/jplbase/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. Specify the event server name as a character string of no more than 255 bytes.

If you omit this option, the event server name is determined in the following order of priority:

1. The logical host name specified in the `JP1_HOSTNAME` environment variable.
2. The local host name, if an asterisk (*) or the local host name (the physical host name returned by the `hostname` command) has priority in the `server` parameter of the event server index file (`index`).
3. The FQDN name, if an at mark (@) or FQDN name has priority in the `server` parameter of the event server index file (`index`).
4. The local host name (the physical host name returned by the `hostname` command).

-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. If you omit this option, the default of 60 applies.

Notes

- The error message KAJP1706-E might be output if you execute the `jevstat` command immediately after an event service starts. In such a case, execute the `jevstat` command a few seconds after the event service starts.
- If you execute the `jevstat` command and the message KAJP1775-E is output to an integrated trace log, the command might have timed out. 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 /jpl/share/
```

Examples of `jevstat` commands and their results:

jevstat command execution examples	Execution results
<code>jevstat</code>	Outputs the status of the event server on the physical host.
<code>jevstat hostzz</code>	Outputs an error message indicating that the specified event server name was not found.
<code>jevstat HOSTZZ</code>	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 wil
l 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 or JP1/Base administrator permission

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

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 or JP1/Base administrator permission

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 `Jiskymnt` 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)

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 or JP1/Base administrator permission

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.

Return values

0	Normal end
1	Abnormal end

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 15–4: 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 15–5: 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 or JPI/Base administrator permission

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-destinatio
n-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 or JP1/Base administrator permission

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 or JP1/Base administrator permission

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 (").

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 or JP1/Base administrator permission

Command directory

In Windows:

```
installation-folder\bin\
```

In UNIX:

```
/opt/jplbase/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 or JP1/Base administrator permission

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 15–6: Items in the key definition parameter file (for adding, deleting and reorganizing keys)

Keyword	Format	Contents
<code>fi-</code>	<i>file-name</i> ^{#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 <i>file-name</i> is four characters fewer than the maximum file name length of the OS.
<code>an-</code>	<i>key-item-name</i> ^{#2}	Specify a key item name when you add a key.
<code>dn-</code>	<i>key-item-name</i> ^{#2}	Specify a key item name when you delete a key.
<code>rn-</code>	<i>key-item-name</i> ^{#2}	Specify a key item name when you reorganize a key. If you want to reorganize all keys, omit <i>key-item-name</i> .
<code>ke-</code>	<i>t=key-attribute</i> <i>, p=key-position</i> <i>, l=key-length</i> <i>[, ISDESC]</i>	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} <i>key-attribute</i> In <i>key-attribute</i> , 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 (DOUBLETYP) <i>key-position</i> The value to be specified in <i>key-position</i> differs depending on the record type. Fixed-length record type:0 to (<i>record-length</i> - 1) Variable-length record type:0 to (<i>minimum-record-length</i> - 1) <i>key-length</i> The value to be specified in <i>key-length</i> differs depending on the key attribute. c (CHARTYPE): 1 to 255 i (INTTYPE): 2 l (LONGTYPE): 4 f (FLOATTYPE): 4

Keyword	Format	Contents
		d (DOUBLETTYPE): 8 ISDESC Indicates that key elements are in descending order. Omitting this keyword indicates that key elements are in ascending order.
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 (000000000) ₂ . In UNIX: Bits 4 to 13 are reserved bits and set to (000000000) 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.

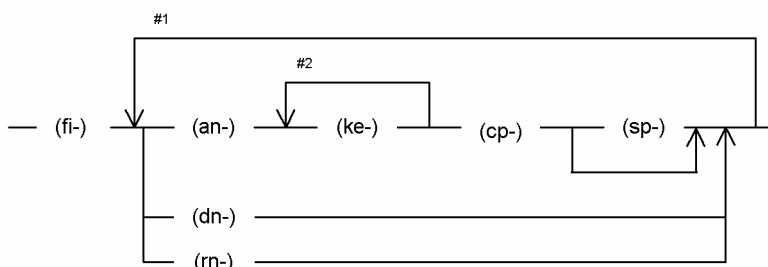
#3: You cannot specify more than one constituent element whose key attribute, key position, key length and key order (ISDESC) are the same.

#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 or JP1/Base administrator permission

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: K0
1 ISAM file name: ISAMFILE Offset: 0x00000000
KAIU342-W A definition file entry does not match the number of key file re
cords.
        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 or JP1/Base administrator permission

Command directory

`/opt/jplbase/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/jplbase/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/jplbase/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/jplbase/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

Jismlocktr (Windows only)

Function

The `Jismlocktr` 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
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

[2]C:\TEMP\TEST11.DRF        File lock table information
usedEntryCount:2            Number of entries in use
--- 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        File lock table information
usedEntryCount:0            Number of entries in use
--- PID --- TID --- fd --- Offset --- lngth --- mode --- time ---
```

Registry information

Lock table information

Format

```
Jismlocktr
```

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 or JP1/Base administrator permission

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.

Notes

- If you want to redirect the record information to a text file, specify the destination file name after >.

Example:

```
Jispert sample > prt.txt
```

- In UJIS environments single-byte Katakana characters are replaced with periods in the command output.

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 or JP1/Base administrator permission

Command directory

/opt/jp1base/bin/

Notes

- 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 `jbsetcnf` 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 or JP1/Base administrator permission

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 (do not add a forward slash (/) to the end of the path) 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
<i>shared-directory</i> /jplbase/conf/	Definition files
<i>shared-directory</i> /jplbase/log/	Log file
<i>shared-directory</i> /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/jplbase/conf/event/index`) of the event service on the local disk. The 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.
- 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 `/shdisk/lnode0`.

At the primary node:

```
jplbase_setup_cluster -h lnode0 -d /shdisk/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:

```
jplbase_setup_cluster -h lnode0
```

Return values

0	Normal end
---	------------

1	Abnormal end
---	--------------

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\

Notes

- Do not execute this command when JP1/Base is active.
- When executing this command, Windows Defender might output warning messages. These warning messages, however, are output due to the registration of services and may be safely ignored.

jp1ping

Function

The `jp1ping` command displays the IP address corresponding to a specified host name and its communication result (the result of executing the `ping` command) for the IP address, based on the JP1/Base communication settings.

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] [-v] [-s]  
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.

-v

Specify this option to display the IP addresses resolved from the host name under the heading `Resolved Host List`, with each address on its own line. If you omit this option, the IP addresses in `Resolved Host List` are displayed all on one line separated by commas.

-s

Specify this option to display how many seconds it took to resolve the IP addresses from the host name, beside `Time Required`.

host-name

Specify the name of a host on the network.

Notes

- If you specify a logical host name that does not exist, the following message is output and processing stops.

The specified logical host does not exist.

- If you specify the `-h` option more than once, the logical host name in the `-h` option specified last takes effect.
- If you specify multiple host names, the host name specified first takes effect.

Return values

0	Normal end
-1	Invalid option (in Windows)
255	Invalid option (in UNIX)
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
jplhosts           : no entry. extract hostlist is disabled.
Search jplhosts    : 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.

The following shows the command output when the `-v` option and `-s` option are specified.

```
C:\>jp1ping -v -s server1
:
Time Required      : 0.005sec
Resolved Host List : server1 -> server1.hitachi.co.jp
(1) 172.16.0.10
(2) 172.16.0.20
```

```
Check with ping command ---  
:
```

openssl

Function

The `openssl` command is provided by OpenSSL.

Format

For details about the format (options) of the `openssl` command, see the official website of OpenSSL.

Required execution permission

For details about execution permission required for the `openssl` command, see the official website of OpenSSL.

Command directory

OS		Command directory
Windows	32-bit	<i>installation-folder</i> \ssl\32mt\bin
• AIX • Linux	32-bit, multithread (for compatibility)	/opt/jp1base/ssl/32mt/bin
	32-bit, single thread (for compatibility)	/opt/jp1base/ssl/32st/bin
	64-bit, multithread	/opt/jp1base/ssl/64mt/bin
	64-bit, single thread	/opt/jp1base/ssl/64st/bin

Notes

- For the latest information about this command, see the official website of OpenSSL.
- To use this command in Windows, you need to set the `OPENSSL_CONF` environment variable on the console that executes the command. Specify the OpenSSL definition file name by using its full path for the `OPENSSL_CONF` environment variable. JP1/Base provides the OpenSSL definition file in the following folder:

In the 32-bit version of Windows:

```
installation-folder\ssl\32mt\ssl\openssl.cnf
```

In the 64-bit version of Windows:

```
installation-folder\ssl\64mt\ssl\openssl.cnf
```

However, you must not set the `OPENSSL_CONF` environment variable for the user environment variable and system environment variable. Set the `OPENSSL_CONF` environment variable in either of the methods described below. Note that both methods are described on the assumption that the OS is the 32-bit version of Windows. For the 64-bit version of Windows, replace the storage folder of the OpenSSL definition file, for example, as necessary.

- Setting method by creating a batch file

Create a batch file to set the `OPENSSL_CONF` environment variable and execute `openssl.exe`, and then execute the batch file on the console.

The contents of the batch file are as follows:

```
-----  
@echo off  
set OPENSSL_CONF=installation-folder\ssl\32mt\ssl\openssl.cnf  
"installation-folder\ssl\32mt\bin\openssl.exe" %*  
exit /b %ERRORLEVEL%
```

Do not enclose the full path to be set in the `OPENSSL_CONF` environment variable by using double quotation marks ("").

In the following execution example, the batch file name is `ssl.exe.bat`.

```
ssl.exe.bat x509 -text -noout -in jplbasessl.pem
```

- Setting method by executing the `set` command on the console

Execute the `set` command that is used to set the `OPENSSL_CONF` environment variable on the console. An example of executing the `set` command is as follows:

```
set OPENSSL_CONF=C:\Program  
Files (x86)\Hitachi\JP1Base\ssl\32mt\ssl\openssl.cnf
```

Do not enclose the full path to be set in the `OPENSSL_CONF` environment variable by using double quotation marks ("").

After executing the `set` command, execute `openssl.exe`.

Examples

The following shows examples of executing the `openssl` command.

When creating private key `jplbasesslecckey.pem` with the elliptic-curve cipher name `prime256v1` in ECC format:

```
openssl ecparam -genkey -noout -name prime256v1 -out jplbasesslecckey.pem
```

When converting private key `jplbasesslecckey.pem` to private key `jplbasessleccpkcs8key.pem` in PKCS#8 format:

```
openssl pkcs8 -topk8 jplbasesslecckey.pem -out jplbasessleccpkcs8key.pem
```

To create a private key `jplbasesslkey.pem` in RSA format:

```
openssl genrsa 2048 -out jplbasesslkey.pem
```

To create a CSR `jplbase.csr`:

```
openssl req -key jplbasesslkey.pem -out jplbase.csr
```

To check the expiration date of a server certificate `jplbasessl.pem`:

```
openssl x509 -text -noout -in jplbasessl.pem
```

Execution result (excerpts):

```
Validity  
Not Before: Jul 21 01:31:49 2015 GMT  
Not After: Jul 18 01:31:49 2025 GMT
```

`Not Before` indicates the date and time when the server certificate was issued.

`Not After` indicates the expiration date of the server certificate.

16

Definition Files

This chapter describes the JP1/Base definition files and the format and syntax of event filters.

List of definition files

Table 16–1: List of definition files

Function	Definition file name and explanation
Startup control	<i>Start sequence definition file (Windows only)</i> (JP1SVPRM.DAT) Sets the sequence for starting and stopping services.
	<i>Service startup delay time/timer monitoring period definition file (Windows only)</i> (Jp1svprm_wait.dat) Sets the length of time for service startup to be delayed and monitored.
Event service	<i>Event server index file</i> (index) Specifies the directory to be used by the event server.
	<i>Event server settings file</i> (conf) Defines the operating environment for the event services.
	<i>Forwarding settings file</i> (forward) Defines which JP1 events are forwarded and the destination event server.
	<i>API settings file</i> (api) Defines the method for connecting from the application program to the event server and the port to use for the connection.
	<i>Additional extended attribute settings files</i> (recv_add_extattr and send_add_extattr) Sets the conditions of JP1 events to which extended attributes are to be added, and the names and values of the extended attributes.
Event conversion	<i>Action definition file for log file trapping</i> Specifies the conditions for converting log data into JP1 events and the retry settings when monitoring fails.
	<i>Log-file trap startup definition file</i> (jevlog_start.conf) Specifies the log file traps to start or stop when the log-file trap management service (daemon) starts, the jevlogstart command is executed (in a cluster environment), or the jevlogstop command is executed (in a cluster environment).
	<i>Log information definition file</i> (jevlogd.conf) Specifies the maximum size and number of storable log files that are used for log file trapping.
	<i>Action definition file for event log trapping (Windows only)</i> (ntevent.conf) Specifies the conditions for converting event log data into JP1 events and the retry settings for when monitoring fails.
Event service definition information collection and distribution	<i>Distribution definition file</i> Specifies the definition information to distribute and the destination host.
User management	<i>Password definition file (Windows only)</i> Specifies password information for multiple OS users or information-search users.
	<i>User permission level file</i> (JP1_UserLevel) Specifies operating permissions for JP1 resource groups accessed by JP1 users.
	<i>User permission definition file</i> Defines operating permissions for JP1 users or DS groups to access JP1 resource groups.

Function	Definition file name and explanation
	<p><i>Directory server modification file (Windows only)</i> 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.</p> <p><i>Directory server linkage definition file (Windows only) (jplbs_ds_setup.conf)</i> Sets the common definition information in order to specify the directory server, when user authentication is performed by linkage to the directory server.</p> <p><i>User mapping definition file (jplBsUmap.conf)</i> Sets mapping information for multiple JP1 users.</p> <p><i>Password policy definition file (jplbs_passwdpolc.conf)</i> Sets a password policy.</p>
Health check function	<p><i>Health check definition file (jbshc.conf)</i> Specifies how to report an error detected by the health check function and what other hosts to monitor by using the health check function.</p> <p><i>Common definition settings file (health check function)</i> Sets the common definition information to enable the health check function.</p>
Process management	<p><i>JP1/Base parameter definition file (jplbs_param_V7.conf)</i> 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.</p> <p><i>Extended startup process definition file (jplbs_service_0700.conf)</i> Specifies the settings in order to automatically restart a process abnormally terminated.</p>
Communication settings	<p><i>jplhosts definition file (jplhosts)</i> Defines new JP1-specific hosts information (jplhosts information) to be applied to the common definition information.</p> <p><i>jplhosts2 definition file (jplhosts2.conf)</i> Defines new JP1-specific hosts information (jplhosts2 information).</p> <p><i>Host access control definition file (jbsdfts_srv.conf)</i> Sets access permissions to control access attempts from other hosts, for example, when providing information to the IM configuration management functionality of JP1/IM.</p> <p><i>SSL communication definition file</i> Sets whether to enable the communication encryption function and the SSL communication settings in the common definition information.</p> <p><i>Non-SSL communication host configuration file</i> Defines the hosts that perform non-SSL communication in an environment where the communication encryption function is enabled.</p>
Local action function	<p><i>Local action environment variable file</i> Sets the environment variables to execute the command specified by the local action function.</p> <p><i>Local action execution definition file (jbslact.conf)</i> Specifies the commands and execution conditions of the local action function.</p> <p><i>Common definition settings file (local action function)</i> Specifies whether to enable the local action function and sets the log information to the common definition information.</p>
Collection of JP1/Base setup information in a single operation	<p><i>Collection information file</i> Specifies the file names and destinations so that users can collect files with desired names and store them in desired destinations when the jbsparamdump command is used to collect JP1/Base setup information.</p>

Function	Definition file name and explanation
Configuration management functionality	<p><i>Common definition settings file (configuration management functionality)</i> Specifies configuration management functionality settings in the common definition information.</p>
JP1/IM command execution or automated action function.	<p><i>Environment variable file</i> Defines the system hierarchy that is to be managed by JP1/IM.</p>
	<p><i>Host group definition file</i> Defines a group of managed hosts in JP1/IM.</p>

Definition files required for each operational case

This section describes the definition files that must be prepared for each operational case, such as for starting JP1/Base or for using JP1/IM or JP1/AJS. This section also describes the definition files that can be modified to match the operation of a logical host when running JP1/Base in a cluster system.

For starting JP1/Base

The following table lists the definition files that are required to start JP1/Base, and the definition files whose settings must be considered before starting JP1/Base.

Table 16–2: Definition files that must be set before JP1/Base can start

Function	Definition file name	Reference
Setup	Language setting file for JP1/Base (jplbs_env.conf)	3.4.2(1) Setting the language for JP1/Base
Event service	Event server index file (index)	Event server index file in 16. Definition Files
	Event server settings file (conf)	Event server settings file in 16. Definition Files
	API settings file (api)	API settings file in 16. Definition Files
Process management	JP1/Base parameter definition file (jplbs_param_v7.conf)	JP1/Base parameter definition file in 16. Definition Files
	Extended startup process definition file (jplbs_service_0700.conf)	Extended startup process definition file in 16. Definition Files

Note that to enable automatic start and stop by the JP1/Base startup control function, you must also set the following commands:

- Automatic start command (jbs_start)
For details, see [jbs_start \(UNIX only\) in 15. Commands](#).
- Automatic stop command (jbs_stop)
For details, see [jbs_stop \(UNIX only\) in 15. Commands](#).

For using JP1/IM

The following table lists the definition files that must be set on the Manager side in order to use JP1/IM to manage and monitor a system.

Table 16–3: Definition files that must be set on the Manager side to use JP1/IM

Function	Definition file name	Reference
Setup	Language setting file for JP1/IM and JP1/AJS (jplbs_param.conf)	3.4.2(1) Setting the language for JP1/Base
Startup control	Start sequence definition file (JP1SVPRM.DAT)	Start sequence definition file (Windows only) in 16. Definition Files
Event service	Additional extended attribute settings files (recv_add_extattr and send_add_extattr)	Additional extended attribute settings files in 16. Definition Files
Event conversion	Action definition file for event log trapping (ntevent.conf)	Action definition file for event log trapping (Windows only) in 16. Definition Files

Function	Definition file name	Reference
Event service definition information collection and distribution	Distribution definition file	<i>Distribution definition file in 16. Definition Files</i>
User management	User mapping definition file (jplBsUmap.conf)	<i>User mapping definition file in 16. Definition Files</i>
Health check function	Health check definition file (jbshc.conf)	<i>Health check definition file in 16. Definition Files</i>
	Common definition settings file (health check function)	<i>Common definition settings file (health check function) in 16. Definition Files</i>
Communication settings	jplhosts definition file (jplhosts)	<i>jplhosts definition file in 16. Definition Files</i>
	jplhosts2 definition file (jplhosts2.conf)	<i>jplhosts2 definition file in 16. Definition Files</i>
Configuration management functionality	Common definition settings file (configuration management functionality)	<i>Common definition settings file (configuration management functionality) in 16. Definition Files</i>
	Configuration file (jbs_route.conf)	<i>Configuration definition file in 16. Definition Files</i>
JP1/IM command execution or automated action function.	Environment variable file	<i>Environment variable file in 16. Definition Files</i>
	Host group definition file	<i>Host group definition file in 16. Definition Files</i>

The following table lists the definition files that must be set on the Agent side in order to user JP1/IM to manage and monitor a system.

Table 16–4: Definition files that must be set on the Agent side to use JP1/IM

Function	Definition file name	Reference
Setup	Language setting file for JP1/IM and JP1/AJS (jplbs_param.conf)	<i>3.4.2(1) Setting the language for JP1/Base</i>
Event service	Forwarding settings file (forward)	<i>Forwarding settings file in 16. Definition Files</i>
Event conversion	Action definition file for log file trapping	<i>Action definition file for log file trapping in 16. Definition Files</i>
	Log-file trap startup definition file (jevlog_start.conf)	<i>Log-file trap startup definition file in 16. Definition Files</i>
User management	User mapping definition file (jplBsUmap.conf)	<i>User mapping definition file in 16. Definition Files</i>
Health check function	Common definition settings file (health check function)	<i>Common definition settings file (health check function) in 16. Definition Files</i>
Communication settings	jplhosts definition file (jplhosts)	<i>jplhosts definition file in 16. Definition Files</i>
	jplhosts2 definition file (jplhosts2.conf)	<i>jplhosts2 definition file in 16. Definition Files</i>
JP1/IM command execution or automated action function.	Environment variable file	<i>Environment variable file in 16. Definition Files</i>

For using JP1/AJS

The following table lists the definition files that are required in order to use JP1/AJS to manage jobs.

Table 16–5: Definition files that must be set to use JP1/AJS

Function	Definition file name	Reference
Setup	Language setting file for JP1/IM and JP1/AJS (jplbs_param.conf)	<i>3.4.2(1) Setting the language for JP1/Base</i>
Startup control	Start sequence definition file (JP1SVPRM.DAT)	<i>Start sequence definition file (Windows only) in 16. Definition Files</i>
Event service	Forwarding settings file (forward)	<i>Forwarding settings file in 16. Definition Files</i>
	Additional extended attribute settings files (recv_add_extattr and send_add_extattr)	<i>Additional extended attribute settings files in 16. Definition Files</i>
Event conversion	Action definition file for log file trapping	<i>Action definition file for log file trapping in 16. Definition Files</i>
	Action definition file for event log trapping (ntevent.conf)	<i>Action definition file for event log trapping (Windows only) in 16. Definition Files</i>
User management	User mapping definition file (jplBsUmap.conf)	<i>User mapping definition file in 16. Definition Files</i>
Communication settings	jplhosts definition file (jplhosts)	<i>jplhosts definition file in 16. Definition Files</i>
	jplhosts2 definition file (jplhosts2.conf)	<i>jplhosts2 definition file in 16. Definition Files</i>

For using an authentication server

The following table lists the definition files that are required in order to use an authentication server to manage users.

Table 16–6: Definition files that must be set to use an authentication server

Function	Definition file name	Reference
User management	Password definition file	<i>Password definition file (Windows only) in 16. Definition Files</i>
	User permission level file (JP1_UserLevel)	<i>User permission level file in 16. Definition Files</i>
	Directory server modification file	<i>Directory server modification file (Windows only) in 16. Definition Files</i>
	Directory server linkage definition file (jplbs_ds_setup.conf)	<i>Directory server linkage definition file (Windows only) in 16. Definition Files</i>
	Common definition settings file (password save format definition)	<i>3.4.6 Setting the password save format</i>
	Password policy definition file (jplbs_passwdpolc.conf)	<i>Password policy definition file in 16. Definition Files</i>

For using a cluster system

The following table lists the definition files that can be modified to match the operation of a logical host when running JP1/Base in a cluster system.

Table 16–7: Definition files that can be modified to match the operation of a logical host when using a cluster system

Function	Definition file name	Reference
Setup	Language type settings file for JP1/IM and JP1/AJS (jp1bs_param.conf)	<i>3.4.2(1) Setting the language for JP1/Base</i>
Event service	Event server settings file (conf)	<i>Event server settings file in 16. Definition Files</i>
	Forwarding settings file (forward)	<i>Forwarding settings file in 16. Definition Files</i>
	Additional extended attribute settings files (recv_add_extattr and send_add_extattr)	<i>Additional extended attribute settings files in 16. Definition Files</i>
Event conversion	Common definition settings file (extended regular expression definition)	<i>3.4.5 Extending regular expressions to be used</i>
Event service definition information collection and distribution	Distribution definition file (forwarding settings file (jev_forward.conf))	<i>Distribution definition file in 16. Definition Files</i>
User management	Password definition file	<i>Password definition file (Windows only) in 16. Definition Files</i>
	User permission level file (JP1_UserLevel)	<i>User permission level file in 16. Definition Files</i>
	Directory server modification file	<i>Directory server modification file (Windows only) in 16. Definition Files</i>
	Directory server linkage definition file (jp1bs_ds_setup.conf)	<i>Directory server linkage definition file (Windows only) in 16. Definition Files</i>
	User mapping definition file (jp1BsUmap.conf)	<i>User mapping definition file in 16. Definition Files</i>
	Common definition settings file (password save format definition)	<i>3.4.6 Setting the password save format</i>
	Password policy definition file (jp1bs_passwdpolc.conf)	<i>Password policy definition file in 16. Definition Files</i>
Health check function	Health check definition file (jbshc.conf)	<i>Health check definition file in 16. Definition Files</i>
	Common definition settings file (health check function)	<i>Common definition settings file (health check function) in 16. Definition Files</i>
Process management	JP1/Base parameter definition file (jp1bs_param_v7.conf)	<i>JP1/Base parameter definition file in 16. Definition Files</i>
	Extended startup process definition file (jp1bs_service_0700.conf)	<i>Extended startup process definition file in 16. Definition Files</i>
Communication settings	jp1hosts definition file (jp1hosts)	<i>jp1hosts definition file in 16. Definition Files</i>
	jp1hosts2 definition file (jp1hosts2.conf)	<i>jp1hosts2 definition file in 16. Definition Files</i>
	Host access control definition file (jbsdfts_srv.conf)	<i>Host access control definition file in 16. Definition Files</i>
	SSL communication definition file	<i>SSL communication definition file in 16. Definition Files</i>

Function	Definition file name	Reference
	Non-SSL communication host configuration file	<i>Non-SSL communication host configuration file in 16. Definition Files</i>
	Configuration file (jbs_route.conf)	<i>Configuration definition file in 16. Definition Files</i>
	Common definition settings file (definition for restricting connections)	<i>K.3 Definition for restricting connections from unintended hosts</i>
Local action function	Local action environment variable file	<i>Local action environment variable file in 16. Definition Files</i>
	Local action execution definition file (jbslcact.conf)	<i>Local action execution definition file in 16. Definition Files</i>
	Common definition settings file (local action function)	<i>Common definition settings file (local action function) in 16. Definition Files</i>
Operation log data output function	Operation log definition file (jp1bs_base_log_setup.conf)	<i>1.5 Settings for outputting operation logs</i>
Configuration management functionality	Common definition settings file (configuration management functionality)	<i>Common definition settings file (configuration management functionality) in 16. Definition Files</i>

Types of parameters

The parameters in definition files are classified into the following types, depending on the necessity of the parameter. Take these types into account when setting up definition files.

Required parameters:

Parameters that you cannot omit in a definition file and for which you must consider appropriate values when using JP1/Base

Custom parameters:

Parameters that you must specify when using specific functions and for which you must consider values appropriate to the operational requirements for JP1/Base

Note that parameters that belong to neither of the above types also exist. You need to specify these parameters only when special settings are required. For these parameters, unless you are specifying special settings, you do not usually need to change their initial settings.

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`)
- Additional extended attribute settings files (`recv_add_extattr` and `send_add_extattr`)
- Local action execution definition file (`jbslcact.conf`)
- `jevexport` command
- JP1 event acquisition function (`JevGetOpen`)

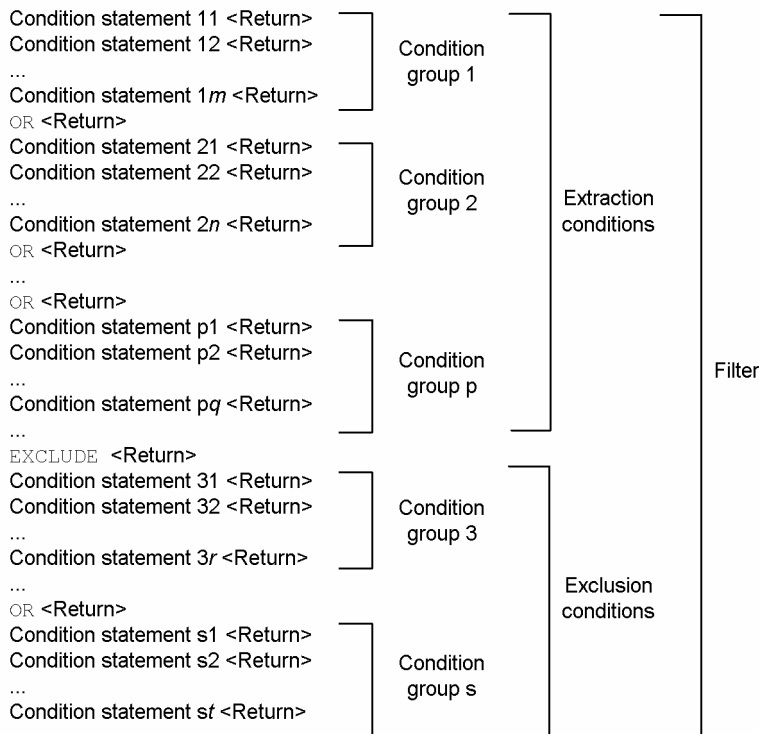
Event filter format

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 16–1: Concept of an event 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.

If the condition group is not defined, then conditions are satisfied unconditionally. However, if the exclusion conditions after `EXCLUDE` are not defined, `EXCLUDE` is ignored.

For the forwarding settings file, undefined extraction conditions are not permitted, and an error occurs if extraction conditions are not defined.

Be aware that if only `OR` is defined for the exclusion conditions or for the extraction conditions of forwarding settings file, or if either of the condition groups before or after `OR` is not defined, it is not considered a formatting mistake and conditions are satisfied unconditionally.

Condition statement format

Write condition statements in the following format:

```
attribute-name Δ comparison-keyword Δ operand-1 Δ operand-2 Δ . . .
```

Δ 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.

Notes

- If a condition statement contains a machine dependent character, the statement cannot be correctly applied.
- In Windows, when you use REGEX as comparison keywords and regular expression is not extended, specify "\n" instead of "%0a" for LF character.

Attribute name

Table 16–8: 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}

Attribute name	Contents	Type and format
B.PROCESSID	Source process ID	Number (0 to 2,147,483,647)
B.TIME	Registered time	Number (0 to 4,294,967,295 = cumulative seconds since UTC 1970-01-01 00:00:00)
B.ARRIVEDTIME	Arrived time	Number (0 to 4,294,967,295 = 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)
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. <i>extended-attribute-name</i> ^{#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 16-9.

#2: For the format of extended attribute names, see [17.1.2 Extended attributes](#).

#3: Character strings are case sensitive.

Comparison keywords

Table 16–9: Comparison keywords in filter condition statements

Comparison keywords	Number of operands	Conditions
IN	1 or more	<p>The attribute value must match one of the operands.</p> <p>When the attribute value is of the string literal type: The operand can be any character string. Example: B.MESSAGE IN KAJP KAVA</p> <p>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. Example: B.REASON IN 1</p> <p>When the attribute value is an event ID: The operand must be a string in the form <i>x:y</i> or <i>x</i> (where <i>x</i> and <i>y</i> are hexadecimals of 1-8 digits). <i>x</i> represents the base code and <i>y</i> represents the extended code of the event ID. Other operands are never matched. Example: B.ID IN 111:0</p>
NOTIN	1 or more	<p>Negation of the IN comparison keyword</p> <p>Example: B.USERNAME NOTIN hitachi</p>

Comparison keywords	Number of operands	Conditions
		<p>Example: B . SEQNO NOTIN 1004959</p> <p>Example: B . ID NOTIN 00003A71</p>
BEGIN	1 or more	<p>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.</p> <p>Example: B . MESSAGE BEGIN KAVA</p>
RANGE	2	<p>The condition statement is satisfied when the attribute name is B . TIME or B . ARRIVEDTIME, and the following conditions are satisfied:</p> <ul style="list-style-type: none"> • The attribute value is a number, or a character string interpreted as a number (0 to 4,294,967,295) • <i>operand-1</i> and <i>operand-2</i> 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 <i>yyyymmddHHMMSS</i> format based on the time zone of the event server operating environment, and <i>operand-1</i> <= <i>attribute value</i> <= <i>operand-2</i>. <p>Example: B . TIME RANGE 20140715000000 20140716000000</p> <p>When the attribute value is a number, specified in an attribute name other than B . TIME or B . ARRIVEDTIME:</p> <p>The condition is satisfied if <i>operand-1</i> and <i>operand-2</i> are interpreted as numbers, and <i>operand-1</i> <= <i>attribute value</i> <= <i>operand-2</i>.</p> <p>Example: B . SEQNO RANGE 1004000 1005000</p> <p>When the attribute value is of string literal type:</p> <p>The condition is satisfied if <i>operand-1</i> <= <i>attribute value</i> <= <i>operand-2</i> when the value is compared in order of its character codes.</p> <p>Example: B . MESSAGE RANGE KAJP1001 KAJP1070</p> <p>When the attribute value is an event ID:</p> <p>If <i>operand-1</i> and <i>operand-2</i> are strings in the form <i>x:y</i> (where <i>x</i> and <i>y</i> are hexadecimals of 1 to 8 digits), the whole interpreted as a 16-digit hexadecimal with <i>y</i> representing the upper 8 digits (extended code) and <i>x</i> representing the lower 8 digits (basic code), the condition is satisfied if <i>operand-1</i> <= <i>attribute value</i> <= <i>operand-2</i>.</p> <p>Example: B . ID RANGE 4780 4790</p> <p>Attribute values of all other types fail the condition.</p>
TRANGE	2	<p>The condition is satisfied if:</p> <ul style="list-style-type: none"> • The attribute value is a number, or a character string interpreted as a number (0 to 4,294,967,295) • <i>operand-1</i> and <i>operand-2</i> 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 <i>yyyymmddHHMMSS</i> format based on the time zone of the event server operating environment, and <i>operand-1</i> <= <i>attribute value</i> <= <i>operand-2</i>. <p>Example: B . TIME TRANGE 20140716010000 20140716013000</p> <p>Attribute values of all other types fail the condition.</p>
DEFINED	0	<p>The condition is satisfied if <i>attribute-name</i> 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 <i>attribute-name</i> represents a basic attribute.</p> <p>Example: E . PRODUCT _NAME DEFINED</p>
NOTDEFINED	0	<p>Negation of the DEFINED comparison keyword</p> <p>Example: E . PRODUCT _NAME NOTDEFINED</p>
SUBSTR	1 or more	<p>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.</p> <p>Example: B . MESSAGE SUBSTR <i>error</i></p>

Comparison keywords	Number of operands	Conditions
NOTSUBSTR	1 or more	Negation of the SUBSTR comparison keyword Example: B.MESSAGE SUBSTR <i>warning</i>
REGEX	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. Example: B.MESSAGE REGEX KAV.[0-9][0-9][0-9][0-9]-E For details on regular expressions, see <i>F. Syntax of Regular Expressions</i> .
WITHIN [#]	2	The condition statement is satisfied when the attribute name is B.TIME or B.ARRIVEDTIME, and the following conditions are satisfied: <ul style="list-style-type: none"> The attribute value is a number, or a character string interpreted as a number (1 to 4,294,967,295) <i>operand-1</i> is M (minutes), H (hours), or D (day). <i>operand-2</i> is a character string that can be handled as a number (unsigned). When <i>operand-1</i> 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 <i>yyyymmddHHMMSS</i> format based on the time zone of the event server operating environment, and (current time - <i>operand-2</i> <= attribute value <= current time). Example: B.TIME WITHIN M 30 Example: B.TIME WITHIN H 12 When <i>operand-1</i> 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 <i>yyyymmddHHMMSS</i> format based on the time zone of the event server operating environment, and 00:00:00 on [today's date - (<i>operand-2</i> - 1)] <= attribute value <= 24:59:59 on today. Example: B.TIME WITHIN D 7

[#]: You can specify this keyword in a filter file used for the `jevexport` command.

Examples of event filter settings

The following are description examples of the IN comparison keyword:

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
```

Select JP1 events whose source user ID is 103.

```
B.USERID IN 103
or
B.USERID RANGE 103 103
```

Select JP1 events whose source event server names are `reysol`.

```
B.SOURCESERVER IN reysol
```

The following are description examples of the BEGIN comparison keyword:

Select JP1 events that issued messages beginning with KAJP or KAVA.

```
B.MESSAGE BEGIN KAJP KAVA
```

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
```

The following are description examples where extended attributes are involved:

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
```

Select JP1 events that have extended attributes with the attribute name TASK_NAME (the attribute value is irrelevant).

```
E.TASK_NAME DEFINED
```

The following is a description example of multiple conditions (AND condition):

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
```

The following is a description example of multiple groups of conditions (OR condition):

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
```

The following is a description example of exclusion condition (EXCLUDE):

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
```

The following is a description example of the TRANGE comparison keyword:

Select JP1 events that occurred on or after June 16, 2002#.

```
B.TIME TRANGE 20020616000000 99999999999999
```

The following are description examples of the WITHIN comparison keyword:

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 20030716010000 20030716013000)
```

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)
```

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)
```

#: 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
```

Parameters by type

Required parameters:

None

Custom parameters:

[ControlValue] section:

- ForcedTerminateExec

[FrontOtherServiceXXX] and [Jp1XXX] sections:

- Name
- ServiceName
- StartCommand
- StopCommand

- Parallel
- Wait
- StopWait

[Command] section:

- ReadyCommand
- StopReadyCommand

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 *15. 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 a value other than YES for this parameter or omit this parameter, JP1/Base will not perform service stop processing at a 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 a value other than YES for this parameter 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 (seconds).

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.
 - Only the services specified for ServiceName= in the [FrontOtherService xxx], [Jp1 xxx], and [OtherService xxx] sections are subject to the definition. The startup sequence for multiple services cannot be controlled.
 - 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 use 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.

- To specify a batch file that contains spaces for the parameters in the sections below, specify `cmd/c "batch-file-name"`. Commands will not execute properly if batch files that contain spaces are specified as they normally are.

[FrontOtherServicexxx], [Jp1xxx], and [OtherServicexxx] sections.

StartCommand parameter

StopCommand parameter

[Command] sections.

ReadyCommand parameter

StopReadyCommand parameter

(example) StopCommand="cmd /c

"D:\Program Files\HITACHI\JP1Base\conf\boot\stop_baseev.bat"

- When specifying a command name and one or more arguments for the parameters in the sections shown below, enclose your specification in quotation marks (" ").

[FrontOtherServiceXXX], [JP1XXX], and [OtherServiceXXX] sections.

StartCommand parameter

StopCommand parameter

[Command] sections.

ReadyCommand parameter

StopReadyCommand parameter

(example) ReadyCommand="D:\Program Files\ABC\start.exe" -

start D:\temp\ABC\conf\start.conf"

Definition examples

```
# 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
```

Parameters by type

Required parameters:

None

Custom parameters:

None

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/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

```
[StartTimeControl]  
DelayTime=60  
SurveillanceTime=600
```


Event server index file

Format

```
server event-server-name directory-name
```

Parameters by type

Required parameters:

- `server`

Custom parameters:

None

File name

`index`

Storage destination directory

In Windows:

```
installation-folder\conf\event\
```

In UNIX:

```
/etc/opt/jplbase/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 and hash mark (#) (code 0x23) 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 an asterisk (*).

- *
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 an environment that supports DNS, 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 [10.1.10 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 16–10: Base directories of the partial paths specified (in Windows)

File name	Directory
Event server settings file or forwarding settings file	<i>installation-folder</i> \conf\event\servers\
Event database	<i>installation-folder</i> \sys\event\servers\
Temporary work files	<i>installation-folder</i> \sys\tmp\event\servers\

Table 16–11: Base directories of the partial paths specified (in UNIX)

File name	Directory
Event server settings file or forwarding settings file	/etc/opt/jplbase/conf/event/servers/
Event database	/var/opt/jplbase/sys/event/servers/
Temporary work files	/var/opt/jplbase/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.
- If there is only one FQDN format event server name in the Event server index file for the JP1/Base physical host and you call the JP1 event acquisition function, add the definition of * (indicating that the event server name runs on local host) as event-server-name. (This works on JP1/Base version 12-10 or later.) Also, the directory name (with underlined) needs to be matched with the existing definition. The use of the product cannot be guaranteed unless the directory name is matched. Also, if the definition is not added, the JP1 event acquisition function fails.

Definition example of the event server index file

```
#-----  
# JP1/Base - Event Server Index  
#-----  
server hostX.d1.hitachi.co.jp default  
server * default
```

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] [auto-forward-off] [suppress-notification-on] [threshold-
suppress-notification-on] [rep-restore]
error-size file-size
trace-size file-size
evtlog-size file-size
fwderr-size file-size
log-keep log-file-count
repetition-noncheck-server { * | event-server-name } ...
restart number-of-restart retry-interval reset time
undisposedids { basic-code | basic-code-basic-code } ...
suppress-notification-interval notification-interval
threshold-suppress-notification-interval notification-interval
```

Parameters by type

Required parameters:

- ports
- forward-limit
- db-size
- remote-server (*event-server-name*, *communication-type*, and *address*)
- options (*remote-receive*, *KAJP1037-hntroff*, *KAJP1037-syslogoff*, *save-rep*, *suppress-notification-on*, and *threshold-suppress-notification-on*)
- undisposedids

Custom parameters:

- client-bind
- users

- eventids
- alt-userid
- buffnum
- include
- remote-server (*port*)
- options (no-sync | sync, v5-unused, conv-off, and auto-forward-off)
- repetition-noncheck-server
- restart
- suppress-notification-interval
- threshold-suppress-notification-interval

File name

conf

Storage destination directory

In Windows:

folder-specified-in-event-server-index-file\

shared-folder\jplbase\event\ (in a cluster system)

The default event server index file (index) is located at *installation-folder*\conf\event\servers\default\.

In UNIX:

directory-specified-in-event-server-index-file/

shared-directory/event/ (in a cluster system)

The default event server index file (index) is located at /etc/opt/jplbase/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 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. When you restart the event service, also restart services for which the event service is a prerequisite.

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 and hash mark (#) (code 0x23) 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.

address

Specify the IP address in one of the following forms. We recommend that you specify `<jplhosts2>`, unless there is a good reason to do otherwise.

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.

- IPv4 addresses

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.

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 must explicitly specify the IP address in the `server` parameter in the API settings file (`api`).

- `<jplhosts2>`

Specify `<jplhosts2>` if you want the event server to communicate using the JP1/Base communication protocol. To communicate using IPv6 addresses, specify `<jplhosts2>` and delete the `client-bind` parameter.

Note:

If you use the IP binding method as the communication protocol, `jplhosts` information or `jplhosts2` information is referenced. If you want to use `jplhosts` information, you must explicitly specify the IP address in the `server` parameter in the API settings file (`api`).

- *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.

If you specify a physical host name in Windows, the host name might not resolve to the intended IP address.

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 `jplimevt` 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 `jplimevtapi` 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. If you specify multiple addresses, events are sent to the address specified first.

To communicate using IPv6 addresses, specify `<jp1hosts2>` in the `ports` parameter and delete the `client-bind` parameter.

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). The default is 0 (no retries are performed). 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.

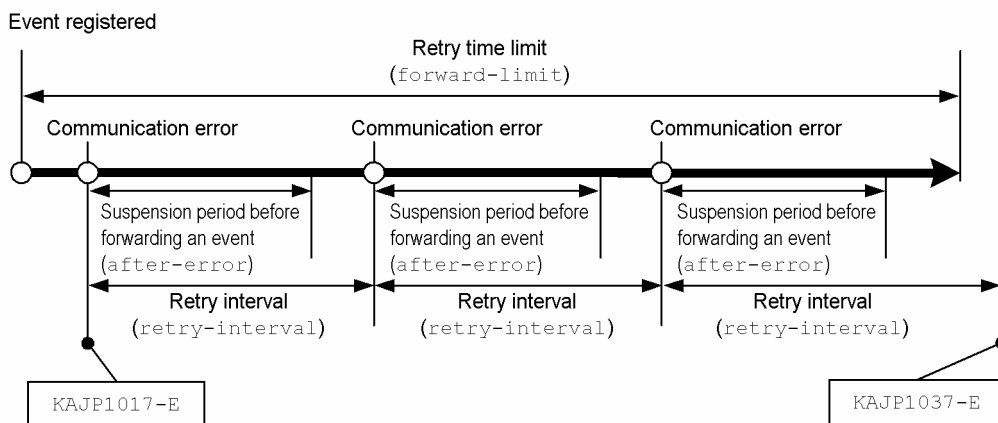
Correlation between the parameters related to retrying

The parameters related to retrying JP1 event transfers are *forward-limit*, *after-error*, and *retry-interval*. By default, if a JP1 event fails to be forwarded, 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 16–2: Correlation between the parameters related to retrying JP1 event transfers



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 relates to functions used to link with products using JP1/SES events in 12-50 and earlier versions of JP1/Base. In 13-00 and later versions of JP1/Base, this setting is no longer required as functions used to link with products using JP1/SES events have been discontinued.

`include ses-conf` *file-name*

This parameter relates to functions used to link with products using JP1/SES events in 12-50 and earlier versions of JP1/Base. In 13-00 and later versions of JP1/Base, this setting is no longer required as functions used to link with products using JP1/SES events have been discontinued.

`include ajs-conf`

This parameter relates to functions used to link with products using JP1/SES events in 12-50 and earlier versions of JP1/Base. In 13-00 and later versions of JP1/Base, this setting is no longer required as functions used to link with products using JP1/SES events have been discontinued.

`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:

$[a \times (b + 64) + (c \times 64) \times d] / 2$ (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 events received from other hosts, and transferred events.

On AIX, make sure that `fsize` for `ulimit` is not exceeded when changing `db-size` in the event server environment setting file (`conf`). Increase `fsize` when setting a value for `db-size` that exceeds `fsize`.

`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:

- *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. If no JP1 event to be forwarded is issued for two seconds or more, the connection will be disconnected.
- *ses*
This parameter relates to functions used to link with products using JP1/SES events in 12-50 and earlier versions of JP1/Base. In 13-00 and later versions of JP1/Base, this setting is no longer required as functions used to link with products using JP1/SES events have been discontinued.
- *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, however, that we recommend that you specify *close* rather than *keep-alive* because the following note applies.

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.

address

Specify the IP address in one of the following formats. We recommend that you specify *<jp1hosts2>*, unless there is a good reason to do otherwise.

- *IP-address*
Specify numbers separated by periods (example: 172.16.50.50).
- *<jp1hosts2>*
Specify *<jp1hosts2>* if you want the event server to communicate using the JP1/Base communication protocol. Also specify *<jp1hosts2>* if you want to communicate using IPv6 addresses. *jp1hosts* information or *jp1hosts2* information is referenced when the IP address of the destination host is resolved.
- *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`] [`auto-forward-off`] [`suppress-notification-on`] [`threshold-suppress-notification-on`] [`rep-restore`]

Specify option flags. You can specify the parameter and a flag on different lines.

`no-sync` | `sync`

Specifying `no-sync` flag (not recommended):

This setting is performance-centric, and is retained for compatibility reasons. The `no-sync` flag allows the system to buffer JP1 events that are 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. Do not specify this flag unless there is a special reason to do so.

Specifying `sync` flag (recommended in a cluster environment):

This setting is reliability-centric and ensures that a JP1 event is written to disk each time the event is issued.

Specifying the `sync` flag ensures that the JP1 events are acquired even 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. Note that, if a delay occurs while the events are written to disk, there might be a significant delay in acquiring JP1 events from a program such as JP1/IM - Manager. At this time, the event database might be switched before JP1 events are obtained, causing those JP1 events to be lost. Therefore, if you specify the `sync` flag, make sure that the number of JP1 events that occur on the system does not exceed the registration performance. Carry out investigations in advance as the registration performance varies depending on the environment.

Omitting the flag (recommended in a non-cluster environment):

This is the default operation, in which performance and reliability are balanced. The system buffers the events and writes them to disk every 10 seconds.

`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 relates to functions used to link with products using JP1/SES events in 12-50 and earlier versions of JP1/Base. In 13-00 and later versions of JP1/Base, this setting is no longer required as functions used to link with products using JP1/SES events have been discontinued.

`v5-unused`

12-50 and earlier versions of JP1/Base suppress the use of all functions provided to ensure compatibility with JP1/SES and JP1/AJS, products available before version 5. In 13-00 and later versions of JP1/Base, this setting is no longer required as functions used to link with products using JP1/SES events have been discontinued. Further, this flag will be treated as being specified even if it is omitted.

`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 $32 + \text{total number of the source event servers} \times 288$ bytes. For details on the duplication prevention table, see [2.3.2 Event database](#).

When you specify the `save-rep` option for the first time in a given environment, execute the `jevdbmkrep` command after changing the setting and before starting the event service.

auto-forward-off

Disables the function that forwards the events listed below, even if they do not match the filter conditions. If you specify this flag, like other events, these events will only be forwarded if they match the filter conditions.

- Event reporting of JP1/Base startup (00004724)
- Event reporting of JP1/Base shutdown (00004725)
- Event reporting of a threshold-based suppression (00003D0B)
- Event reporting of a stop of a threshold-based suppression (00003D0C)
- Event reporting of a stop of all threshold-based suppressions (00003D0D)
- Event reporting of the continuation of threshold-based suppressions (00003D0E)

suppress-notification-on

Issues a JP1 event reporting that the event forwarding state activated by the `jevagtfw` command is continued. Specify this flag on the event server for the manager host on which the `jevagtfw` command was executed.

threshold-suppress-notification-on

Issues a JP1 event, reporting to the manager that the event forwarding state activated by a threshold is continued. Specify this flag on the event server for the agent host on which the threshold-based suppression of event-forwarding was set up.

rep-restore

Automatically repairs the event database duplication prevention table if it is corrupted when the event service starts. This parameter is invalid if the `save-rep` flag is not specified.

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 (`fwder. *`).

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.

$a + (b \times c) \times d$ (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 1,000,000.

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.

$a + (b + c + d) \times e$ (bytes)

a: Basic part (1 KB)

b: Amount of output log data necessary to register one event \times Number of events registered per day

c: Amount of output log data necessary to acquire one event \times Number of events acquired per day

d: Amount of output log data necessary to transfer one event \times 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 16–12: 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`). If you set the communication type to `keep-alive`, the amount of log data will be smaller. However, make an estimate on the assumption that the communication type is set to `close`.

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.

$\text{Number-of-events-acquired}^{\#1} \times \text{number-of-events-registered-in-event-database} + \text{number-of-events-registered-per-day}^{\#2}$

#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 (`imevtterr.*`). When a file exceeds the specified size, it is overwritten from the beginning. Specify a number from 65536 to 2147483647 (bytes). The default is 1,000,000.

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.

$$a + (b + c + d) \times e \text{ (bytes)}$$

a: Basic part (1 KB)

b: Amount of log output necessary to register one event \times Number of events registered per day

c: Amount of log output necessary to acquire one event \times Number of events acquired per day

d: Amount of log output necessary to transfer one event \times 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 16–13: 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. 300	Approx. 700	Approx. 400

#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.

$$\text{Number-of-events-acquired}^{\#1} \times \text{number-of-events-registered-in-event-database} + \text{number-of-events-registered-per-day}^{\#2}$$

#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 1,000,000.

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.

$$\text{Number-of-event-transfer-failure-to-store} \times (150 + \text{length-of-event-server-name} + \text{length-of-destination-event-server-name})$$

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, event service trace log files and event service transfer error log file 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.

`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 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

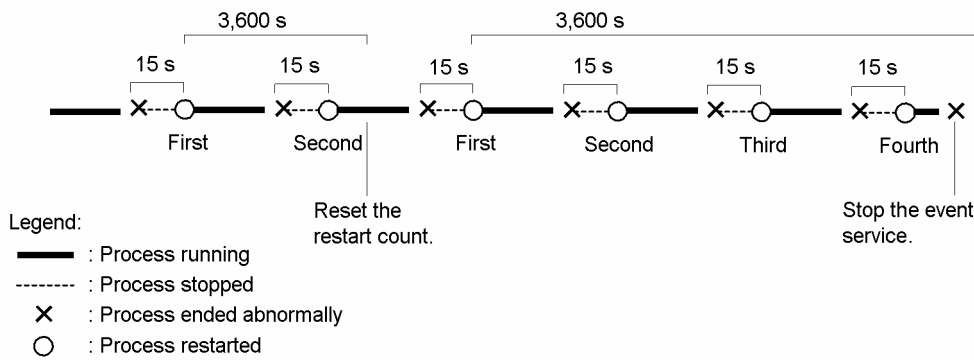
Specify how long an event service process will wait to restart after it ends abnormally. If a restart fails, the process will wait until the specified interval elapsed before another attempt is made to restart the service. The recommended value is 15 (seconds). Specify a number from 0 to 3600. If you 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 16–3: 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 16–14: 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 (DBMgr)	Manages the event database.
	jevservice (SESEmu)	This is the SES compatibility function. This does not start in JP1/Base 13-00 and later versions.
	jevservice (EvtAPI)	Accepts registration or acquisition requests of JP1 events.
	jevservice (FwdRcv)	Receives the forwarded JP1 events.
	jevservice (FwdMgr)	Forwards JP1 events.

`undisposedids { basic-code | basic-code-basic-code } ...`

Specify the event IDs that are excluded from discarding of the received events for event forwarding suppression. Even when the setting to discard events received from an agent is enabled, the JP1 events with the event IDs specified here are received from the agent.

You can specify multiple values for this parameter. If you omit this parameter, all the JP1 events that are subject to discard are discarded.

Note that log file trapping and event log trapping might generate a large volume of events, depending on the condition. Therefore, in the initial settings, JP1 events whose event IDs are 3A71 (JP1 events converted by event log trapping) are discarded. This means that event IDs (2000-3A70, 3A72-7FFF7FFF) other than 3A71 are specified for the `undisposedids` parameter.

basic-code

Specify the event ID basic code in a hexadecimal value of 1 to 8 digits.

basic-code–basic-code

Specify the range for event ID basic codes, each in a hexadecimal value of 1 to 8 digits separated by a hyphen.

suppress-notification-interval notification-interval

Specify an interval for issuing a JP1 event reporting that event forwarding activated by the `jevagtfw` command is continued. Specify a decimal value from 60 to 86,400 (seconds). If you omit this parameter, 3,600 (seconds) is assumed.

This parameter is enabled only when the `suppress-notification-on` flag is specified in the `options` parameter.

threshold-suppress-notification-interval notification-interval

Specify an interval for issuing a JP1 event reporting that event forwarding activated by a threshold is continued. Specify a decimal value from 60 to 86,400 (seconds). If you omit this parameter, 3,600 (seconds) is assumed.

This parameter is enabled only when the `threshold-suppress-notification-on` flag is specified in the `options` parameter.

Note

In JP1/Base 11-00 or later, you no longer need to specify the `log-level` parameter. However, if you do specify it, JP1/Base operation is not adversely affected.

Definition examples

```
# For port number, use jplimevt and jplimevtapi defined
# in the system services file.
ports 0.0.0.0 jplimevt jplimevtapi
# Programs executed only in user root and adm can acquire
# JP1 events.
users root adm
# Programs compatible to JP1/Base can issue and acquire all
# JP1 events.
eventids *
# 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
# 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 are connected by phone
# line dial ups, so the connections will be frequently interrupted.
remote-server host1 keep-alive
remote-server host2 keep-alive
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

```
# Forwarding setting block
to-upper
event-filter
end-to
:
or
to event-server-name
event-filter
end-to
:
# Forwarding-suppression setting block
suppress identifier unit-time threshold check-count [destination]
event-filter
end-suppress
```

Parameters by type

Required parameters:

None

Custom parameters:

- to-upper or to
- suppress

File name

forward

Storage destination directory

In Windows:

folder-specified-in-event-server-index-file\

shared-folder\jplbase\event\ (in a cluster system)

The default event server index file (*index*) is located at *installation-folder*\conf\event\servers\default\.

In UNIX:

directory-specified-in-event-server-index-file\

shared-directory/event/ (in a cluster system)

The default event server index file (*index*) is located at /etc/opt/jplbase/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. This file also specifies conditions for the suppression of event-forwarding by using a threshold.

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 *15. Commands*. When you restart the event service, you also need to restart services for which the event service is a prerequisite.

Definition details

The following conventions apply to entries in the forwarding settings file (`forward`).

- The forwarding settings file (`forward`) is a text file in which each line is no more than 1,023 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 and hash mark (#) (code 0x23) at the start of a line.
- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- Letters are case sensitive.

Definition details of the forwarding setting block:

`to-upper`

If the forwarding setting block is defined in the `to-upper` format, JP1 events are forwarded to a server at a higher level in the hierarchy defined in JP1/IM - Manager. A forwarding setting block is from `to-upper` to `end-to`.

`to event-server-name`

If the forwarding setting block is defined in the `to` format, you can specify the destination event server name. *event-server-name* is case sensitive. You need to specify a remote event server name that is specified in the event server settings file (`conf`) in the local server. A forwarding setting block is from `to` to `end-to`.

event-filter

Specify the conditions for the target JP1 events. For details on the description format of an event filter, see *Event filter syntax*.

Definition details of the forwarding-suppression setting block:

`suppress identifier unit-time threshold check-count [destination]`

Specify conditions used for the threshold-based suppression of event-forwarding. A forwarding-suppression setting block (a condition for the suppression of event-forwarding) is from `suppress` to `end-suppress`.

Note that JP1 events that are subject to evaluation on each condition for the suppression of event-forwarding (`suppress`) are the JP1 events being filtered by the forwarding setting (`to`) that also have a matching destination and event filter specified.

identifier

Specify a name for each condition for the suppression of event-forwarding with alphanumeric characters from 1 to 12 bytes. This information is used to identify a condition for the suppression of event-forwarding when starting or stopping the event forwarding suppression. Specify a unique character string within the event server.

unit-time

Specify a time duration for which the threshold is evaluated in seconds from 1 to 3,600. The duration specified here will be used as a unit for *check-count*.

threshold

Specify a number of JP1 events that determines an occurrence of large numbers of events with a value from 1 to 72,000. If the number of JP1 events that match suppression conditions (both destination and event filter) per *unit-time* is equal to or more than this threshold, the system determines that a large number of events has occurred.

check-count

Specify the number of *unit-times* used to determine an occurrence or convergence of large numbers of events with a value from 1 to 3,000. If the number of events consecutively exceeds the threshold during a unit time the number of times specified here, the system determines that a large number of events has occurred, and starts event forwarding suppression. Similarly, if the number of events consecutively falls below the threshold during a unit time the number of times specified here, the system determines that a large number of events have converged, and stops the event forwarding suppression.

Note that you can set a different number for starting and stopping the event forwarding suppression by separating the values by a comma (,). For example, specifying 3, 5 defines an occurrence condition of 3 times, and a convergence condition of 5 times. Specifying 3 defines occurrence and convergence conditions of 3 times.

[*destination*]

Specify the name of a destination event server subject to the conditions for the suppression of event-forwarding. JP1 events that are forwarded to the event servers specified here are evaluated by the conditions for suppression of event-forwarding.

As a destination, specify one of the items below. If the destination is not specified, all destination event servers are subject to the conditions for suppression of event-forwarding.

- *
All the destination event servers are subject to the conditions for suppression of event-forwarding.
- *event-server-name*
Specify the destination event server name that is subject to the condition for suppression of event-forwarding. *event-server-name* is case sensitive.
- (upper)
The higher-level host defined in the configuration definition information is assumed as the destination event server name. If no higher-level host is defined in the configuration definition information, the corresponding condition for suppression of event-forwarding becomes invalid.

event-filter

The same as the forwarding setting block.

Notes

- In a forwarding settings file (`forward`), you can specify multiple forwarding setting blocks and forwarding-suppression setting blocks.
- If you specify an event filter that contains Japanese characters in a forwarding settings file (`forward`), the encoding must be consistent with the locale settings (such as the `LANG` environment variable) specified for the system when the event service started. The JP1 event will not be forwarded unless this condition is met.
- 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.

- If multiple forwarding setting blocks (`to` to `end-to`) that have the same destination assigned are specified, forwarding processing is done in the order of event filter specified in each block. 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.
- If multiple forwarding-suppression setting blocks (`suppress` to `end-suppress`) are specified, conditions for the suppression of event-forwarding (`suppress`) are evaluated in the following manner, to determine whether forwarding suppression is started or stopped:
 - Evaluation is performed on all the conditions for suppression of event-forwarding (`suppress`) that have a matching destination.
 - A JP1 event that was evaluated as a suppression target by one or more conditions for suppression of event-forwarding (`suppress`) that have the matching destination, is suppressed from being forwarded. Forwarding of those events is restarted when the JP1 event is evaluated as a non-suppression target by all the conditions for suppression of event-forwarding (`suppress`) that have the matching destination.

Definition examples

Definition examples of a forwarding setting block

Shown below are examples of forwarding settings for forwarding JP1 events in the following system configuration.

Table 16–15: Example of forwarding settings

Host name	Role in configuration
<code>jp1-svs1</code>	Integrated manager
<code>jp1-svs2</code>	Submanager
<code>jp1-sva1</code>	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/NT_LOGTRAP`

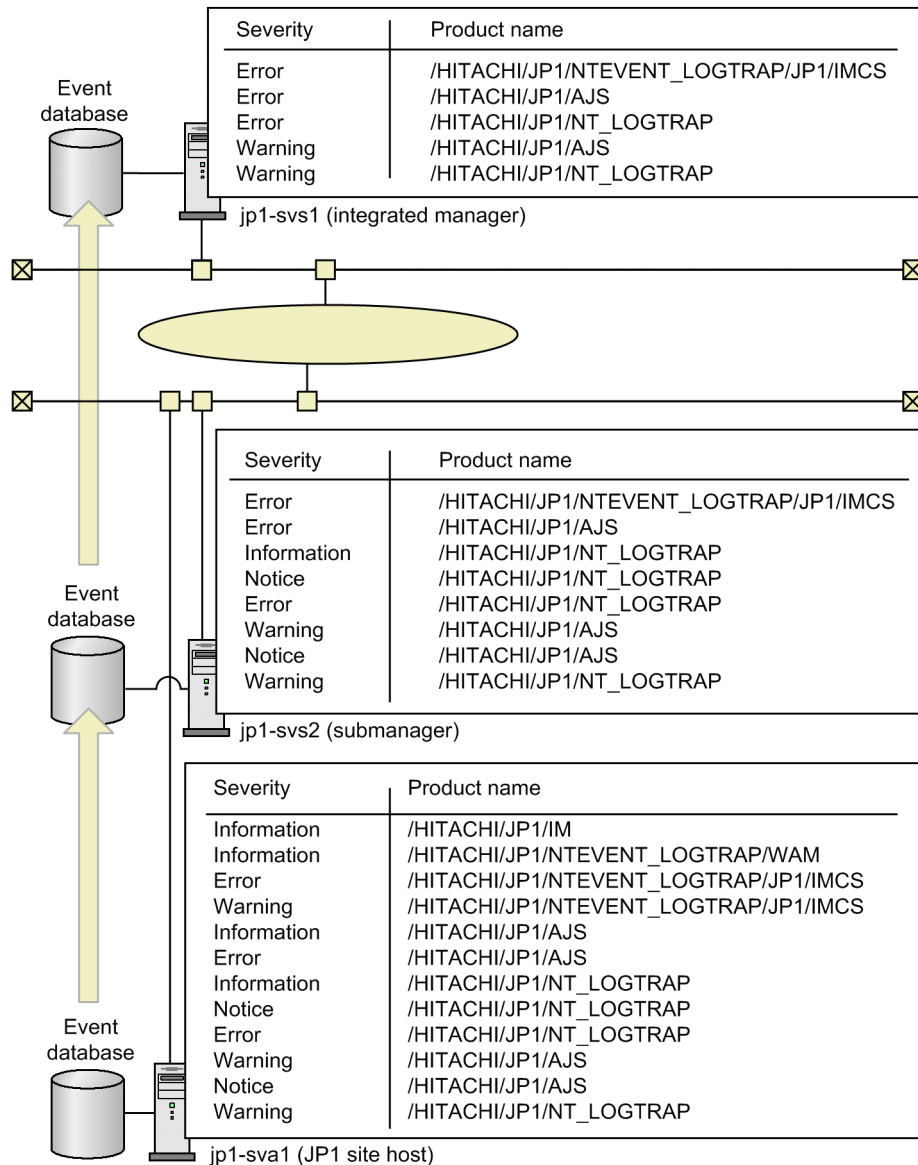
JP1 events are forwarded from `jp1-svs2` to `jp1-svs1` if any one of the following is true:

- `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/NT_LOGTRAP`, and `SEVERITY` is set to `Warning`

The flow of JP1 event transfers is shown below.

Figure 16–4: Definition examples and flow of JP1 event transfers

Flow of JP1 event transfers



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/NT_LOGTRAP
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/NT_LOGTRAP
end-to

```

Definition examples of a forwarding-suppression setting block (condition for suppression of event-forwarding)

Shown below is a definition example of a forwarding-suppression setting block (condition for suppression of event-forwarding) matching the following conditions:

- Monitored log file name of the JP1 event is /tmp/logfile1.
- Destination of the JP1 event is a higher-level host defined in the configuration definition information.
- Event forwarding is suppressed when, regarding 60 seconds as a unit time, a condition in which 900 or more JP1 events occur in a 60-second unit time occurs consecutively five times. The forwarding suppression is stopped when a condition in which 899 or less JP1 events occur in a 60-second unit time occurs consecutively five times.

```

suppress log1 60 900 5 (upper)
E.OBJECT_NAME IN /tmp/logfile1
end-suppress

```


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
bridge name-of-host-that-uses-bridge
```

Parameters by type

Required parameters:

- `server` (*event-server-name* and *communication-type*)

Custom parameters:

- `server` (*address* and *port*)
- `client`
- `bridge`

File name

`api`

Storage destination directory

In Windows:

`installation-folder\conf\event\`

In UNIX:

`/etc/opt/jplbase/conf/event/`

Description

Defines the method for connecting from the application program to the event server and the port to use for the connection. Under normal circumstances, there is no need to change the default settings. 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 changed the `ports` parameter of the event server settings file (`conf`) from the default value, change the API settings file accordingly.

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 and hash mark (#) (code 0x23) 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 of the connection destination in one of the formats shown 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. We recommend that you specify `<jp1hosts2>`, unless there is a good reason to do otherwise.

- *IP-address*

Specify numbers separated by periods (example: 172.16.50.50).

- `<jp1hosts2>`

Specify `<jp1hosts2>` if you want application programs to connect to the event server using the JP1/Base communication protocol, and if you want to communicate using IPv6 addresses. When the IP address of the destination host is resolved, `jp1hosts2` information is referenced, but `jp1hosts` information is not referenced.

- *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) 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 `jplimevtapi`.

- *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 `client` parameter is omitted and the OS automatically assigns the source connection address. 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 IP address in one of the following formats:

- IPv4 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.
- IPv6 address
Specify hexadecimal numbers separated by colons (example: `2001:db8::28`). 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 1,000,000. Log information is output only when the API is loaded and when an error occurs.

bridge *name-of-host-that-uses-bridge*

Specify the name of the local event server that is up and running when SSL communication is enabled for event services and the JP1 event acquisition function (JevGetEvent) is being used on a remote host. For details on the JP1 event acquisition function (JevGetEvent), see the manual *JP1/Base Function Reference*.

Specify this parameter only if the event service of a physical host is not up and running. If you omit this parameter, it is assumed that a physical host is set.

Additional extended attribute settings files

Format

```
# comment
add
filter
event-filter
end-filter
E.extended-attribute-name attribute-value
...
end-add [exit]
...
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File names

`recv_add_extattr` (file for transfer reception)

`send_add_extattr` (file for event registration)

`add_extattr.model` (model file for an additional extended attribute settings file)

Storage destination directory

For Windows:

folder-specified-in-event-server-index-file\

shared-folder\jplbase\event\ (in a cluster configuration)

In the initial settings of the event server index file (`index`), the specified folder is *installation-folder*\conf\event\servers\default\.

For UNIX:

directory-specified-in-event-server-index-file/

shared-directory/event/ (in a cluster configuration)

In the initial settings of the event server index file (`index`), the specified directory is `/etc/opt/jplbase/conf/event/servers/default/`.

Description

Additional extended attribute settings files are used to set the conditions for JP1 events to which extended attributes are to be added, and to set the names and values of the extended attributes. There are additional extended attribute settings files for transfer reception (`recv_add_extattr`) and for event registration (`send_add_extattr`).

The settings in additional extended attribute settings files are required to define through referring to the *Recommended definition method* below. In the initial state, these files are not provided.

If the additional extended attribute settings file for transfer reception (`recv_add_extattr`) is created, extended attributes are added based on the definitions in the file when transferred JP1 events are received. If the additional extended attribute settings file for event registration (`send_add_extattr`) is created, extended attributes are added based on the definitions in the file when JP1 events are registered in the event database.

The following table describes the JP1 events to which extended attributes are added by a definition file.

Definition file	Target JP1 events
Additional extended attribute settings file for transfer reception (<code>recv_add_extattr</code>)	<ul style="list-style-type: none"> Events issued to the local event server from another event server[#] (JP1 event registered reason: 3) Events transferred to the local event server from another event server according to the specified transfer settings (JP1 event registered reason: 4)
Additional extended attribute settings file for event registration (<code>send_add_extattr</code>)	<ul style="list-style-type: none"> Events issued from the local event server to the local event server (JP1 event registered reason: 1) Events issued from the local event server to another event server[#] (JP1 event registered reason: 2)

[#]: If the `jevsend` or `jevsendd` command is executed with the `-d` option, which specifies the destination event server, the definitions take effect in the following files: the additional extended attribute settings file for event registration on the registration source and the additional extended attribute settings file for transfer reception on the send destination.

Application of settings

The settings are applied when the event service is started or restarted, or when an additional extended attribute settings file is reloaded by the `jevextreload` command. For details about this command, see *jevextreload* in 15. *Commands*. Note that if the event service is restarted, all services that use the event service must also be restarted.

Definition details

The following conventions apply to entries in the additional extended attribute settings files (`recv_add_extattr` and `send_add_extattr`):

- These files are text files in which each line can have 1,023 or fewer 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 and hash mark (#) (code 0x23) at the start of a line.
- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- Letters are case sensitive.

`add ... end-add [exit]`

A sequence of entries from `add` to `end-add` is an attribute addition setting block, which contains a filter block and extended attribute specification. You can specify multiple attribute addition setting blocks. If multiple attribute addition setting blocks are specified, JP1/Base processes them in the order they are specified (the first block is processed first). Note that the keyword `end-add` can be followed by the keyword `exit`. If the condition specified in an attribute addition setting block is satisfied and `exit` is specified in that block, processing of the subsequent attribute addition setting blocks is skipped. If the filter block is omitted, JP1/Base assumes that the condition is satisfied. You cannot omit both the filter block and extended attribute specification.

`filter ... end-filter`

A sequence of entries from `filter` to `end-filter` is a filter block, which specifies a definition for filtering JP1 events to which an extended attribute is to be added. The following shows the format of a filter block:

```
filter
event-filter
end-filter
```

If the filter block is omitted, all JP1 events are subject to conversion. For the event filter, you can also specify an exclusion condition. For details about the writing format of an event filter, see *Event filter syntax*.

E. *extended-attribute-name attribute-value*

This is an extended-attribute specification parameter. Specify the name and value of an extended attribute (user-specific information) to be added to JP1 events. By specifying multiple extended-attribute specification parameters, you can add multiple extended attributes to one JP1 event. Each JP1 event can have a maximum of 100 extended attributes (calculated as the combined total of the common information and user-specific information). However, the total length of extended attribute values that can be defined for JP1 events cannot exceed 10,000 bytes. You can add extended attributes as long as these limitations are not exceeded. Note that in one attribute addition setting block, you cannot specify the same extended attribute name more than once.

You can omit the extended-attribute specification parameters. To exclude specific JP1 events from being the targets for addition of extended attributes, define the condition that identifies the target JP1 events in the event filter, and then specify `exit` after `end-add` of the attribute addition setting block.



Note

If you specify a multi-byte character as an extended attribute value, when the JP1 event character code is C, the specified character becomes garbled. If you want to specify a multi-byte character, add character code (B.CODESET) conditions to the event conditions, with different character strings defined for the character code 8859_1 (C) and other character codes.

E. *extended-attribute-name*

Following the string E., specify the name of the extended attribute to be added. The name can be a maximum of 32 bytes. You can use uppercase letters, numeric characters, and underscores (_). Note that the first 7 bytes of each extended attribute name is fixed to JP1ADD_. That is, you can specify a maximum of 25 bytes after E.JP1ADD_.

attribute-value

Specify the value of the extended attribute whose name is specified by the E. *extended-attribute-name* entry. You can enter a character string that is from 1 to 255 bytes. For the value of an extended attribute, you cannot specify a blank (null string). You cannot specify a value that includes line breaks, either.

Notes

- If an extended attribute is added to a JP1 event that already has that extended attribute, the extended attribute is updated with the new value.
- When a JP1 event with extended attributes added is transferred, the added extended attributes are also transferred together.

Recommended definition method

- Though attribute addition can be done on an agent host, we recommend that you do it on the manager host in order for integrated management of events to add attributes.
- The processing for adding extended attributes affects the event registration performance in proportion to the number of attribute addition setting blocks multiplied by the number of events. Therefore, we recommend that you consider the following notes when defining the additional extended attribute settings file. Note that in the processing for adding extended attributes, attribute addition setting blocks are processed from the beginning for each JP1 event.

- When JP1/IM - Manager is running in a hierarchical structure of three or more levels, configure the additional extended attribute settings file in the site manager or sub manager.
- You can reduce the processing for adding extended attributes by defining an attribute addition setting block at the beginning that includes a condition for JP1 events to which extended attributes are not added.
- Conditions for all the JP1 events and for JP1 events that occur frequently must be defined as higher levels in the additional extended attribute settings file.
- Specify `exit` after `end-add` in each attribute addition setting block, except when adding a different attribute for each condition to a single JP1 event.
- The total number of attribute addition setting blocks defined in the additional extended attribute settings file must be no more than 2,500. Although an error does not occur even if you define 2,500 or more attribute addition setting blocks, the event registration performance might degrade and operation might be affected.

Definition examples

The following is an example definition that adds the name of a business group to which the agent host belongs as an extended attribute to JP1 events received on the manager side.

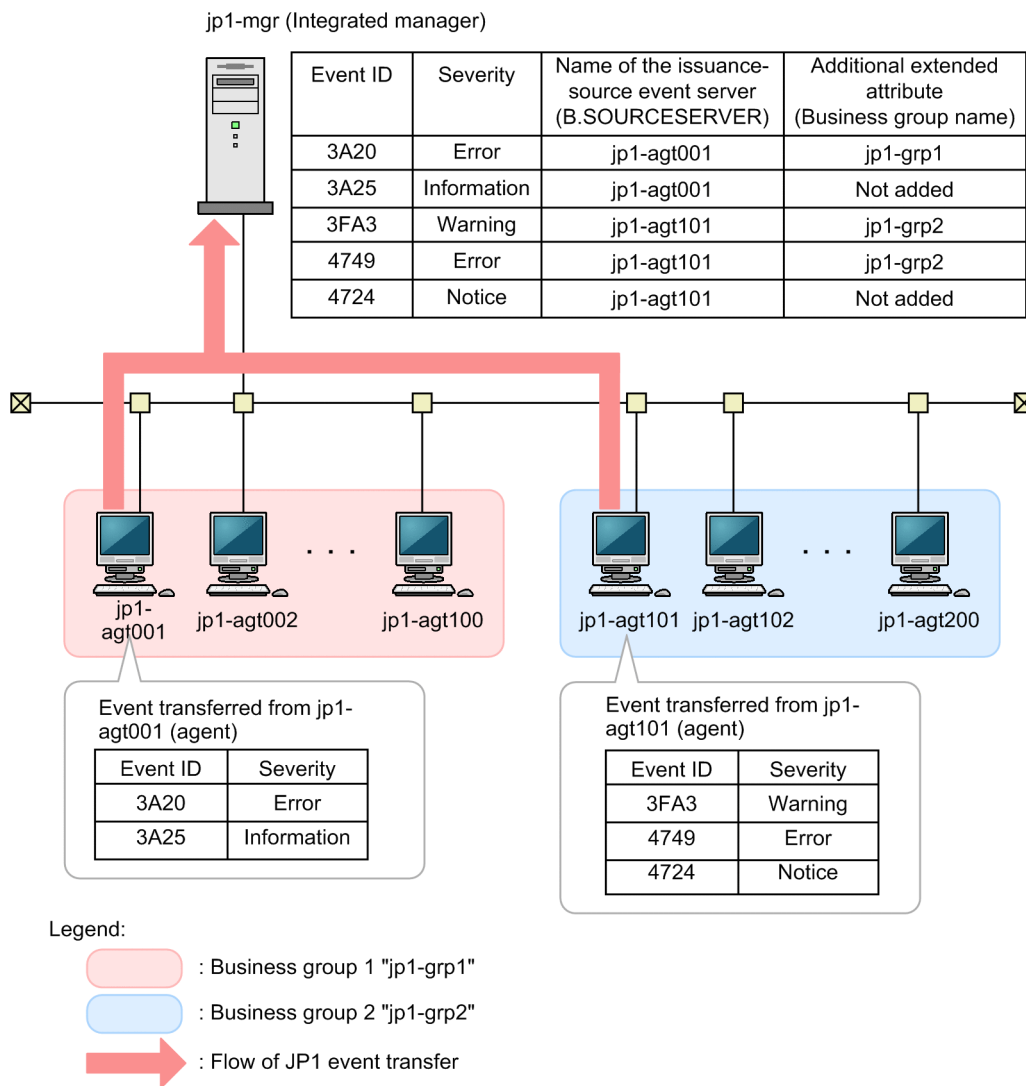
Table 16–16: System configuration for the definition example

Host name	Host type
<code>jp1-mgr</code>	Integrated manager
<code>jp1-agt001 to jp1-agt100</code>	Agent (business group 1)
<code>jp1-agt101 to jp1-agt200</code>	Agent (business group 2)

Conditions for adding the extended attribute for the integrated manager (`jp1-mgr`)

- The extended attribute is added to JP1 events whose severity (`SEVERITY`) is not `Information` and `Notice`.
- Business group name `jp1-grp1` is added to JP1 events transferred from agents (`jp1-agt001 to jp1-agt100`) in business group 1 as extended attribute `JP1ADD_GROUPNAME`.
- Business group name `jp1-grp2` is added to JP1 events transferred from agents (`jp1-agt101 to jp1-agt200`) in business group 2 as extended attribute `JP1ADD_GROUPNAME`.

Figure 16–5: Flow of JP1 event transfer in the definition example



Example definition of the additional extended attribute settings file (`recv_add_extattr`) for transfer reception in the integrated manager (`jp1-mgr`)

```
# Exclude JP1 events whose severity is Information or Notice from the target of extended attribute addition.
add
filter
E.SEVERITY IN Information Notice
end-filter
end-add exit
# Add business group name jp1-grp1 as extended attribute JP1ADD_GROUPNAME
# to JP1 events transferred from agents (jp1-agt001 to jp1-agt100).
add
filter
B.SOURCESERVER RANGE jp1-agt001 jp1-agt100
end-filter
E.JP1ADD_GROUPNAME jp1-grp1
end-add exit
# Add business group name jp1-grp2 as extended attribute JP1ADD_GROUPNAME
# to JP1 events transferred from agents (jp1-agt101 to jp1-agt200).
add
filter
```

```
B.SOURCESERVER RANGE jp1-agt101 jp1-agt200
end-filter
E.JP1ADD_GROUPNAME jp1-grp2
end-add exit
```

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 }
upd-output-event={ 0 | 1 }
FILETYPE={ SEQ | SEQ2 | SEQ3 | WRAP1 | WRAP2 | HTRACE | UPD }
RECTYPE={VAR { '\n ' | 'end-of-line-character' | 'end-of-line-symbol'} | FIX record-length }
HEADLINE=number-of-header-lines
HEADSIZE=header-size
unset-extattr={ [TRAP_ID,TRAP_NAME] | [TRAP_ID] | [TRAP_NAME] }
MARKSTR=[!] "regular-expressions"
[!] "regular-expression"#
ACTDEF=[{EXIT}][<severity>] event-ID [!] "regular-expressions"
[!] "regular-expression"#
```

#: The regular expression *n* represents multiple specifications.

Parameters by type

Required parameters:

None

Custom parameters:

- FILETYPE
- RECTYPE
- HEADLINE
- HEADSIZE
- MARKSTR
- ACTDEF

File name

Any

`jevlog.conf.model` (model file of an action definition file for log file trapping)

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. Create an action definition file for log file trapping from the model file (`jevlog.conf.model`) in the following directory.

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 *15. 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 Δ Δ =SEQ  
ACTDEF=0 Δ message
```

where Δ 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. The default is 3.

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.

`upd-output-event={ 0 | 1 }`

Specify whether to output JP1 events (00003A25 or 00003A26) when a monitoring target log file is detected, in situations where `UPD` is specified as the output file type for log files. If you omit this parameter, 0 is assumed. For output formats other than `UPD`, this parameter is ignored.

`0`

Specify this value if you do not want the log file trapping function to output the JP1 events.

`1`

Specify this value to output the JP1 events.

`FILETYPE={ SEQ | SEQ2 | SEQ3 | WRAP1 | WRAP2 | HTRACE | UPD }`

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.

SEQ3 (Windows only)

Specify SEQ3 when, in Windows, the system deletes the file when it reaches a certain size and then writes log data to a new file with the same name as the deleted file.

If you use a remote-monitoring log file trap with the IM configuration management functionality to monitor a log file of this type on a remote host, you can monitor the file as a SEQ2 file. However, when using a log file trap on a local machine, this type of log file needs to be monitored as SEQ3.

Notes

- When monitoring the log file as SEQ3, if the system deletes a log file that contains data written since the last time the file was read, the log file trap cannot read that data. Caution is required when monitoring files that are deleted immediately after reaching the maximum size.
- If you monitor SEQ2 files as SEQ3, when the log file is renamed and if the log file contains data written since the last time the file was read, the log file trap cannot read that data. This problem does not occur when the file is monitored as SEQ2.

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.

Notes

- 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.
- When a wrap-around file has any of the following characteristics, conversion to JP1 events might be delayed or not happen at all:
 - The file wraps around repeatedly within a short time.
 - Log data exceeding the file's capacity is output all at once.
 - The same log data is output multiple times.

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).

Apply WRAP2 when monitoring integrated trace log files.

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.
- Messages output to the integrated trace log might corrupt if the messages from multiple processes are output at the same time. To monitor a specific message, enable the exclusive control functionality for the integrated trace log. For details on exclusive control, see *hntr2conf* in 15. *Commands*.

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.

In Windows, the monitoring of Unicode files is supported for logs that are output in UTF-8 character encoding. Logs output in UTF-16 character encoding cannot be monitored.

UPD

Specify `UPD` to ensure you always monitor the latest iteration of a log file.

To monitor the latest log files, use a wildcard pattern when you specify the file name of the monitored log file in the `jevlogstart` command. When the log file trap starts, the log-file trap management service (or daemon) monitors the most recently updated log file of those that match the wildcard pattern. As long as the trap is active, the service (or daemon) continuously switches its monitoring target to the newest file that matches the wildcard pattern.

The log file trap can keep track of a maximum of 1,000 log files matching the wildcard pattern. Files whose full path and file name exceed 256 bytes are not monitored.

`UPD` files must be sequential files (a log file that is written to continuously over time).

`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.

If you monitor Unicode files in Windows and BOM exists at the beginning of the files, specify the header size excluding the BOM size (3 bytes for UTF-8 and 2 bytes for UTF-16).

```
unset-extattr={ [TRAP_ID,TRAP_NAME] | [TRAP_ID] | [TRAP_NAME] }
```

In JP1/Base Version 10-50 or later, extended attributes of the JP1 events output by the log file trap include the monitor ID (JP1_TRAP_ID) and monitoring target name (JP1_TRAP_NAME). Specify these parameters if you do not want to output these attribute values. If you omit these parameters, the monitor ID and the monitoring target name are output.

TRAP_ID, TRAP_NAME

Specify this parameter if you do not want to output neither the monitor ID nor the monitoring target name.

TRAP_ID

Specify this parameter if you do not want to output the monitor ID.

TRAP_NAME

Specify this parameter if you do not want to output the monitoring target name.

```
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)
  Δ Δ Δ Δ Δ "MARK"
  Δ : 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. After all values of this parameter are evaluated, ACTDEF is evaluated. 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.

You can specify multiple instances of this parameter. The number of instances that can be specified is not limited. If you specify multiple instances, they are combined with the OR condition. All log messages that match the specification of any instance are converted into JP1 events.

The regular expression specified in this parameter targets only a certain length of an input log message from the beginning. The length is specified by the -m option of the jevlogstart command.

For details about extending regular expressions, see [3.4.5 Extending regular expressions to be used](#).

If you want to monitor Unicode files in Windows, you must specify extended regular expressions. In this case, extended regular expressions are used for filtering regardless of whether the regular expression extension setting ("REGEXP"="EXTENDED") is specified. For details about how to specify extended regular expressions, see [F.2 Extended regular expressions that can be used when regular expressions are extended](#).

You cannot omit this parameter.

{EXIT}

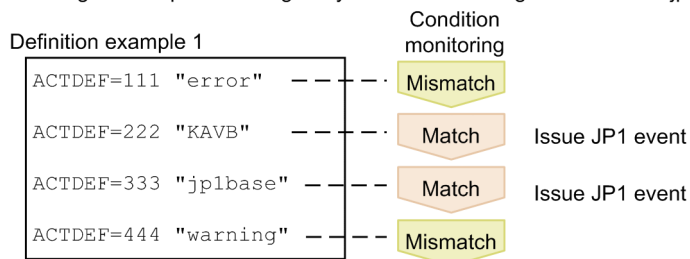
This parameter applies when specifying multiple ACTDEF parameters. Specify {EXIT} to halt monitoring log data as soon as data matching the condition tagged with {EXIT} has been detected.

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.

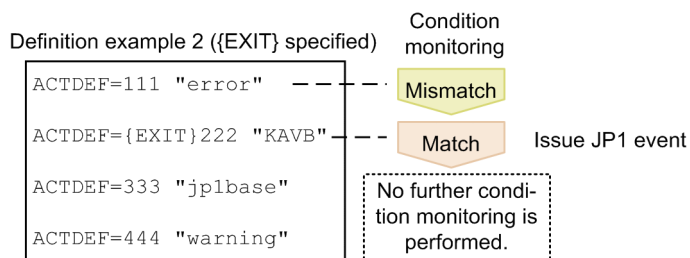
The following figure shows how the processing differs according to whether {EXIT} is specified.

Figure 16–6: Example of specifying an action definition file for log file trapping

Processing when a particular log entry contains the strings "KAVB" and "jplbase".



A JP1 event is issued every time the log entry matches a condition.



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.

```
ACTDEF=00000333 "jp1base"(line feed)
  Δ Δ Δ Δ Δ "error"
  Δ : Space
```

Notes

- In JP1/Base 11-00 or later, the default of the `retry-times` parameter has been changed from 0 to 3.
- 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 or 00003A27) are issued if the log file reaches a set size and is swapped over after log file trapping starts. For details on these JP1 events, see [17.3.1\(16\) Details about event ID 00003A22](#) and [17.3.1\(19\) Details about event ID 00003A27](#).

If you receive one of these JP1 events (00003A22 or 00003A27), check the status of the log file indicated in the error message, and make sure that the correct output format (`FILETYPE`) is specified in the action definition file for log file trapping.

If you continue with the incorrect format specified, the file will not be monitored correctly. Define the correct data output format and restart the log file trap.

The table below describes the possible causes of these JP1 events (00003A22 or 00003A27) for each output format.

Table 16–17: 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The log file size is smaller than before being re-created under a different name.
SEQ3 (Windows only)	<ul style="list-style-type: none"> The log file size is smaller than before.
WRAP1	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The log file is deleted. The log file is deleted and re-created with the same name.#
HTRACE	<ul style="list-style-type: none"> The log file is deleted. The log file is deleted and re-created with the same name.
UPD	<ul style="list-style-type: none"> 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.

#: The log file might be a SEQ2 file. Check the file format specified in the action definition file for log file trapping.

Definition examples

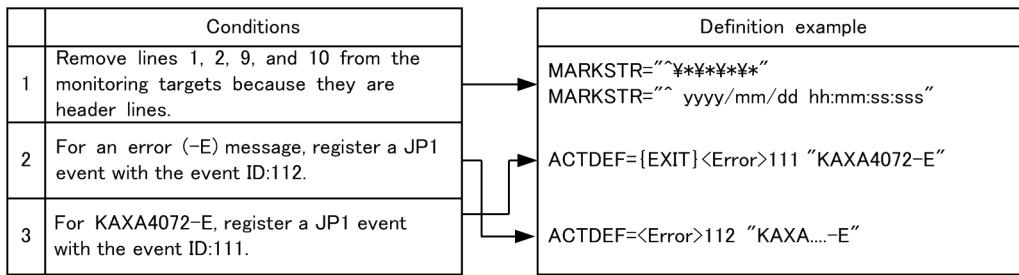
- Examples of defining MARKSTR and ACTDEF parameters

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:

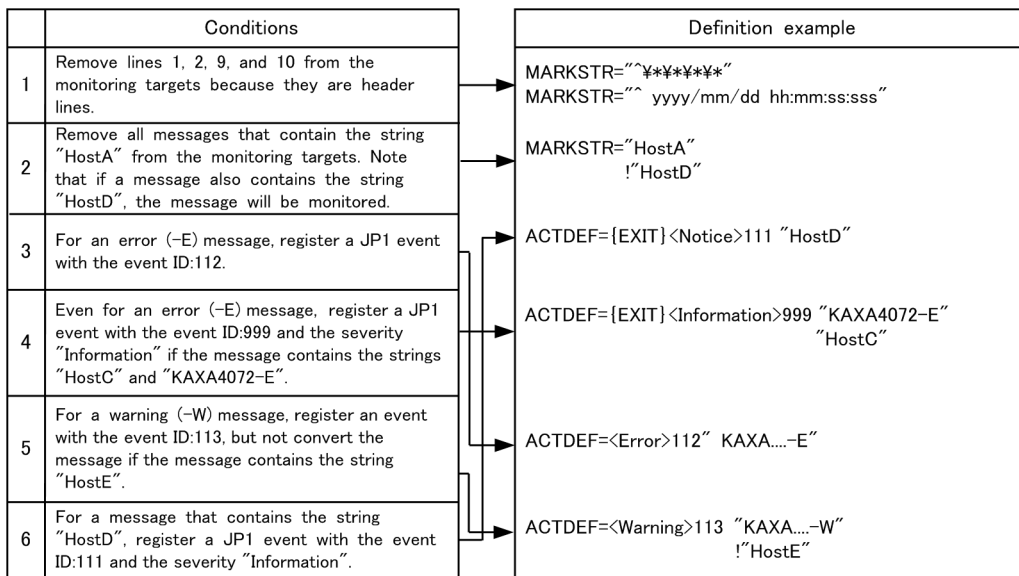
The left part of the following figure lists conditions for log file trapping, and the right part provides examples of defining the action definition file for log file trapping.



● Conditions 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 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		Definition example
1	The log file type is a sequential file.	FILETYPE=SEQ
2	The record length is variable and there is \n at the end of the line.	RECTYPE =VAR '\n'
3	Three lines from the top are the header lines.	HEADLINE=3
4	Remove a record that contains the strings "====" and "MARK" from the monitoring targets.	MARKSTR ="====" "MARK"
5	Remove a record that contains the string "info" but does not contain the string "jp1base" from the monitoring targets.	MARKSTR ="info" !"jp1base"
6	Convert a record that contains the string "message" to a JP1 event with the event ID:0.	ACTDEF =0 "message"
7	Convert a record that contains the strings "jp1base" and "KAVA" to a JP1 event with the event ID:00000111:00000000.	ACTDEF =00000111:00000000 "jp1base" "KAVA"
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.	ACTDEF =222 "jp1base" !"warning"
9	Convert a record that contains the string "abnomal" to a JP1 event with the event ID:0001222:00000000, and perform no further monitoring.	ACTDEF={EXIT}1222 "abnomal"
10	Convert a record that contains the strings "jp1base" and "error" to a JP1 event with the event ID:00000333:00000000.	ACTDEF =00000333 "jp1base" "error"

Log-file trap startup definition file

Format

```
START_OPT=[ {SKIP} ] [<startup-LANG>] monitored-name :jevlogstart-command-options
:
START_OPT_CLS=[ (cluster-ID) ] [<startup-LANG>] monitored-name :jevlogstart-command-options
:
```

Parameters by type

Required parameters:

None

Custom parameters:

- START_OPT
- START_OPT_CLS

File name

jevlog_start.conf

Storage destination directory

In Windows:

installation-folder\conf\event\

In UNIX:

/etc/opt/jp1base/conf/event/

Description

A log-file trap startup definition file specifies the log file traps to be started and stopped when any of the following occurs:

- The log-file trap management service (daemon) is started
- The `jevlogstart` command is executed (in a cluster environment)
- The `jevlogstop` command is executed (in a cluster environment)

A log-file trap startup definition file is not provided by default. Users can create the file, or the file can be created as definition information (part of a profile) by IM configuration management.

For each log file trap started by a log-file trap startup definition file, a startup record (KAVA3661-I) and startup results (KAVA3662-I) are output to the log-file trap startup execution results log. If a parameter is specified incorrectly, a warning message is output and the parameter is ignored.

Log-file trap startup execution results log data is output to the following files:

In Windows:

installation-folder\log\jevlog_start\jevlog_start{1|2|3}.log

In UNIX:

/var/opt/jp1base/log/jevlog_start/jevlog_start{1|2|3}.log

When a log file trap is started up by using a startup definition file for log file traps, a timeout period applies.

If the `jevlogstart` command does not finish within the timeout period, processing of the executed `jevlogstart` command continues, but the startup of the log file trap is interrupted. The command will move on to start up the next definition.

Reference note

Establishing a connection to an event service upon startup of a log file trap might take time, causing a timeout.

If a timeout occurs, the result of executing the `jevlogstart` command is not output to the "Message" value of the KAVA3662-I message, so you cannot tell whether the startup ended in failure. The log file trap might have stopped due to a failure in connecting to the event service.

It is recommended that you configure the settings to retry connections to event services.

Application of settings

The settings are applied when:

- The log-file trap management service (daemon) starts
- The `jevlogstart` command (cluster environment only) is executed.

When you execute the `jevlogstop` command (cluster environment only), the log-file trap management service (daemon) stops the log file traps based on the contents of the log-file trap startup definition file read by the `jevlogstart` command.

Definition details

The following conventions apply to the contents of the log-file trap startup definition file (`jevlog_start.conf`):

- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- Define one parameter per line.
- Start writing from column 1.
- Link parameters and their values with equal signs. You can enter spaces between the parameter and equal sign, but not between the equal sign and the value.
- You cannot write a comment between a value (or the last of multiple values) and the subsequent linefeed character. Spaces are allowed.

`START_OPT=[{ SKIP }] [<startup-LANG>] monitored-name:jevlogstart-command-options`

Specify the log file traps to start when the log-file trap management service (daemon) starts, and the startup options for each log file trap.

You can specify this parameter and the `START_OPT_CLS` parameter a maximum of 200 times in total. If the `START_OPT` parameter and the `START_OPT_CLS` parameter appear more than 200 times in total, the 201st and subsequent occurrences are ignored.

The log-file trap management service (daemon) does not start or stop the log file traps specified in this parameter when you execute the `jevlogstart` (cluster environment only) or `jevlogstop` (cluster environment only) command.

`{ SKIP }`

Specify this option to skip startup of log file trapping by the `START_OPT` parameter. Specify `SKIP` in uppercase letters enclosed in curly brackets (`{ }`).

If `{ SKIP }` is omitted, log file trapping is started.

This option is updated when log file trapping is started or stopped by the profile management function of IM Configuration Management. This option is deleted from the definition when log file trapping is started and is added to the definition when log file trapping is stopped.

`START_OPT_CLS=[(cluster-ID)] [<startup-LANG>] monitored-name:jevlogstart-command-options`

Specify the log file traps to start when you execute the `jevlogstart` (cluster system only) command and stop when you execute the `jevlogstop` (cluster system only) command, and the startup options for the log file traps. Specify this parameter to collectively start and stop log file traps in the event of a failover in an environment where log files are being monitored on a shared disk in a cluster environment.

You can specify this parameter and the `START_OPT` parameter a maximum of 200 times in total. If the `START_OPT` parameter and the `START_OPT_CLS` parameter appear more than 200 times in total, the 201st and subsequent occurrences are ignored.

The log-file trap management service (daemon) does not start or stop the log file traps specified in this parameter when it starts.

<startup-LANG>

In UNIX, specify the value of the `LANG` environment variable at execution of the `jevlogstart` command in angle brackets (< >). For details about the values that can be specified, see *Table 3-5 Encodings and LANG environment variable values in UNIX* in *3.4.2 Setting the language (for UNIX)*.

If you omit the value of the `LANG` environment variable, the assumed encoding is the encoding set in the `LANG` environment variable used when the log file trap management daemon is started.

In Windows, this parameter has no effect and will be ignored.

monitored-name

Specify the monitor name of the log file trap. The character string preceding the colon (:) is interpreted as the monitor name.

Monitor names must be no more than 30 bytes long, and can contain alphanumeric characters, hyphens, and underscores. Names must start with an alphanumeric character, and are case sensitive.

Do not specify the same monitor name more than once.

jevlogstart-command-options

Specify the options of the `jevlogstart` command. When the log-file management service (daemon) starts or the `jevlogstart` (cluster system only) command is executed, the system generates a `jevlogstart` command line from the contents of this parameter and *monitored-name*, and uses it to start the log file trap.

For details on the options you can specify, see *jevlogstart* in *15. Commands*.

Only for Windows, there is a limit on the maximum number of specified characters. The maximum number is calculated as follows:

$16 + \text{Length of } monitored\text{-name in bytes} + \text{Length of the options of the } jevlogstart \text{ command in bytes} \leq 4,096 \text{ bytes}$

When JP1/Base is linked with IM configuration management, make sure that you specify the name of an action definition file for log file trapping (`-f` option) for *jevlogstart-command-options*.

The monitoring target of the log file trap will be the value specified in *monitored-name* of the `START_OPT` or `START_OPT_CLS` parameter, so the `-a` option is ignored if specified.

If you specify the `-cluster` option for the `jevlogstart` (cluster system only) command, the parameter is invalid and the definition is ignored.

The current directory of the `jevlogstart` command is as follows:

In Windows:

installation-folder\COMMAND

In UNIXL

/opt/jp1base/command

If you specify a relative path in a command option, it is interpreted relative to this location.

(*cluster-ID*)

Specify the cluster ID in parentheses. The cluster ID is an ID number that identifies a cluster system. In an environment with multiple cluster systems, users can assign any number they choose in the range from 0 to 99.

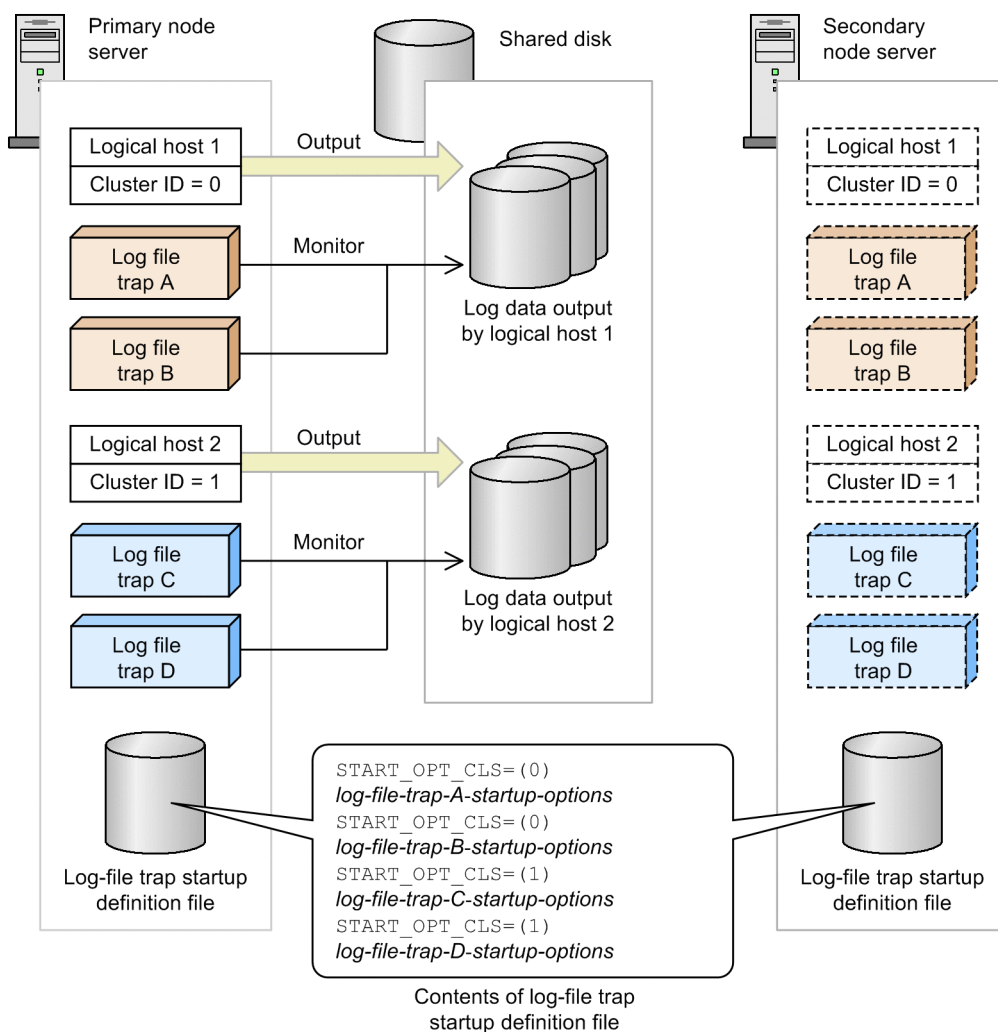
As the cluster ID, specify a decimal value in the range from 0 to 99. The default is 0.

Defining log file trapping in an environment with multiple cluster systems

In environments with multiple cluster systems, choose a cluster ID for each logical host, and define the log file traps to be started and stopped on each of these hosts when a failover occurs.

The following figure shows how to configure log file trapping in an environment with multiple cluster systems.

Figure 16–7: Configuration example for environment with multiple cluster systems



In this example, the cluster ID of logical host 1 is 0. The log data output by logical host 1 is monitored by log file trap A and log file trap B. Thus, in the log-file trap startup definition file, define startup options for log file traps A and B for cluster ID 0.

Similarly, define startup options for log file traps C and D as the log file traps for cluster ID 1.

In the cluster software, register the following commands for execution at failover of logical host 1 and logical host 2:

At failover of logical host 1:

- `jevlogstart -cluster 0`
- `jevlogstop -cluster 0`

At failover of logical host 2:

- `jevlogstart -cluster 1`
- `jevlogstop -cluster 1`

With these commands registered in this manner, the system starts and ends log file traps A and B when logical host 1 fails over, and starts and ends log file traps C and D when logical host 2 fails over.

For details on the commands you can register with the cluster software, see *jevlogstart (cluster environment only)* and *jevlogstop (cluster environment only)* in 15. *Commands*.

Definition examples

```
#Specify log file traps to start when service (daemon) starts.
START_OPT=<ja_JP.eucJP>KANSI1:-f /etc/~/jevlog.conf /fil/aaa.log
:
#Specify log file traps to start when jevlogstart -cluster [cluster-ID] is i
ssued.
#Specify log file traps to stop when jevlogstop -cluster [cluster-ID] is iss
ued.
START_OPT_CLS=(1)<ja_JP.eucJP>KANSI2:-f /etc/~/jevlog.conf /share/aaa.log
:
```

Log information definition file

Format

```
log-keep number-of-log-files
log-size file-size
```

Parameters by type

Required parameters:

None

Custom parameters:

None

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 the file does not exist, the default number of log files and default file size apply. Create and modify the log information definition file (jevlogd.conf), if necessary.

Application of settings

Start the log-file trap management service (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 a definition contains an error, the default applies.
- 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. 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. The default is 1,000,000 (bytes).

Log information is output when the log-file trap management service (or daemon) starts and when an error occurs.

Definition examples

```
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
matching-level [0 | 1]
filter-check-level [0 | 1]
ext-attr-option extended-attribute-name
unicode-trap [0 | 1]
# filter
filter log-type [id=event-ID] [trap-name=trap-name]
condition-statement-1
condition-statement-2
:
condition-statement-n
end-filter
```

Parameters by type

Required parameters:

None

Custom parameters:

- matching-level
- filter-check-level
- unicode-trap
- filter
- id
- trap-name

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 retry settings when monitoring fails.

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 `jveltreload` command. For details on the `jveltreload` command, see [jveltreload \(Windows only\)](#) in *15. 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. The default is 3.

`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.

`matching-level [0|1]`

Specify the comparison level for the event log and definitions when the log entry explanation cannot be read because, for example, you specified a `message` attribute in the filter condition but the message 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.

`ext-attr-option extended-attribute-name`

Specify this option to create additional extended attributes other than A0 to A6, PLATFORM, and PPNNAME.

You can add multiple extended attributes by separating the attribute names with single-byte spaces. The attributes can be specified in any order.

The following table lists the extended attributes you can specify:

Extended attribute	Meaning
A7	Windows logging level
A8	Windows log keywords
A9	Windows log opcode
OS_VERSION	Windows version number

If you omit this parameter, the event service does not create these extended attributes when it converts JP1 events. The following shows an example in which all four extended attributes are created:

```
ext-attr-option A7 A8 A9 OS_VERSION
```

unicode-trap [0 | 1]

Specify the matching method for event log trapping.

Although the Windows event log is output in the Unicode format, JP1/Base itself does not support Unicode. Therefore, if the event log contains Unicode-specific environment-dependent characters, mismatches in event log trap regular expressions might occur or garbled event log data might be registered in the JP1 event. This parameter causes the event log trapping function to use a Unicode search-based matching method, to prevent mismatches in regular expressions and garbled event log data.

If you specify 0, the matching method for event log trapping is based on the Windows system locale. Because the event log is converted to a character code supported by JP1/Base before matching, mismatches in event log trap regular expressions might occur or garbled event log data might be registered in the JP1 event. Also, the default code set is used when JP1 events are registered.

If you specify 1, the matching method for event log trapping is based on a Unicode search. Because the event log data are matched in its original Unicode-format characters, the event log data can be registered in a JP1 event without garbling. Also, UTF-8 is used as the code set when JP1 events are registered. Extended regular expressions are applied as the regular expressions used for condition statements in event filters.

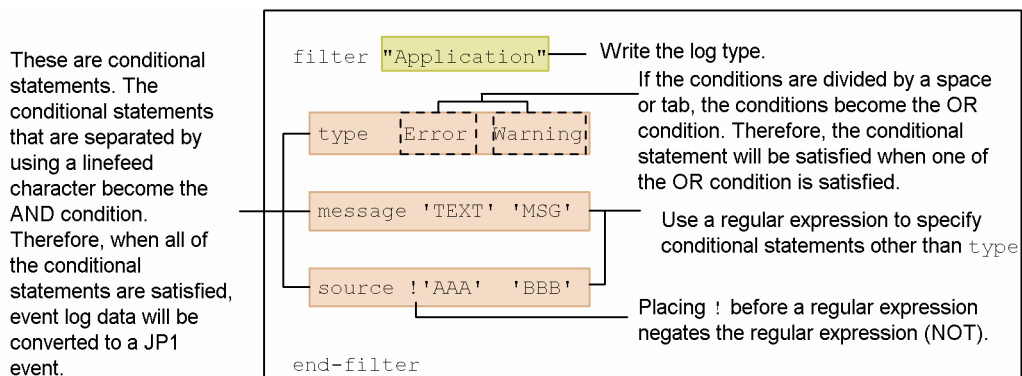
If you omit this parameter, the value 0 is used.

Note that the value set for this parameter cannot be changed by reloading (`jeventreload` command). If you change the value set for this parameter, restart the event log trapping service.

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 define multiple filters in the file, the system parses them in the order they are defined (from the top down), and parsing stops when the first valid filter is parsed. You must specify at least one filter condition. The following figure shows the syntax conventions of a filter.

Figure 16–8: Filter syntax conventions (action definition file for event log trapping)



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. Note that the same log type can be specified for multiple filters.

The following shows the log types that can be specified:

- Windows logs^{#1, #2}

- "Application"
- "Security"
- "System"
- "Setup"
- Application and service logs
 - "DNS Server"
 - "Directory Service"
 - "File Replication Service"
 - "DFS Replication"^{#3}
 - "Internet Explorer"
 - "Key Management Service"
 - "HardwareEvents" and others^{#4}

#1

You cannot specify "Forwarded Events" output to a Windows log.

#2

The event service cannot properly convert an event log entry transferred to an application or system event log from a remote machine. To monitor event log data generated on a remote machine, use an event log trap on the machine that generated the event.

#3

You cannot specify Japanese characters.

#4

Use the following procedure to check the log types you can specify in a filter. Log types that do not meet the criteria are invalid.

1. At the MS-DOS command prompt, execute the `wevtutil` command and review the list of log types registered in the system.

An example of the command line is as follows:

```
>wevtutil el
```

2. For each log type listed in step 1, check whether the log is enabled and the log type.

An example of the command line is as follows:

```
>wevtutil gl Application
```

```
name: Application
```

```
enabled: true
```

```
type: Admin
```

```
:
```

You can specify a log type in a filter if both of the following conditions are met:

```
- enabled is true
```

```
- type is Admin or Operational
```

[id=event-ID]

Specify the event ID to be assigned when a JP1 event is registered on the event server. Each event ID consists of high-order 4 bytes (basic code) and low-order 4 bytes (extended code) separated by a colon (:). The basic and extended

codes are written with hexadecimal values. You can omit the extended code. When you omit it, you can also omit a colon (:). If omitted, 0 is assumed. For both basic and extended codes, if the specified value has eight or fewer digits, 0s are prefixed. Specify values that users can specify. That is, specify values in the range from 0:0 to 1FFF:0 and the range from 7FFF8000:0 to 7FFFFFFF:0. For the extended code, you must specify 0.

The following shows three examples of an event ID. The representations in these examples have the same meaning.

```
id=0000011A:00000000
id=11A:0
id=11A
```

Do not insert a space or tab between `id=` and an event ID. Conversely, insert a space between `log-type` and `trap-name=trap-name`. You can specify the same event ID for multiple filters. If you omit this parameter, 00003A71 is assumed as the event ID.

[`trap-name=trap-name`]

Specify the trap name that is used to identify the filter through which the JP1 event was converted (from an event log message) and registered. Specify a trap name of no more than 30 bytes. You can use alphanumeric characters, hyphens (-), and underscores (_). The trap name must begin with an alphanumeric character. Uppercase and lowercase are distinguished.

Do not insert a space or tab between `trap-name=` and `trap-name`. You can specify the same trap name for multiple filters. If you omit this parameter, no extended attributes are created when the JP1 event is converted. This parameter is not specified in the action definition file for event log trapping in the initial state.

Condition statement format

In *condition-statement*, specify an attribute name (shown in the table below) and the corresponding item that is displayed in the **General** tab of the Event Viewer properties.

Table 16–18: Attribute names that can be specified in filter condition statements

Attribute name	Meaning
<code>type</code>	Specify log types. Specify the level displayed in the Event Viewer properties, by referring to <i>Table 16-19 Log types specifiable in type and the corresponding JP1 event severity</i> . In Windows Vista or later, specify the level displayed in the Event Viewer properties, referring to <i>Table 16-12 Log types specifiable in type and the corresponding JP1 event severity</i> . Audit_success and Audit_failure are displayed in Keyword in the Event Viewer properties.
<code>source</code>	Specify the source information displayed in the Event Viewer properties. If information is different, change the specified information to the source information.
<code>category#</code>	Specify the category information displayed in the Event Viewer properties.
<code>id</code>	Specify the event ID information displayed in the Event Viewer properties.
<code>user</code>	Specify the user name displayed in the Event Viewer properties.
<code>message#</code>	Specify the message text displayed in the Event Viewer properties.
<code>computer</code>	Specify the computer name displayed in the Event Viewer properties.
<code>level#</code>	Specify the level displayed in the Event Viewer properties.
<code>keyword#</code>	Specify the keyword displayed in the Event Viewer properties.

Attribute name	Meaning
opcode#	Specify the opcode displayed in the Event Viewer properties.

#

- 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 a message 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.
- If the event service fails to convert the level, keyword, or opcode, the associated numerical value is registered in brackets, in the same manner as a failed category conversion.
- The event log trapping function cannot trap the following message because it is output by the event viewer:
For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.
- Event Viewer might not display the string `Microsoft-Windows-` prefixed to source names in the event log, due to the specification of Event Viewer. Therefore, specifying a source name displayed in Event Viewer for the `source` attribute might cause a mismatch.

Whether the string `Microsoft-Windows-` is prefixed can be checked with **More Information** in the **General** tab, or with **System>Provider>Name** in the **Details** tab of Event Viewer. However, some source names cannot be checked in Event Viewer. For such a source name, if the JP1 event converted from an event log message is registered on the event server, check the `PRODUCT_NAME` extended attribute. Then, use the `source` part of `/HITACHI/JP1/NTEVENT_LOGTRAP/source` as the source name. Alternatively, when you specify a source name in the condition statement, use a partial match ("`source-name`") rather than a complete match ("`^source-name$`") or forward match ("`^source-name`").

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 16–19: 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
Critical	Critical	Critical
Verbose	Verbose	Information
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 than 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.

To specify a single quotation mark (`'`) in a regular expression, place a backslash (`\`) before the single quotation mark. 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*.

If `1` is specified for the `unicode-trap` parameter, use extended regular expressions for condition statements. For details about how to extend regular expressions, see *3.4.5 Extending regular expressions to be used*.

If an event log message contains a line feed character, because the statements in the `filter` are AND conditions, we recommend that you split the message and specify them separately.

If you absolutely need to specify a line feed character in a regular expression for operational reasons, note the following:

- Line feed characters differ between the applications that output the data. If the character code is `\n`, specify `\n`. If the character code is `\r\n`, specify `.\n`. Note that which code a line feed has cannot be visibly distinguished. Contact the application developer or conduct an operation test before starting monitoring.

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.)
- The file name `nthevent2.conf` is a reserved name. Do not use this name when you back up definition files.
- If `1` is specified for `unicode-trap`, and a JP1 event for which UTF-8 is used as the code set is registered, upgrade the JP1/Base on the host to which the JP1 event is to be forwarded to version 8 or later.
- In JP1/Base 11-00 or later, you no longer need to specify the `trap-interval` and the `jplevent-send` parameters. However, if you do specify these parameters, JP1/Base operation is not adversely affected.
- In a JP1/Base version earlier than 11-00, the default of the `retry-times` parameter was `0`. From JP1/Base version 11-00, the default has been changed to `3`.

Supplied action definition file for event log trapping

According to the setting in the supplied action definition file for event log trapping (`nthevent.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
```

If you use the action definition file for event log trapping (`nthevent.conf`) and forwarding settings file (`forward`) in their default state, the message `KAJP1037-E` is output to the event log and converted to a JP1 event when an attempt to forward a JP1 event fails. 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 "Applica
tion"
    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
```

Definition example 5: Specifying the event ID and trap name of a JP1 event

In this example, if a log message satisfies the condition of filter 1, the message is converted to a JP1 event with event ID 0000111A. At this time, Action-1 is set for the JP1_TRAP_NAME attribute.

If a log message satisfies the condition of filter 2, the log message is converted to a JP1 event with event ID 0000111B. At this time, Action-2 is set for the JP1_TRAP_NAME attribute.

Filter 1:

- Type: Application log
- Type: Error

Filter 2:

- Type: Application log
- Type: Warning

```
# Filter 1
filter "Application" id=111A trap-name=Action-1
    type Error
end-filter
# Filter 2
filter "Application" id=111B trap-name=Action-2
    type Warning
end-filter
```

Distribution definition file

Format

```
[destination-host, . . . ]  
definitions  
[ &destination-host, . . . ]  
definitions  
[destination-host, . . . ]@action-definition-file-name  
definitions  
:
```

Parameters by type

Required parameters:

None

Custom parameters:

- *destination-host*
- *definitions*
- @*action-definition-file-name*

File name

Table 16–20: Names of distribution definition file

Definition file for distribution destination	Name of distribution definition file
Forwarding settings file	[<i>jev_forward.conf</i> <i>any file</i>]
Action definition file for log file trapping	[<i>jev_logtrap.conf</i> <i>any file</i>]
Log-file trap startup definition file	[<i>jev_logstart.conf</i> <i>any file</i>]
Action definition file for event log trapping	[<i>jev_ntevent.conf</i> <i>any file</i>]

Storage destination directory

Table 16–21: Storage locations of distribution definition files (in Windows)

Definition file for distribution destination	Storage location
Forwarding settings file	<i>event-folder</i> #\
Action definition file for log file trapping	<i>installation-folder</i> \conf\
Log-file trap startup definition file	<i>installation-folder</i> \conf\event\
Action definition file for event log trapping	<i>installation-folder</i> \conf\event\

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

- *installation-folder*\conf\event\servers\default

Table 16–22: Storage locations of distribution definition files (in UNIX)

Definition file for distribution destination	Storage location
Forwarding settings file	<i>event-directory</i> #/
Action definition file for log file trapping	/etc/opt/jplbase/conf/
Log-file trap startup definition file	/etc/opt/jplbase/conf/event/
Action definition file for event log trapping	/etc/opt/jplbase/conf/event/

#: Replace *event-directory* with the following directory:

- /etc/opt/jplbase/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 appropriate location, with the default file name or a name of your choice.

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 15. *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*

Specify a file name or relative path of your choice only if you want to distribute the definition information of the log file trap definition file. The definition information is distributed to the specified file or relative path under the following folder on the target host:

- In Windows: *installation-folder*\conf\
- In UNIX: /etc/opt/jp1base/conf/
- Specify a file name so that the length of the full path, including the above folder, does not exceed 256 bytes.
- Note that you cannot use tabs, spaces, or the following symbols when specifying the distribution definition file: :, /, ;, *, ?, ", <, >, or |. Furthermore, you cannot use ". ." in the file name to indicate a higher-level directory.

jevlog.conf is the default action definition file name when you omit this parameter.

If @*operation-definition-file-name* is specified after [], the definition information will be distributed to a file of the specified file name or relative path on all of the hosts specified in [].

definitions

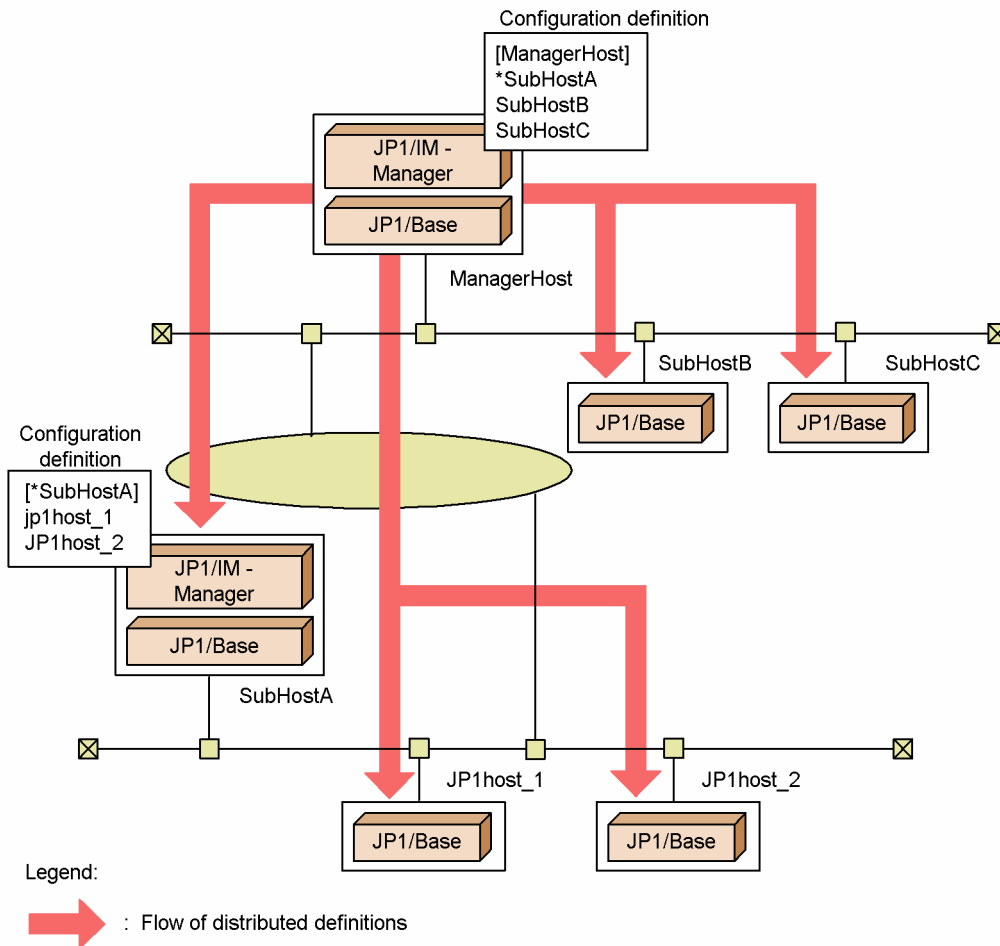
Specify definitions you want to distribute to each host. The file format is the same as that of each definition file. For details, see the following sections:

- 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 16–9: 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 *JP1/Integrated Management 3 - 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/NT_LOGTRAP
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/NT_LOGTRAP  
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-or-information-search-user-name:password
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

Any

Storage destination directory

Any

Description

Sets password management information for multiple OS users or information-search 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 *15. 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-or-information-search-user-name

Specify one or more OS user names or information-search 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.

To register an information-search user, type the name in the format of *aduser/OS-user-name-used-as-the-information-search-user*.

password

Specify the password for the *OS-user-name-or-information-search-user-name*. If you omit the password, the OS user or information-search user is registered in the password information as an OS user or information-search 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

```
jp1user1:passwd000
```

User permission level file

Format

```
; Comment  
JP1-user:JP1-resource-group=JP1-permission-level:JP1-resource-group=JP1-permission-level: . . .
```

Parameters by type

Required parameters:

None

Custom parameters:

- *JP1-user*
- *JP1-resource-group*
- *JP1-permission-level*

File name

JP1_UserLevel

Storage destination directory

In Windows:

installation-folder\conf\user_acl\
shared-folder\jplbase\conf\user_acl\ (in a cluster system)

In UNIX:

/etc/opt/jplbase/conf/user_acl/
shared-directory/jplbase/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 *15. 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). Specify no more than 64 bytes as the JP1 resource group.

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`.

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. The JP1 resource group to specify here should be determined in consultation with the manuals of JP1 products that use JP1/Base user authentication. 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`. The JP1 permission level to specify here should be determined in consultation with the manuals of JP1 products that use JP1/Base user authentication.

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.
- Each line must end with a linefeed character(Windows:CR(0x0d) and LF(0x0a), UNIX:LF(0x0a)).

Definition examples

```
jpladmin:*=JP1_AJS_Admin,JP1_JPQ_Admin,JP1_Console_Admin
```

User permission definition file

Format (To specify a JP1 user)

```
; Comment  
JP1-user:JP1-resource-group=JP1-permission-level:JP1-resource-group=JP1-permission-level: . . .
```

Format (To specify a DS group)

```
; Comment  
[DS-group-name]:JP1-resource-group=JP1-permission-level:JP1-resource-group=JP1-permission-level: . . .
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

Any

Storage destination directory

Any

Description

This file defines operating permission for a JP1 user or DS group to access JP1 resource groups. The JP1 user can be a standard user, linkage user, or DS user. Specify this definition file for the `-f` option of the `jbssetacl` command.

Application of settings

Executing the `jbssetacl` command by specifying this definition file with the `-f` option applies the settings to the authentication server or directory server. When you make a change to operating permissions of a DS user or DS group, you must restart JP1/Base or execute the reload command (`jbsaclreload`). For details about the commands, see [jbssetacl](#) and [jbsaclreload](#) in *15. Commands*.

Definition details

Use one line per entry to assign JP1 permission level to the JP1 user or DS group you want to register or modify to allow access to JP1 resource groups. The permissible number of characters on one line is 4,096 bytes or less. The character `;` and the following characters through a carriage return are treated as comments. An entry consists of two or more fields delimited by a `:`. The following explains how to write individual fields.

JP1-user-name

Specify a JP1 user name. 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. Permissible characters for a JP1 user name are limited to ASCII characters except `* / \ " ' ^ [] { } () : ; | = , + ? < >`, space, and tab characters.

[DS-group-name]

Specify a security group name of a directory server.

You can specify this field only for the operation to use a DS user.

Permissible number of characters is 1 through 256 (bytes). Permissible characters for a DS group name are limited to ASCII characters except * / \ " ' ^ [] { } () : ; | = , + ? < > , and tab characters.

JP1-resource-group=JP1-permission-level

Specify a JP1 resource group and JP1 permission level (JP1 user or DS group operating permission). Specify no more than 64 bytes as the JP1 resource group.

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`.

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. The JP1 resource group to specify here should be determined in consultation with the manuals of JP1 products that use JP1/Base user authentication. 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 or DS group 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 or DS group 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 of JP1 user or DS group 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`. The JP1 permission level to specify here should be determined in consultation with the manuals of JP1 products that use JP1/Base user authentication.

Note

Even in the case to register to the Active Directory a JP1 user (DS user) that requires login authentication only and does not require JP1 operating permission, setting of JP1 operating permission attribute is necessary. In such a case, specify the character string `none` to indicate that no JP1 operating permission is required. An example (JP1 user name is `jpluserx`) is shown below.

```
jpluserx:*=none
```

Definition examples

To define a JP1 resource group and JP1 permission level for JP1 user name `jpladmin`:

```
jpladmin:*=JP1_AJS_Admin,JP1_JPQ_Admin,JP1_Console_Admin
```

To define a JP1 resource group and JP1 permission level for DS group name `GRP-Adm`:

```
[GRP-Adm]:*=JP1_AJS_Admin,JP1_JPQ_Admin,JP1_Console_Admin
```

Directory server modification file (Windows only)

Format

```
"SERVER"=directory-server-name-or-domain-name
"PORT"=destination-port-number
"SEARCH_USER_DN"=information-search-user-ID
"BASE_DN"=container-object-ID#
"ATTR_NAME"=relative-ID-or-attribute-name
"SSL"=dword:{00000000 | 00000001}
"AREC_EXCLUSIVE"=dword:{00000000 | 00000001}
```

#:

The BASE_DN parameter can be specified only for the operation to use a linkage user.

Parameters by type

Required parameters:

None

Custom parameters:

None

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 *15. Commands*.

Triggers to make definitions effective are explained below.

- For operation to use a linkage user
Definitions become effective at the time of login authentication.
- For operation to use a DS user
Definitions become effective at the time of JP1/Base (authentication server) start. If directory server linkage definition is changed after JP1/Base starts, restart of JP1/Base or execution of the reload command (`jbs_spm�_reload`) is required.

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

```
"SERVER"="host-B.domain.local"  
"PORT"=dword:0000027C  
"SEARCH_USER_DN"="CN=Groupcsearcher,OU=GroupC,DC=domain,DC=local"  
"BASE_DN"="OU=JP1,DC=domain,DC=local"  
"ATTR_NAME"="CN"  
"SSL"=dword:00000001
```

Directory server linkage definition file (Windows only)

Format

```
[JP1_DEFAULT\JP1BASE\DIRSRV]
"ENABLE"=dword:{00000000 | 00000001 | 00000002}
"SERVER"=directory-server-name-or-domain-name
"PORT"=Destination-port-number
"SEARCH_USER_DN"=information-search-user-ID
"BASE_DN"=container-object-ID#
"ATTR_NAME"=relative-ID-or-attribute-name
"SSL"=dword:{00000000 | 00000001}
"AREC_EXCLUSIVE"=dword:{00000000 | 00000001}
```

:

The BASE_DN parameter can be specified only for the operation to use a linkage user.

Parameters by type

Required parameters:

None

Custom parameters:

- ENABLE
- SERVER
- SEARCH_USER_DN
- BASE_DN
- ATTR_NAME
- SSL

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 user 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 15. *Commands*.

Triggers to make definitions effective are explained below.

- For operation to use a linkage user
Definitions become effective at the time of login authentication.
- For operation to use a DS user
Definitions become effective at the time of JP1/Base (authentication server) start. If directory server linkage definition is changed after JP1/Base starts, restart of JP1/Base or execution of the reload command (`jbs_spmd_reload`) is required.

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`. Specify `00000001` to link with a directory server using a linkage user. Specify `00000002` to link with a directory server using a DS user. When omitted from the common definition information, the default of `00000000` applies.

SERVER

Specify the directory server name or domain name to link with the directory server with linked users.

Specify the domain name to link with the directory server with DS users.

`jp1hosts` information or `jp1hosts2` information cannot resolve the name of the linked directory server or domain name to an IP address. Therefore, specify a linked directory server or a domain name so that the OS `hosts` file, for example, can resolve the name.

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.



Note

You can define only one domain controller host name for this parameter.

If, however, there are multiple domain controllers under a domain, you can reference all of them by specifying the name of that domain for this parameter.

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`.

If this parameter is not specified in the common definition information, the following port numbers are assumed:

- When SSL is not used: 389 (`00000185`)
- When SSL is used: 636 (`0000027C`)

SEARCH_USER_DN

Specify the ID for the information-search user who will access the directory server. You can specify a character string that is from 1 to 4,095 bytes. For the case of operation to use a linkage user, an information-search user is a directory server user who has view permission for the search-origin container object and the underlying container objects. For

the case of operation to use a DS user, specify the user who has the write permission to the JP1 operating permission for users or groups. To invalidate this parameter, define "SEARCH_USER_DN=""

You must specify this parameter for the case to use the directory server linkage extension function for the operation to use a linkage user or for the case of operation to use a DS user.

BASE_DN

This parameter is valid only for the operation to use a linkage user.

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.

If you specify the SEARCH_USER_DN parameter, the directory server will be able to link with the JP1 user in the container object specified with this parameter.

ATTR_NAME

Specify attribute names of the relative ID that is used as a JP1 user name and DS group. You can enter a character string that is from 1 to 255 bytes.

If you specify the SEARCH_USER_DN parameter, you will be able to specify one of the following attributes as the attribute used for the JP1 user name: Note that when UserPrincipalName is specified, the DS group name is assumed to be sAMAccountName. Ensure that the names are unique across multiple domains.

- CN
- sAMAccountName
- UserPrincipalName

Note on using CN

To use the expanded directory server linkage function, make sure that the value of the CN attribute of each OS user (linked with a JP1 user) under the container object specified for the BASE_DN parameter is unique.

SSL (Can be omitted)

Specify whether to use SSL. Specify as 00000000 if you do not want to use SSL. When omitted from the common definition information, the default of 00000001 applies.

AREC_EXCLUSIVE (Can be omitted)

Specify how to connect to the directory server that is specified with the SERVER parameter, when linked users are used. Specify 00000000 to perform normal name resolution on connection. Specify 00000001 to perform simplified name resolution. This parameter is assumed to be 00000000 when the setting is not included in the common definition information. The value of 00000001 is useful when it takes a long time to resolve the name of the directory server.

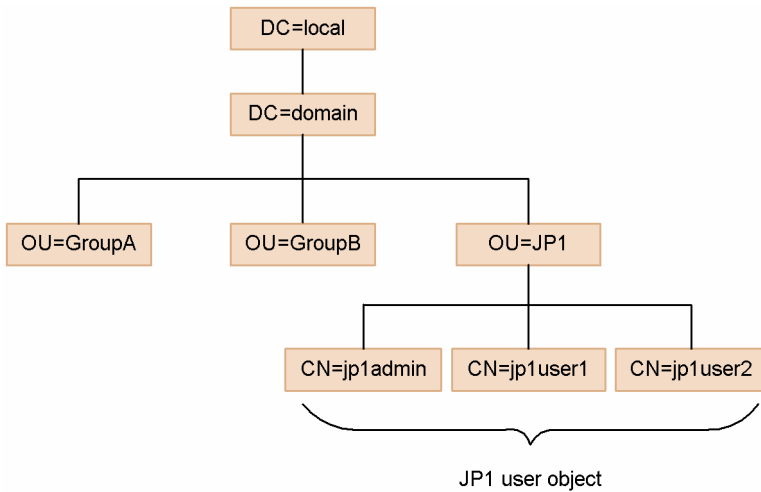
Note

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

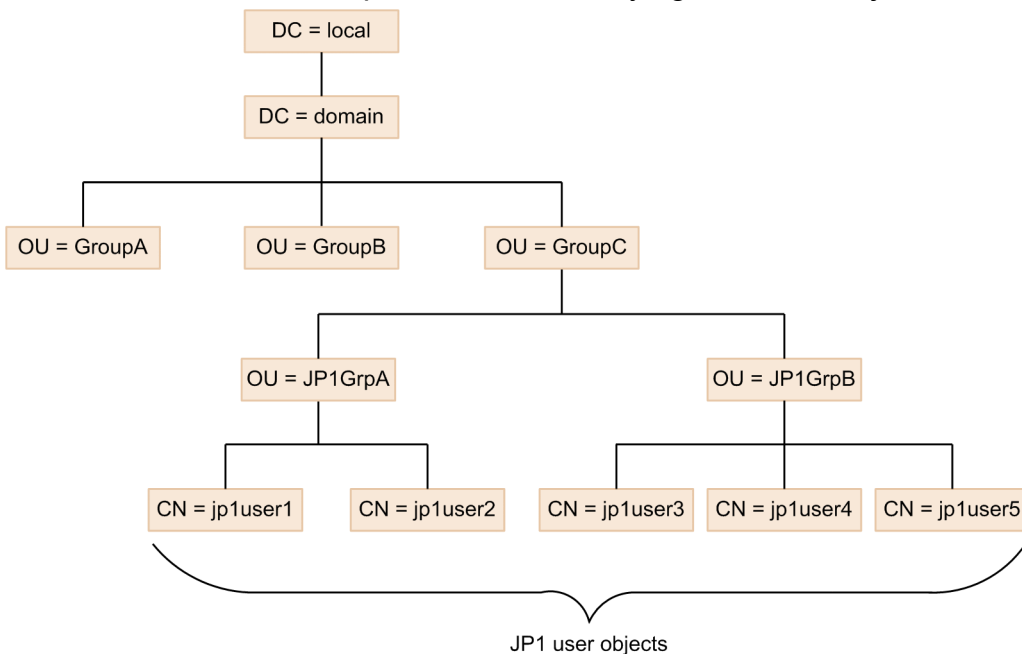
The following shows an example of a definition for performing user authentication linking with the directory server in the configuration shown below.

Figure 16–10: Example of directory server configuration (when linking the container object "OU=JP1" to the directory server)



```
[JP1_DEFAULT\JP1BASE\DIRSRV]
"ENABLE"=dword:00000001
"SERVER"="host-A.domain.local"
"PORT"=dword:0000027C
"SEARCH_USER_DN"="CN=Groupcsearcher,OU=GroupC,DC=domain,DC=local"
"BASE_DN"="OU=JP1,DC=domain,DC=local"
"ATTR_NAME"="CN"
"SSL"=dword:00000001
```

Figure 16–11: Example of directory server configuration (when linking the container object "OU=GroupC" and the underlying container objects to the directory server)



```
[JP1_DEFAULT\JP1BASE\DIRSRV]
"ENABLE"=dword:00000001
"SERVER"="host-A.domain.local"
"PORT"=dword:0000027C
```

```
"SEARCH_USER_DN"="CN=Groupcsearcher,OU=GroupC,DC=domain,DC=local"  
"BASE_DN"="OU=GroupC,DC=domain,DC=local"  
"ATTR_NAME"="sAMAccountName"  
"SSL"=dword:00000001
```


User mapping definition file

Format

```
; Comment  
JP1-user-name:server-host-name:user-list
```

Parameters by type

Required parameters:

None

Custom parameters:

- *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 *15. 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, add the host name definition in FQDN format.

Specifying a logical host in **Server host**

Specify the logical host name. If you are using domain names with the DNS service without defining logical hosts in `jplhosts` or `jplhosts2` information, add the logical host name definition in FQDN format.

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 *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*, *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *JP1/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* in Windows, 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 (`jplBsUmap.conf`). Any information you enter in the GUI will be reflected in this file.

Definition examples

```
jpladmin:*:Administrator
```

Password policy definition file

Format

```
[JP1_DEFAULT\JP1BASE\PASSWDPOLC]
"ENABLE"=dword:{00000000 | 00000001}
"PASSWD_LEN_MIN"=dword:hexa-decimal-number
"NUM_OF_CHAR_TYPE_MIN"=dword:hexa-decimal-number
"REQ_CHAR_TYPE"=character-type
```

Parameters by type

Required parameters:

None

Custom parameters:

- ENABLE
- PASSWD_LEN_MIN
- NUM_OF_CHAR_TYPE_MIN
- REQ_CHAR_TYPE

File name

jp1bs_passwdpolc.conf

Storage destination directory

In Windows:

installation-folder\conf\passwdpolc\
shared-folder\jp1base\conf\passwdpolc\ (in a cluster system)

In UNIX:

/etc/opt/jp1base/conf/passwdpolc/
shared-directory/jp1base/conf/passwdpolc/ (in a cluster system)

Description

Sets common definition information on the authentication server to set a password policy. If a secondary authentication server is installed, this file must be set on both the primary authentication server and the secondary authentication server.

If a password policy check is enabled, the authentication server determines that a password is valid if the password satisfies all the conditions set out by the policy items.

When setting this file on a logical host, you have to set it on both the primary node and the secondary node. In this case, you have to change JP1_DEFAULT of [JP1_DEFAULT\JP1BASE] to the logical host name.

Application of settings

When the `jbssetcnf` command is executed, the contents of the password policy definition file (`jp1bs_passwdpolc.conf`) are added to the common definition information. For details on the `jbssetcnf` command, see *jbssetcnf* in 15. Commands.

Definitions become effective at the time of JP1/Base (authentication server) start.

Definition details

The following conventions apply to entries in the password policy definition file.

- 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\PASSWDPOLC]
```

This section writes configuration information for password policy checks. To set a logical host, change `JP1_DEFAULT` to the logical host name.

```
"ENABLE"=dword:{00000000 | 00000001}
```

Specify whether to enable or disable the password policy check. Specify `dword:00000001` to enable the function. Specify `dword:00000000` to disable the function. If you omit this parameter from the common definition information, `dword:00000000` is assumed.

The parameters that follow are valid when `dword:00000001` is specified for the `ENABLE` parameter.

```
"PASSWD_LEN_MIN"=dword:hexa-decimal-number
```

Specify the minimum number of characters each password must contain in hexadecimal notation. You can specify a value in the range from `00000006` (6 characters) to `00000020` (32 characters).

If no value is set for this parameter, it is assumed that the default value `00000006` (6 characters) is set.

```
"NUM_OF_CHAR_TYPE_MIN"=dword:hexa-decimal-number
```

Specify the number of character types that must be used in a password in hexadecimal notation.

You can specify a value in the range from `00000000` (0) to `00000004` (4). When no value is set, it is assumed that the default value `00000000` (0) is set. When `00000000` (0) is set, any number of character types can be used in a password. There are four available character types, including numbers, uppercase alphabetic characters, lowercase alphabetic characters, and symbols.

```
"REQ_CHAR_TYPE"=character type
```

Specify a character type that must be used in a password. When specifying multiple character types, separate them with commas (,). The parameter values are case-insensitive.

NUM

The use of one or more numbers (0 to 9) is mandatory.

UPPER

The use of one or more uppercase alphabetic characters (from A to Z) is mandatory.

LOWER

The use of one or more lowercase alphabetic characters (from a to z) is mandatory.

SYMBOL

The use of one or more symbols is mandatory.

Only ASCII characters, except \, ", :, tabs, and spaces, can be used in a password.

When mandatory character types are not set in the common definition information, it is assumed that no mandatory character type is specified for passwords. Similarly, when invalid values (values other than those described above) are specified, it is assumed that no mandatory character type is specified for passwords.

Definition example

An example of a definition used when password policy checks are enabled is provided below. In this example, the following password policy is set:

- At least eight characters must be included in a password.
- A password must use at least three character types.
- A password must use one or more numbers, uppercase alphabetic characters, and lowercase alphabetic characters.

```
[JP1_DEFAULT\JP1BASE\PASSWDPOLC]
"ENABLE"=dword:00000001
"PASSWD_LEN_MIN"=dword:00000008
"NUM_OF_CHAR_TYPE_MIN"=dword:00000003
"REQ_CHAR_TYPE"="NUM,UPPER,LOWER"
```

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)
TIMEOUT=communication-timeout-value (seconds)
STOP_CHECK={YES | NO}
ERROR_DETAIL={YES | NO}
POLLENDMSG={YES | NO}
HOST=host-name1, host-name2, . . .
THRESHOLD={monitoring-threshold | host-name:monitoring-threshold}, . . .
```

Parameters by type

Required parameters:

None

Custom parameters:

[OTHER_HOSTS] section

- INTERVAL
- TIMEOUT
- ERROR_DETAIL
- HOST
- POLLENDMSG
- THRESHOLD

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

Restart JP1/Base or execute the `jbs_spmc_reload` command to apply the settings.

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.
- The health check definition file is a text file in which each line has no more than 1,023 bytes.

[JP1_EVENT]

This section is about issuing JP1 events.

OUTPUT={ YES | NO }

Specify whether to issue a JP1 event upon the detection of a problem during a health check. Specify YES or NO. The default is YES.

RECOVER={ YES | NO }

Specify whether to issue a JP1 event upon recovery from the problem detected during a health check. 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 either `syslog` or the event log upon the detection of a problem during a health check. Specify YES or NO. The default is YES.

RECOVER={ YES | NO }

Specify whether to output a message to either `syslog` or the event log upon recovery from the problem detected during a health check. 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:

$$(current-interval) + ((KAVA7227-I-output-time - KAVA7219-W output-time) \times 1.1)$$

TIMEOUT=*communication-timeout-value* (seconds)

Specify how long the monitoring host (manager) that performed polling to the monitored host can wait for a response from the monitored host.

You can specify from 1 to 3,600 in seconds. The default is 60.

If the monitored host does not respond until the specified time elapses, message KAVA7223-E or KAVA7229-W is output, and monitoring fails.

STOP_CHECK={YES | NO}

Specify whether to monitor starting and stopping of monitored hosts. Specify YES or NO. If you do not specify a value, NO is assumed.

ERROR_DETAIL={YES | NO}

Specify whether to include detailed information in the message (KAVA7223-E or KAVA7229-W) that is output if remote host monitoring fails. You can specify YES or NO. The default is NO.

POLLENDMSG={YES | NO}

Specify whether the polling completion message (KAVA7239-I) is to be output. Specify YES or NO. If you do not specify a value, NO is assumed.

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 2,500 remote hosts can be specified. Hosts in excess of this maximum are not monitored. Host names are case-sensitive.

When you specify multiple host names, you can use a multi-line specification, in addition to the single-line specification shown above. The following shows examples of single-line and multi-line specifications whose meanings are the same:

- Example of a single-line specification

```
HOST=hostA,hostB,hostC
```

- Example of a multi-line specification

```
HOST=hostA
```

```
HOST=hostB
```

```
HOST=hostC
```

THRESHOLD={*monitoring-threshold* | *host-name:monitoring-threshold*}, . . .

Specify the threshold for judging whether an error has occurred on the monitored remote host. The value you specify (as the threshold) determines how many successive monitoring failures will cause JP1/Base to assume an error on the monitored host and report the error to the monitoring host (manager).

You can specify a value in the range from 1 to 64. If you omit this parameter, 1 is assumed as the value of *monitoring-threshold*.

monitoring-threshold

The value specified for *monitoring-threshold* is applied to all monitored hosts. The default is 1. If you specify multiple values, only the first specified value takes effect.

host-name : monitoring-threshold

The value specified for *monitoring-threshold* is applied to the monitored host specified for *host-name*. For *host-name*, specify a character string of no more than 255 bytes. The monitoring threshold specified in *host-name : monitoring-threshold* format takes precedence over the monitoring threshold specified in *monitoring-threshold* format.

For *host-name*, specify a host name that completely matches the host name specified for the `HOST` parameter, including the case. If you specify different thresholds with the same host name, the first specified one takes effect.

You can specify multiple monitoring thresholds in single-line and multi-line specification formats. The following shows examples of single-line and multi-line specifications whose meanings are the same:

- Example of a single-line specification
`THRESHOLD=1,hostA:3,hostB:5`
- Example of a multi-line specification
`THRESHOLD=1`
`THRESHOLD=hostA:3`
`THRESHOLD=hostB:5`

Notes

- If the `TIMEOUT` value (communication timeout) is greater than the `INTERVAL` value (remote-host monitoring interval), monitoring might not be completed within a monitoring interval. In normal operation, do not change the communication timeout from the initial value of 60 (seconds). If you change the communication timeout, set a value smaller than the remote-host monitoring interval. If you set a communication timeout that is longer than the remote-host monitoring interval, message KAVA7237-W is output.
- For detailed information, such as user actions for the error reported by message KAVA7223-E or KAVA7229-W if `YES` is set for the `ERROR_DETAIL` parameter, see *JPI/Base Messages*.
- For *host-name* in the `THRESHOLD` parameter, you can specify one of the monitored hosts specified for the `HOST` parameter. If you specify a host that is not a monitored host, message KAVA7238-W is output.
- If you set the `THRESHOLD` parameter, detection of an error on the monitored host is delayed by the number of times specified as the monitoring threshold. In normal operation, do not change the monitoring threshold from the initial value of 1. Consider whether to adjust the monitoring threshold value if you encounter a monitoring error such as that shown in *2.7.5(5) Operation when a monitoring error occurs due to a temporary failure*.

Common definition settings file (health check function)

Format

```
[JP1_DEFAULT\JP1BASE\JBShc]
"ENABLE"=dword:{00000000 | 00000001}
"FAILOVER"=dword:{00000000 | 00000001}
```

Parameters by type

Required parameters:

None

Custom parameters:

- ENABLE
- FAILOVER

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

This file is used to add the health check function settings to the common definition information. The health check function is disabled by default.

Application of settings

When the `jbssetcnf` command is executed, the health check function settings are added to the common definition information. For details on the `jbssetcnf` command, see *jbssetcnf* in *15. Commands*.

Definition details

The following conventions apply to entries in the common definition settings file (health check function).

- 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. If you omit this parameter from the common definition information, dword:00000000 is assumed.

"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. If you omit this parameter from the common definition information, dword:00000000 is assumed.

#: 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}
```

Parameters by type

Required parameters:

None

Custom parameters:

- SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT
- SEND_PROCESS_RESTART_EVENT
- SEND_AUTHSRV_EVENT

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. Normally, you do not need to change the initial settings.

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 *15. 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. If you omit this parameter from the common definition information, `dword:0` is assumed.

SEND_PROCESS_RESTART_EVENT

Specifies whether to issue a JP1 event when the process is restarted. If you omit this parameter from the common definition information, `dword:0` is assumed.

SEND_AUTHSRV_EVENT

Specifies whether to issue a JP1 event when the authentication server is swapped. If you omit this parameter from the common definition information, `dword:0` is assumed.

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 |
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

jplbs_service_0700.conf

Storage destination directory

In Windows:

installation-folder\conf\

shared-folder\jplbase\conf\ (in a cluster system)

In UNIX:

/etc/opt/jplbase/conf/

shared-directory/jplbase/conf/ (in a cluster system)

Description

This file contains information on what processes to automatically restart, should a process abnormally stop, regardless the reason. Normally, you do not need to change the initial settings.

The following is a list of processes that are managed by the extended startup process definition file.

Table 16–23: Processes managed by the extended startup process definition file

Parent process	Function	Child process	Function
jbs_spmc	JP1/Base process management	jbscomd	Inter-process communication A prerequisite process for the jbsrvmgr process and the jbslact process
		jcocmd	Command execution
		jbsroute	Configuration management
		jbsessionmgr	Authentication server
		jbsplugin	Plug-in service
		jbsbcd	Health check (for local host monitoring)
		jbsbchstd	Health check (for remote host monitoring)
		jbsrvmgr	Service management control This process depends on the jbscomd process

Parent process	Function	Child process	Function
		jbslcact	Local action This process depends on the jbscomd process

Application of settings

Execute the `jbs_spm�_reload` command or restart JP1/Base to apply the settings. For details on the `jbs_spm�_reload` command, see *jbs_spm�_reload* in 15. *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.

For groups of processes that have dependencies, set the same value to all child processes.

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_spm�_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.
- If you want to restart a process in a cluster system, use the cluster software.

Definition examples

- Action to take if a process ends abnormally

The following conditions are set for JP1/Base processes:

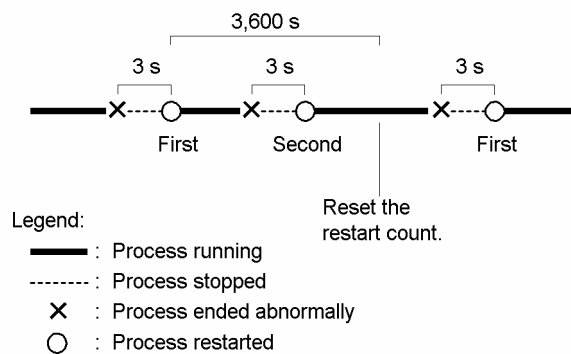
- Restart or not: Restart
- Number of restarts: 4
- Retry interval: 3 seconds
- Restart count reset time:3,600 seconds

```

jcccmd|C:\ProgramFiles\HITACHI\JP1Base\bin\jcccmd.exe||1|4|3|3600|
jbsroute|C:\ProgramFiles\HITACHI\JP1Base\bin\jbsroute.exe|-o,600|1|4|3|3600|
jbsessionmgr|C:\ProgramFiles\HITACHI\JP1Base\bin\jbsessionmgr.exe||1|4|3|3600|
jbsplugin|C:\ProgramFiles\HITACHI\JP1Base\bin\jbsplugin.exe||1|4|3|3600|

```

Figure 16–12: 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.

- Action to take if a process with a dependency ends abnormally

The following action must be taken if a process with a dependency ends abnormally:

- Restart or not: Restart
- Number of restarts: 4
- Retry interval: 3 seconds
- Restart count reset time:21,600 seconds

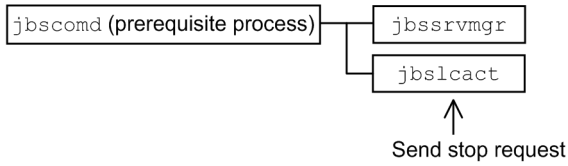
```

jbscomd|C:\Program Files\Hitachi\JP1Base\bin\jbscomd.exe||1|4|3|21600|
jcccmd|C:\Program Files\Hitachi\JP1Base\bin\jcccmd.exe||0|3|3|21600|
jbsroute|C:\Program Files\Hitachi\JP1Base\bin\jbsroute.exe|-o,600|0|3|3|21600|
jbsessionmgr|C:\Program Files\Hitachi\JP1Base\bin\jbsessionmgr.exe||0|3|3|21600|
jbsplugin|C:\Program Files\Hitachi\JP1Base\bin\jbsplugin.exe||0|3|3|21600|
jbsbcd|C:\Program Files\Hitachi\JP1Base\bin\jbsbcd.exe||0|3|3|21600|
jbschostd|C:\Program Files\Hitachi\JP1Base\bin\jbschostd.exe||0|3|3|21600|
jbsrvmgr|C:\Program Files\Hitachi\JP1Base\bin\jbsrvmgr.exe|jbscomd|1|4|3|21600|
jbslcact|C:\Program Files\Hitachi\JP1Base\bin\jbslcact.exe|jbscomd|1|4|3|21600|

```


Figure 16–13: Example action to take if a process with a dependency ends abnormally

(1) Process terminates abnormally (2) Processes stop



Legend:

—— : Dependency relationship with prerequisite process

If the prerequisite process, `jbscomd`, stops abnormally, the dependent processes `jbsrvmgr` and `jbslcact`, also stop. If the "run or not" parameter is set to "restart", dependent processes restart after the prerequisite process has finished restarting.

Set the same value for the "run or not" parameter to all the process groups that have dependencies.

jp1hosts definition file

Format

```
# Comment  
host-name IP-address, IP-address, IP-address
```

Parameters by type

Required parameters:

None

Custom parameters:

None

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 contains hosts information specific to JP1. A `jp1hosts` definition file is provided by default, but cannot be used in its initial state. When you use the default `jp1hosts` definition file, you must first edit it according to the use in JP1/Base. If you create your own `jp1hosts` definition file, store it in the same folder as the default `jp1hosts` file.

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 *15. 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*
Specify the correspondence between host names and IP addresses. *host-name* and *IP-address* must be separated by one or more spaces or tab characters.

host-name

- You can use ASCII characters only.

- You cannot use the following characters:
" / \ [] ; : | = , + ? < >
- Do not specify a string that is recognized as an IP address.

IP-address

- Specify an IPv4 address. You cannot specify an IPv6 address.
- Delimit multiple IP addresses with commas (,). Any space or tab characters before and after the comma are ignored.
- Each IP address must be specified in the format *W.X.Y.Z*. Each of *W*, *X*, *Y*, and *Z* is a decimal number in the range from 0 to 255.
- If you set more than one IP address, JP1/Base uses the first IP address set for each host name.
- If you use the IP binding method for sending, the first IP address set for the local host name is used as the source *IP-address*.
- 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.

jp1hosts2 definition file

Format

```
# Comment
+DefaultResolve {0 | 1}
+PhysicalMerge {0 | 1}
host-name IP-address IP-address IP-address
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

jp1hosts2.conf 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 contains hosts information specific to JP1. A jp1hosts2 definition file is provided by default, and you can also create and edit your own.

Application of settings

Execute the `jbshosts2import` command to apply the information in a jp1hosts2 file. For details on the `jbshosts2import` command, see [jbshosts2import](#) in *15. Commands*.

Definition details

The following conventions apply to entries in the jp1hosts2 definition file:

- A jp1hosts2 definition file consists of one line per entry. There is no limit to the number of characters per line.
- You can define a maximum of 10,000 hosts in a jp1hosts2 definition file.
- A hash mark (#) (code 0x23) at the start of a line indicates a comment.

```
+DefaultResolve {0 | 1}
```

Specify how the system uses the OS hosts file or other methods to resolve host names that are not defined in the jp1hosts2 information. If you omit this parameter, 0 is assumed.

0

Resolve IPv4 addresses only.

1

Resolve IPv4 and IPv6 addresses.

+PhysicalMerge {0 | 1}

Specify whether to enable the physical merge mechanism. The physical merge mechanism merges `jp1hosts2` information for a physical host with that of a logical host. This parameter only applies to the `jp1hosts2` information on logical hosts. If there is no `jp1hosts2` information for the logical host or you omit this parameter from the `jp1hosts2` information on a logical host, 1 applies.

0

Disables the physical merge mechanism.

1

Enables the physical merge mechanism.

Conventions when merging `jp1hosts2` information

If the same host name is defined in the `jp1hosts2` information of the physical and logical hosts, the definition in the `jp1hosts2` information on the logical host applies. An example of merging `jp1hosts2` information is shown below.

jp1hosts2 information on physical host	jp1hosts2 information on logical host	Merged jp1hosts2 information on logical host
hostA addr1 hostB addr2 hostC addr3	hostB addr4 hostD addr5	hostB addr4 hostD addr5 hostA addr1 hostC addr3

The `+DefaultResolve` parameter is also subject to merging, according to the criteria below. The `+PhysicalMerge` parameter is not merged.

- If there is no `+DefaultResolve` parameter in the `jp1hosts2` information on the logical host, the definition for the physical host applies.
- If a `+DefaultResolve` parameter is specified in the `jp1hosts2` information on the logical host, the definition for the logical host applies.

host-name IP-address IP-address IP-address

Specify the correspondence between host names and IP addresses. *host-name* and *IP-address* must be separated by one or more spaces or tab characters.

host-name

- You can use ASCII characters only.
- You cannot use the following characters:
" / \ [] ; : | = , + ? < >
- Do not specify a string that is recognized as an IP address.

IP-address

- You can specify IPv4 and IPv6 addresses.
- Delimit multiple IP addresses with one or more space or tab characters, or a comma (,).
- You can specify a maximum of four IPv4 addresses and four IPv6 addresses for a given host, for a total of eight IP addresses.

- If you specify multiple IP addresses for a remote host, JP1/Base uses the first IP address of those specified to communicate with the host.
- If you use the IP binding method as the communication protocol for sending, the source IP address depends on the destination IP address type. If the destination host uses an IPv4 address, JP1/Base uses the first IPv4 address associated with the local host name. If the destination host uses an IPv6 address, JP1/Base uses the first IPv6 address of the local host name.

Format of IPv4 addresses

- An IPv4 address must be specified in the format *W.X.Y.Z*. Each of *W*, *X*, *Y*, and *Z* is a decimal number in the range from 0 to 255.

Format of IPv6 addresses

- An IPv6 address must be specified in the format *A:B:C:D:E:F:G:H*. Each of *A*, *B*, *C*, *D*, *E*, *F*, *G*, and *H* is a hexadecimal value in the range from 0 to *ffff*.
- You can omit the initial zero from numerical values that begin with a zero.
- For 0000, specify 0.
- Consecutive fields of four zeros can be replaced by two colons, but only once per address.

Example:

Before: 0123:0000:0000:0000:4567:0000:0000:89ab

After: 123::4567:0:0:89ab

Notes on specifying IPv6 addresses

The following addresses will be ignored:

- IPv4-compatible address (addresses other than `::1` and `::0` whose upper 96 bits are zeroes)
- IPv4-mapped address (addresses in which the upper 80 bits are zeroes and the 16 bits from the 81st to 96th bit are ones)
- IPv6 link-local addresses (addresses whose upper 10 bits are 1111 1110 10)
Example: `fe80::`
- Multicast addresses (addresses whose upper 8 bits are ones)
- Brackets ([]), addresses with no values (: :), network interface (%), or subnet mask (/)

Host access control definition file

Format

```
AllowHost {  
  upper-host  
  all-host  
  host host-name-1  
  host host-name-2  
  ...  
  host host-name-n  
}
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

`jbsdfts_srv.conf`

Storage destination directory

In Windows:

installation-folder\conf\jbsdfts

shared-folder\jplbase\conf\jbsdfts\ (in a cluster system)

In UNIX:

`/etc/opt/jplbase/conf/jbsdfts`

shared-folder/jplbase/conf/jbsdfts/ (in a cluster system)

Description

This file specifies which host has access permissions when linking with the IM configuration management functionality 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 *15. 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*.

SSL communication definition file

Format

```
[JP1_DEFAULT\JP1BASE\SSL]
"ENABLE"=dword:{00000000 | 00000001}
"CERTIFICATEFILE"=server-certificate-file-name
"CACERTIFICATEFILE"=route-certificate-file-name
"PRIVATEKEYFILE"=private-key-file-name
"SSLPROTOCOL"=SSL-(TLS)-versions
"SSLCIPHERS"=encryption-suites
"BASESSL"=service-names
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

`jp1bs_ssl.conf` (SSL communication definition file)

`jp1bs_ssl.conf.model` (model file of an SSL communication definition file)

Storage destination directory

For Windows:

installation-folder\conf\

shared-folder\jp1base\conf\ (in a cluster system)

For UNIX:

/etc/opt/jp1base/conf/

shared-directory/jp1base/conf/ (in a cluster system)

Description

This file is used to set the SSL communication settings, such as whether to enable the communication encryption function (SSL communication), the server certificate file name, and the root certificate storage location, in the common definition information.

Application of settings

When the `jbssetcnf` command is executed, the contents of the SSL communication definition file are added to the common definition information. For details about the `jbssetcnf` command, see [jbssetcnf](#) in *15. Commands*.

The changes to the common definition information are applied when JP1/Base is restarted.

Definition details

The following shows the conventions for specifying the SSL communication definition file:

- Do not place a space or tab before or after an equal sign (=) or a comma (,), or at the beginning or end of a line. If you do so, an error occurs during execution of the `jbsssetcnf` command.
- Lines containing only a line break are ignored.

[JP1_DEFAULT\JP1BASE\SSL]

In this section, specify the SSL communication settings, such as whether to enable the communication encryption function (SSL communication). If you are using a logical host, specify `JP1_DEFAULT` as the logical host name.

"ENABLE"=dword:{00000000 | 00000001}

Specify whether to enable the communication encryption function (SSL communication). To enable encrypted communication, specify `dword:00000001`. To disable encrypted communication, specify `dword:00000000`. If this specification does not exist in the common definition information, JP1/Base assumes that `dword:00000000` is specified.

If you specify `dword:00000001`, you can set hosts that perform non-SSL communication by using the non-SSL communication host definition file (`jp1bs_nosslhost.conf`).

The following parameters are enabled if the `ENABLE` parameter is set to `dword:00000001`:

"CERTIFICATEFILE"=*server-certificate-file-name*

Specify the full path name of the server certificate file to be used for the communication encryption function. You can enter a character string that is from 1 to 255 bytes. Specify this parameter on the server-side host in SSL communication, such as a host on which you execute the command or a host on which you start the certificate server process. To disable this parameter, specify "CERTIFICATEFILE"="".

"CACERTIFICATEFILE"=*route-certificate-file-name*

Specify the full path name of the root certificate file that is used for the communication encryption function. If multiple files are required as a route certificate, combine them into a single file, and specify the name of the file. You can enter a character string that is from 1 to 255 bytes. Specify this parameter on all hosts that uses SSL communication.

"PRIVATEKEYFILE"=*private-key-file-name*

Specify the full path name of the private key file that was specified when you requested the CA to issue a server certificate to be used for the communication encryption function. You can enter a character string that is from 1 to 255 bytes. Specify this parameter on the server-side host in SSL communication, such as a host on which you execute the command or a host on which you start the certificate server process. To disable this parameter, specify "PRIVATEKEYFILE"="". In addition, when using elliptic-curve cryptography, specify the private key file name in PKCS#8 format.

"SSLPROTOCOL"=*SSL-(TLS)-versions*

Specify the version of SSL communication. You can specify `TLSv1_3` and `TLSv1_2`.

`TLSv1_3`

Specify this value to use TLS1.3.

`TLSv1_2`

Specify this value to use TLS1.2.

Specify this parameter on the server-side host in SSL communication, such as a host on which you execute the command or a host on which you start the certificate server process. To specify multiple suites, separate each of them by using a colon (:). To disable this parameter, specify "SSLPROTOCOL"="".

"SSLCIPHERS"=*encryption-suites*

Specify an encryption suite of SSL communication that is defined in RFC5246 in which TLS1.2 is specified, and in RFC8446 in which TLS1.3 is specified. If you do not specify this parameter, a strong encryption suite is automatically set according to the server certificate. Therefore, you do not have to specify this parameter normally.

If you want to use an encryption suite, specify it in the format supported by OpenSSL. For example, if you want to use `TLS_DHE_RSA_WITH_AES_256_CBC_SHA256`, specify `DHE-RSA-AES256-SHA256`. For details about encryption suites, see the official website of OpenSSL.

When specifying an ECC-format encryption suite, specify an encryption suite listed in the table below according to the TLS version in use.

SSL version	Encryption suites (SSLCIPHERS)
TLS1.2	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA256
TLS1.3 [#]	<ul style="list-style-type: none"> • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256

#

The TLS1.3 encryption suite listed in the table above can also be specified for an RSA encryption server certificate as TLS1.2 and TLS1.3 use different key conversion and digital signature algorithms.

To specify multiple suites, separate each of them by using a colon (:). You can enter a character string of a length that is from 1 to 255 bytes. Specify this parameter on the server-side host in SSL communication, such as a host on which you execute the command, or a host on which you start the certificate server process. To disable this parameter, specify `"SSLCIPHERS=""`.

Note that if you enable SSL communication in JP1/IM and JP1/AJS3 - Manager, some encryption suites might not be available. For details, see the release notes of the relevant products.

`"BASESSL"=service-names`

Specify the names of services for which the communication encryption function is enabled. You can specify `jp1bsuser`, `jp1imcmda`, and `jp1bsagent`. If you specify both of these values, separate them by a comma (,).

`jp1bsuser`

Specify this value to enable SSL communication on the authentication server (user authentication).

`jp1imcmda`

Specify this value to enable SSL communication for execution of JP1/IM commands. For details about the communication encryption function (SSL communication) of JP1/IM, see the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`jp1bsagent`

Specify this value to enable SSL communication in the following control that supports SSL communication.

Transfer of JP1 events, search for JP1 events, reception of JP1 events, automatic action, execution of commands, management of configurations, and health checks performed between the manager host's JP1/IM - Manager and JP1/Base and the agent host's JP1/Base

Specify this parameter on all hosts that use SSL communication.

However, for the service name `jp1bsagent`, this parameter cannot be specified on the hosts specified in the non-SSL communication host configuration file.

Note

- The parameters shown above are also used when you enable SSL communication in JP1/IM and JP1/AJS3 - Manager. For details, see the manuals for the relevant products.
- If you set the SSL communication definition file on the logical host, you must set the file on both the active and standby nodes. In this case, replace the `JP1_DEFAULT` part in `[JP1_DEFAULT\JP1BASE\SSL]` by the logical host name.

- For security purposes, do not store a server certificate (CERTIFICATEFILE), root certificate (CACERTIFICATEFILE), or private key (PRIVATEKEYFILE) in a directory from which the data collection tool collects data. For details about the collection targets of the data collection tool, see *18.3.1 Data that must be collected when a problem occurs (in Windows)* and *18.3.2 Data that must be collected when a problem occurs (in UNIX)*.

Definition examples

```
[JP1_DEFAULT\JP1BASE\SSL]
"ENABLE"=dword:00000001
"CERTIFICATEFILE"="C:\JP1\SSL\cert.pem"
"CACERTIFICATEFILE"="C:\JP1\SSL\cacert.pem"
"PRIVATEKEYFILE"="C:\JP1\SSL\certkey.pem"
"SSLPROTOCOL"="TLSv1_2"
"BASESSL"="jplbsuser,jplimcmda,jplbsagent"
```

Non-SSL communication host configuration file

Format

```
[NO_SSL_HOST]
non-SSL communication host name-1
non-SSL communication host name-2
:
```

Parameters by type

Required parameters:

None

Custom parameters:

Non-SSL communication host name

File name

jp1bs_nossl.conf (non-SSL communication host configuration file)

jp1bs_nossl.conf.model (model file of a non-SSL communication host configuration file)

Storage destination directory

In Windows:

installation-folder\conf\

In UNIX:

/etc/opt/jp1base/conf/

Description

This file is used to set destination and originating hosts that do not perform SSL communication in an environment where the communication encryption function (SSL communication) is enabled. The settings specified in this file are applicable to physical hosts, logical hosts, and event services.

In an environment where SSL communication is enabled, SSL communication is used to access hosts not specified in this file. Even when this file does not exist, SSL communication is used between the destination host and the originating host.

Application of settings

After editing the non-SSL communication host configuration file, start or restart JP1/Base services and event services to apply the settings specified in the file.

Definition details

Specify the names of the destination and originating hosts that do not perform SSL communication. The following rules apply to the non-SSL communication host configuration file:

- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- Each line must end with a linefeed character.
- You can use ASCII characters only.

- You cannot use the following characters:
" / \ [] ; : | = , + ? < >
- Define one host name in each line.
The host names are case-insensitive and must be 255 bytes or less.
Single-byte spaces or tabs specified at the beginning or end of a host name are ignored.
- You can define a maximum of 100 hosts.
- If you specify the same host name multiple times, only the first value specified becomes valid.

Note

The non-SSL communication host configuration file is referenced by physical hosts, logical hosts, and any event services. It is therefore important to ensure that reliable communication can be maintained even when the non-SSL communication host configuration file is edited by mistake while it is in use. To this end, three generations of non-SSL communication host configuration file with a generation number assigned to each one of them as well as the non-SSL communication host configuration file with all errors removed from it are saved upon the startup of JP1/Base and event services. Do not delete the saved files.

Table 16–24: Location in which the non-SSL communication host configuration files are saved

	For Windows	For UNIX
When JP1/Base is started	<p>On a physical host:</p> <pre>installation- folder\sys\nossl_base.conf installation-folder\sys\nossl_base{1 2 3}.conf</pre> <p>On a logical host:</p> <pre>shared- folder\jplbase\sys\nossl_base.conf shared- folder\jplbase\sys\nossl_base{1 2 3}.conf</pre>	<p>On a physical host:</p> <pre>/var/opt/ jplbase/sys/nossl_base.conf /var/opt/jplbase/sys/ nossl_base{1 2 3}.conf</pre> <p>On a logical host:</p> <pre>shared-directory/ jplbase/sys/nossl_base.conf shared-directory/jplbase/sys/ nossl_base{1 2 3}.conf</pre>
When event services are started	<p>On a physical host:</p> <pre>installation- folder\sys\tmp\event\servers\defa ult\nossl_evt.conf installation- folder\sys\tmp\event\servers\defa ult\nossl_evt{1 2 3}.conf</pre> <p>On a logical host:</p> <pre>shared- folder\jplbase\event\nossl_evt.co nf shared- folder\jplbase\event\nossl_evt{1 2 3}.conf</pre>	<p>On a physical host:</p> <pre>/var/opt/jplbase/sys/tmp/event/ servers/default/nossl_evt.conf /var/opt/jplbase/sys/tmp/event/ servers/default/nossl_evt{1 2 3}.conf</pre> <p>On a logical host:</p> <pre>shared-directory/event/ nossl_evt.conf shared-directory/event/nossl_evt{1 2 3}.conf</pre>

When the non-SSL communication host configuration file contains an error, JP1/Base services and event services ignore the line containing the error and start up after outputting only the KAVB3920-W or KAJP1510-W message to the log.

Definition examples

Examples of a definition (or definitions) in a non-SSL communication host configuration file are provided below.

When SSL communication takes place during communication with all hosts:

To use encrypted communication during communication with all hosts, define only the `[NO_SSL_HOST]` line.

```
[NO_SSL_HOST]
```

When both non-SSL communication and SSL communication take place during communication with a specific host:

Non-SSL communication takes place during communication with `hostA` and SSL communication takes place during communication with all the other hosts.

```
[NO_SSL_HOST]  
hostA
```

Local action environment variable file

Format

```
Environment variable name 1=variable-value-1
[Environment variable name 2=variable-value-2]
:
```

Parameters by type

Required parameters:

None

Custom parameters:

None

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
:
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

`jbslcact.conf`

Storage destination directory

In Windows:

`installation-folder\conf\lcact`

`shared-folder\jplbase\conf\lcact` (in a cluster system)

In UNIX:

`/etc/opt/jplbase/conf/lcact/`

`shared-directory/jplbase/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](#).

Note that only the following JP1 events registered on the local event server are subject to the execution condition of the local action (event filter):

- Event issued from the local event server to the local event server (JP1 event registered reason: 1)
- Event issued from another event server to the local event server (JP1 event registered reason: 3)

An example is an event registered by using the `jevsend` command (with the `-d` option specified) or the `jevsendd` command from another event server of the local host to the local event server.

JP1 events forwarded from another event server (JP1 event registered reason: 4) are not applicable.

[`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 [2.8.2 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}` (Windows only)

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 16–25: 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 (<i>basic-code:extended-code</i>)
	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:

- 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 Δ line2`, whereas Δ 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}
"CODECONV"=dword:{00000000 | 00000001}
```

Parameters by type

Required parameters:

None

Custom parameters:

None

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 *15. Commands*.

Next, either execute the `jbsspmdd_reload` command or restart JP1/Base to apply the common definition information settings. For details on the `jbsspmdd_reload` command, see *jbsspmdd_reload* in *15. Commands*.

Definition details

The following conventions apply to entries in the common definition settings file (local action function).

- 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. When omitted from the common definition information, the default of 00100000 (1,024 KB) applies.

"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. When omitted from the common definition information, the default of 00000004 (four files) applies.

"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 you omit this parameter or specify a value that cannot be specified in the common definition information, the default of `dword:00000000` applies.

"CODECONV"=`dword:{00000000 | 00000001}`

Specifies whether to convert the character code when expanding attribute values from a JP1 event by specifying an attribute variable name. Specify `dword:00000000` to expand the attribute value as is in the JP1 event character code. Specify `dword:00000001` to convert the attribute value to match the character code used in the operation environment before expanding. If you omit this parameter or specify a value that cannot be specified in the common definition information, the default of `dword:00000000` applies.

Collection information file

Format

```
information-identifier<FILE>file-name  
:
```

Parameters by type

Required parameters:

None

Custom parameters:

None

File name

`jbsparamdump.conf`

Storage destination directory

In Windows:

`installation-folder\conf\`

In UNIX:

`/etc/opt/jplbase/conf/`

Description

When the `jbsparamdump` command is used to collect the JP1/Base setup information, this file is used to specify file names and destinations so that users can collect files with desired names and store them in desired destinations.

For example, if your operation has multiple action definition files for log file trapping that have different user-specified names, you can specify the destinations and names for the files so that definition information of the action definition files for log file trapping can be collected.

For details on the `jbsparamdump` command, see [jbsparamdump](#) in *15. Commands*.

Application of settings

The setting is referenced when you execute the `jbsparamdump` command.

Definition details

The following conventions apply to entries in the collection information file:

- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- Duplicate *information-identifiers* can be omitted.
- <FILE> between *information-identifier* and *file-name* cannot be omitted.
- Space and tab characters included in *information-identifier* are regarded as part of the information identifier.
- Space and tab characters between <FILE> and *file-name* are ignored.
- Space and tab characters at the end of the *file-name* are ignored.

- The character code of the file must match the character code in the environment in which the `jbsparamdump` command is executed.

information-identifier

Specify a character string of no more than 256 bytes, for identifying collection targets.

file-name

Specify a collection target file name in full path. Only the text format file can be specified.

Definition example

The following shows a definition example and an output example when the `jbsparamdump` command is executed:

Definition example:

```
# LOGTRAP DEFINITIONS
LOGTRAP_AP1<FILE>D:\temp\jevlog_ap1.conf
LOGTRAP_AP2<FILE>C:\Program Files\HITACHI\JP1Base\conf\jevlog_ap2_1.conf
LOGTRAP_AP2<FILE>C:\Program Files\HITACHI\JP1Base\conf\jevlog_ap2_2.conf
```

Output example (userconf.prm file):

```
***JP1/Base User Configurations(FileVersion=105000 TimeStamp=2013/09/12 14:22:13)
*****LOGTRAP_AP1<FILE>D:\temp\jevlog_ap1.conf Contents of the jevlog_ap1.conf file ***End LOGTRAP_AP1(SUCCESS)
*****LOGTRAP_AP2<FILE>C:\Program Files\HITACHI\JP1Base\conf\jevlog_ap2_1.conf Contents of the jevlog_ap2_1.conf file ***End LOGTRAP_AP2(SUCCESS)
*****LOGTRAP_AP2<FILE>C:\Program Files\HITACHI\JP1Base\conf\jevlog_ap2_2.conf Contents of the jevlog_ap2_2.conf file ***End LOGTRAP_AP2(SUCCESS)
```

Common definition settings file (configuration management functionality)

Format

```
[JP1_DEFAULT\JP1BASE\JBS_ROUTE]
"JBSRT_DISTRIB_VERSION"=dword:{00000000 | 00000001}
"JBSROUTE_COM_TIMEOUT"=dword:hexa-decimal-number
```

Parameters by type

Required parameters:

None

Custom parameters:

- JBSRT_DISTRIB_VERSION
- JBSROUTE_COM_TIMEOUT

File name

Any

`jbsrt_setup.conf.model` (Model file for the common definition settings file (configuration management functionality))

Storage destination directory

The model file for the common definition settings file (configuration management functionality) is stored in the directories listed below. Create a common definition settings file with a file name of your choice by copying the model file.

In Windows:

installation-folder\conf\route\
shared-folder\jp1base\conf\route\ (in a cluster system)

In UNIX:

/etc/opt/jp1base/conf/route/
shared-directory/jp1base/conf/route/ (in a cluster system)

Description

This file is used to set the specified information on the configuration management functionality to the common definition information. If you newly installed JP1/Base, JBSRT_DISTRIB_VERSION is set to 1 (differential distribution method). If you installed JP1/Base by overwriting a JP1/Base version earlier than 11-10, JBSRT_DISTRIB_VERSION is not defined (in which case, the batch distribution method will be used).

For details about the differential distribution functionality, see [2.6.3 Managing the system's hierarchical configuration by using commands](#).

Application of settings

When the `jbssetcnf` command is executed, the information in the common definition settings file (configuration management functionality) is added to the common definition information. The value set for JBSRT_DISTRIB_VERSION in the common definition takes effect when the `jbsrt_distrib` command is

executed. The value of common definition `JBSROUTE_COM_TIMEOUT` is applied when the `jbs_spm�_reload` command is executed or JP1/Base is restarted. For details about the `jbssetcnf` command and the `jbsrt_distrib` command, see *jbssetcnf* and *jbsrt_distrib* in 15. *Commands*.

Definition details

The following rules apply to the common definition settings file (configuration management functionality):

- Do not use a space or tab before or after an equal sign (=) or at the beginning or end of a line. If a space or tab is used in these locations, an error occurs when the `jbssetcnf` command is executed.
- Lines containing only a linefeed character are ignored.

```
[JP1_DEFAULT\JP1BASE\JBS_ROUTE]
```

This section specifies the configuration management functionality settings. If you set up a logical host, use `JP1_DEFAULT` as the logical host name.

```
"JBSRT_DISTRIB_VERSION"=dword:{00000000 | 00000001}
```

Specify whether to use the batch distribution method or the differential distribution method to distribute configuration definition information. To use the batch distribution method, specify `dword:00000000`. To use the differential distribution method, specify `dword:00000001`. If the specified value is not a value that can be specified in the common definition information or no value is specified, `dword:00000000` is assumed.

```
"JBSROUTE_COM_TIMEOUT"=dword:hexa-decimal-number
```

Specify a communication timeout value (in seconds) in a hexadecimal number for the execution of configuration distribution or configuration synchronization. The permissible range is from `00000001` (1 second) through `00015180` (86,400 seconds). If any invalid value is specified, the initial value `00000258` (600 seconds) for a starting up case or, for a reloading case, a previously effective value before reloading is assumed. If no value is specified, the initial value `00000258` (600 seconds) is assumed.

Notes

If you specify a large value for communication timeout (`JBSROUTE_COM_TIMEOUT`), it may take too much time to execute the `jbsrt_distrib` or `jbsrt_sync` command for configuration management functionality or to set system hierarchical configuration (IM configuration) using IM configuration management. We recommend that you use the initial value of 600 seconds as it is.

Reconsider the communication timeout value if timeout occurs in such a case explained in 2.6.3 (5) *Reviewing the communication timeout value*.

Configuration definition file

Format

```
[manager-host-1]
managed-host
managed-host
:
[manager-host-2]
managed-host
:
```

File name

`jbs_route.conf` (configuration definition file)

`jbs_route.conf.model` (model file for the configuration definition file)

Storage directory

In Windows

For a physical host:

`Base-path\conf\route\`

For a logical host:

`shared-folder\jplbase\conf\route\`

In UNIX

For a physical host:

`/etc/opt/jplbase/conf/route/`

For a logical host:

`shared-directory/jplbase/conf/route/`

Description

This file defines the system hierarchy that is to be managed by JP1/IM.

JP1/IM operates under a hierarchical system configuration that consists of managers that manage the system and agents. There can be a hierarchy under each manager, which enables JP1/IM to manage systems of various sizes.

The system hierarchy is managed by JP1/Base, which is the prerequisite product that provides the core functionality of JP1/IM.

Based on the hierarchy information that is defined in this file, the JP1/IM functions operate as follows:

- JP1 event forwarding
Important JP1 events are forwarded from lower-level hosts to higher-level hosts, as defined in the configuration definition information (when the default settings are used).
- Automated actions and command execution
Automated action and command execution requests can be issued to hosts specified in the configuration definition information.

You must enter a linefeed on the last line of the file.

When the definitions are applied

The specified configuration definition information takes effect when the following commands are executed for applying the definitions:

- `jbsrt_distrib` (distributes definition information)
- `jbsrt_sync` (synchronizes definition information at the highest manager)
- `jbsrt_del` (deletes definition information)

Information that is specified

[*manager-host*]

- Specifies the host name of a manager.
The manager is the host where JP1/IM - Manager is installed.
- Express the host name using from 1 to 255 alphanumeric characters, the hyphen (-), and the period (.).
- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- If you divide the system configuration definition, place an asterisk (*) immediately before the host name that is duplicated in (continued to) another configuration definition file.

managed-host

- Specifies the name of a host that is managed by the specified manager.
- Express the host name using from 1 to 255 alphanumeric characters, the hyphen (-) and the period (.).
- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- If you divide the system configuration definition, place an asterisk (*) immediately before the host name that is duplicated in (continued from) another configuration definition file.
- JP1/Base must be installed on a managed host. A managed host cannot be defined under more than one manager.
- Specify a host name that is registered in the `hosts` file or on the DNS server, or a host name that is defined in `jp1hosts` or `jp1hosts2`.
- If you specify an asterisk (*) as part of the host name, which is not permitted, the `jbsrt_distrib` command will not delete the configuration definition information that follows that host name.
- You cannot specify an alias name for a host.
- If you use the automated action function or the command execution function, specify for a managed host the same host name that is specified in the command execution or automated action function. If the host is a physical host, specify the host name that is returned by the `hostname` command.

Example definition

The following describes examples of configuration definition files for a JP1/IM system based on the system hierarchy shown in the table below. The first example is of a batch definition; the second example is of divided definitions.

Table 16–26: JP1/IM system hierarchy (example)

Integrated manager	Site manager	Agents
jp1sv1	jp1sv2	jp1ag1, jp1ag2

Integrated manager	Site manager	Agents
	jp1sv3	jp1ag3, jp1ag4, jp1ag5

Example of a batch definition:

To create a batch definition, edit the configuration definition file at the integrated manager as follows (there is no need to edit the files at the site managers or agents):

Configuration definition file for integrated manager jp1sv1:

```
[jp1sv1]
jp1sv2
jp1sv3
[jp1sv2]
jp1ag1
jp1ag2
[jp1sv3]
jp1ag3
jp1ag4
jp1ag5
```

Example of divided definitions:

To create divided definitions, edit a configuration definition file at the integrated manager and at each site manager as follows (there is no need to edit files at the agents):

Configuration definition file for integrated manager jp1sv1:

```
[jp1sv1]
*jp1sv2
*jp1sv3
```

Configuration definition file for site manager jp1sv2:

```
[*jp1sv2]
jp1ag1
jp1ag2
```

Configuration definition file for site manager jp1sv3:

```
[*jp1sv3]
jp1ag3
jp1ag4
jp1ag5
```

Environment variable file

Format

```
environment-variable-name-1=variable-value-1  
[environment-variable-name-2=variable-value-2]  
:  
:
```

File name

Use any file.

Storage directory

In Windows

Any folder on the host where commands are executed

In UNIX

Any directory on the host where commands are executed

Description

This file defines environment variables to be used when commands are executed at managed hosts in JP1/IM.

When you use automated actions and JP1/IM - View to execute commands on managed hosts in JP1/IM, you can specify environment variables as part of the execution environments for the commands. You can set environment variables by using environment variable files that are specified in the format described here.

An environment variable file can have any name. By creating multiple environment variable files, you can specify an appropriate file for each command that is to be executed.

If no applicable environment variable file is specified in a Windows environment, the system's environment variables are used for command execution.

You must enter a linefeed code at the end of each line.

The upper limit for one line is 1,023 bytes. If specifying multi-byte character code, encoding is the JP1/Base character code.

Do not specify character strings that are not in the format *environment-variable-name=variable-value*. If a specification is invalid, the command might terminate abnormally, depending on the OS on the host where the command is executed.

When the definitions are applied

An environment variable file is referenced when execution of a command begins.

Information that is specified

environment-variable-name

Specify the name of an environment variable.

You cannot specify an environment variable that contains a linefeed character.

variable-value

Specify a value for the environment variable.

The upper limit for one line is 1,023 bytes. Encoding for the environment variable file is the character code for the managed host on which commands are executed.

By specifying the system environment variable name as this value, you can inherit the system environment variable value.

If you specify a system environment variable, enclose the variable name in the character sequences <- and ->, such as <-variable->.

Host group definition file

Format

```
host-group-name
{
  host-name-1
  host-name-2
  :
  :
}
```

File name

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file defines a group of managed hosts in JP1/IM.

When a command is to be executed in JP1/IM by means of an automated action or a JP1/IM - View operation, you can set a group of hosts where the command is to be executed and then execute the command on all of those hosts in the batch mode.

When the definitions are applied

The specified information takes effect after you execute the `jcocmddef` command.

If you set a logical host in a cluster configuration, set the file at both the primary and secondary nodes.

Information that is specified

host-group-name

Specifies a name for identifying the host group.

Express a host group name using from 1 to 32 alphanumeric characters. The space character and two-byte characters cannot be used.

You execute a command on a host group by specifying the name of the host group. For example, you can specify a host group name in `d=execution-host-name-or-group-name` in the automated action definition file or in **Target host** in the Execute Command window.

host-name

Specifies the name of a host that is to be a member of the group.

Express a host name using from 1 to 255 alphanumeric characters. The space character and two-byte characters cannot be used.

Note that only a monitored host defined in a configuration definition file can be specified here.

Deleting a host group

To delete a host group, create an empty definition with the name of the host group that is to be deleted from the host group definition file, and then execute the `jcocmddef` command.

Editing a host group

To edit an existing host group definition, re-create the host group definition file using the same host group name, and then execute the `jcocmddef` command.

17

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.

17.1 JP1 event attributes

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.

17.1.1 Basic attributes

Table 17–1: Basic attributes of JP1 events

Attribute	Format ^{#1}	Contents
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. ^{#7}
Event ID	Two numeric values (32 bits) ^{#2}	An 8-byte value indicating the application program that issued the event and the event contents.
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
Source process ID	Numeric value (32 bits)	Process ID of the application program that issued the event.
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).
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.
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).
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).
Source user name	Character string (0 to 20 bytes)	User name of the source process.
Source group name	Character string (0 to 20 bytes)	Group name of the source process. Null string in Windows and Java.
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.

Attribute	Format ^{#1}	Contents
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.
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.)
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.)
Source serial number	Numeric value (32 bits)	Serial number in the event database on the source host (unchanged at event transfer). ^{#6}
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. ^{#4}
Message	Character string (0 to 1,023 bytes) ^{#5}	Message text indicating the JP1 event contents.
Detailed information	Character string or byte string (0 to 1,024 bytes) ^{#5}	Any data.

#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: The values include:

- 8859_1 (ISO-8859-1)
- SJIS (shift JIS)
- EUCJIS (EUC Japanese)
- UTF-8 (Japanese UTF-8)

#5: 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

#6: The value is in the range of 0 to 2,147,483,647. The value returns to 0 when it reaches 2,147,483,647. However, a number in the sequence might appear to be missing because of a Registered reason-2 event that is internally used.

17.1.2 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. Note that setting items differ depending on the JP1 program. The program-specific information is extended information that is not common information.

Table 17–2: 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, 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.)
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.
End time	END_TIME	Time at which execution completed, as the number of seconds since UTC 1970-01-01 00:00:00.
Result code	RESULT_CODE	Result code represented as a character string of decimal (base 10) numbers.

17.2 List of JP1 events output by JP1/Base

Table 17–3: JP1 events output by JP1/Base

Event ID	Occurrence	Message
00001011	When an agent host is added during scale out	Agent host (<i>agent-host-name</i>) has scale-out.
00003D00	When the event database is switched	Event DB was switched from <i>old-database-number</i> to <i>new-database-number</i> .
00003D04	When the event service restart function restarts an abnormally stopped process	The event service was recovered by restarting an internal function.
00003D05	When a specified amount of time has passed since event forwarding suppression was performed by the <code>jevagtfw</code> command	Suppression of event-forwarding by the <code>jevagtfw</code> command has continued for <i>total-suppression-time</i> seconds. (server = <i>host-name</i>)
00003D06	When event forwarding suppression is performed by using the <code>jevagtfw</code> command	Event-forwarding from <i>host-name</i> is now being suppressed.
00003D07	When event forwarding is suppressed by using the <code>jevagtfw</code> command	The suppression of event-forwarding from <i>host-name</i> was stopped.
00003D08	When received events are discarded by using the <code>jevagtfw</code> command	The events received from <i>host-name</i> are now being discarded.
00003D09	When discarding of received events is stopped by using the <code>jevagtfw</code> command	Discarding of events received from <i>host-name</i> was stopped.
00003D0B ^{#4}	When threshold-based suppression of event-forwarding is started by detecting the occurrence of a large number of events based on a threshold	<i>host-name</i> will start the threshold-based suppression of event-forwarding. (suppression ID = <i>identifier</i>)
00003D0C ^{#4}	When threshold-based suppression of event-forwarding is stopped by detecting convergence of a large number of events based on the threshold	<i>host-name</i> stopped the threshold-based suppression of event-forwarding. (suppression ID = <i>identifier</i>)
00003D0D ^{#4}	When threshold-based suppression of event-forwarding is stopped by reloading (executing the <code>jevreload</code> command) or by stopping the event service	<i>host-name</i> stopped all threshold-based suppressions of event-forwarding.
00003D0E ^{#4}	When a specified amount of time has passed since the threshold-based suppression of event-forwarding was started	Suppression of event-forwarding by <i>host-name</i> has continued for <i>total-suppression-time</i> seconds. (suppression ID = <i>identifier</i>)
00003A10 ^{#3}	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 ^{#3}	When a log file trap cannot start log file monitoring	Monitoring of the relevant log file cannot start.
00003A21 ^{#3}	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.

Event ID	Occurrence	Message
00003A22#3	When an application log file is in error status	Monitoring of the relevant log file cannot continue.
00003A25#3	When a log file trap starts, or begins monitoring its first log file	The log file (<i>file-type</i>) will now be monitored.
00003A26#3	When a log file trap switches its monitoring target during the monitoring process	A different log file (<i>file-type</i>) is now being monitored.
00003A27#3	When monitoring an UPD type log file, the status of the monitored log file becomes abnormal	The log file (<i>file-type</i>) can no longer be properly monitored.
00003A28#3	When more than the maximum number of files match a monitoring target name that includes a wildcard pattern	Monitoring will now stop because the number of files corresponding to the monitoring file name exceeds the maximum.
00003A29#3	When a log file trap cannot identify a log file to monitor	Monitoring will now stop because no log files can be identified for monitoring.
00003A2A#3	When the addition of a file causes the number of potential monitoring targets to approach the maximum	<i>number-of-files</i> files correspond to the monitoring file name.
00003A30	When a remote monitoring log (log file trap or event log trap) terminates abnormally and then restarts	Log data from the termination previous to this startup might not be registered as JPI events.
00003A31	When a remote monitoring log (log file trap or event log trap) terminates abnormally in a state where a connection can be established with the event service	The remote monitor stopped due to an error that prevents processing.
00003A32	When a remote monitoring log (log file trap or event log trap) was able to reconnect to the event service	Event issuance was delayed because the system retried the remote monitor.
00003A71 or the event ID specified in the filter of the action definition file for event log trapping	When a log message for a Windows event is detected	Windows event-log message
Event ID specified in the ACTDEF parameter in the action definition file for log file trapping#3	When a record of an AP log file is detected	Contents of one line of log file data
00003FA0#1	When the command execution control receives an command execution request from the Execute Command window	[<i>host-name:JPI-user-name</i>] Command execution started.
00003FA1#1	When the command execution requested from the Execute Command window completes	[<i>host-name:JPI-user-name</i>] Command execution ended normally.
00003FA2#1	When command execution from the Execute Command window is not performed for some reason	[<i>host-name:JPI-user-name</i>] 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	[<i>host-name</i>] The execution time of command execution exceeded the regulation value (<i>number sec</i>)

Event ID	Occurrence	Message
	automated action is performed after the issuance interval of the elapse time event has been exceeded.	
00003FA5#1	When a threshold of queued commands is specified in the <code>jcocmddef</code> command. When the number of queued commands has reached the threshold of the automated action	In <i>target-host-name</i> , the number of queued commands requested from <i>source-host-name</i> has exceeded the threshold (xx).
00003FA6#1	When a threshold of queued commands is specified in the <code>jcocmddef</code> command. When the threshold of queued commands for the automated action is specified as 0	In <i>target-host-name</i> , the number of queued commands requested from <i>source-host-name</i> has become 0.
00003FA7	When automatic re-organization of the command execution log file has failed	Restoration of the command execution log file failed.
00004700#2	When an authentication server is blocked	<i>connection-sequence: authentication-server-name</i> was successfully blocked.
00004701#2	When an authentication server is unblocked	<i>connection-sequence: authentication-server-name</i> was successfully unblocked.
00004702#2	When all authentication servers are blocked	All authentication servers are blocked.
00004720#2	When the process ends abnormally	<i>component-name management-target-process-name</i> has ended abnormally.
00004721#2	When an attempt to start a process results in a timeout	A <i>component-name</i> timeout occurred in <i>management-target-process-name</i> Processing continues.
00004722#2	When an abnormally ended process is restarted	Restart of the <i>component-name management-target-process-name</i> has finished.
00004724#4	When JP1/Base has finished the startup process	JP1/Base has started on the host <i>host-name</i> .
00004725#4	When JP1/Base will be stopped	JP1/Base will now end on the host <i>host-name</i> .
00004740	When a monitored process ends abnormally	<i>function-name</i> ended abnormally.
00004741	When a monitored process has been unable to access (update) shared memory for a set time (SEVERITY:Error)	<i>function-name</i> has been processing for <i>nn</i> seconds.
00004742	When a monitored process has been unable to access (update) shared memory for a set time (SEVERITY:Warning)	<i>function-name</i> has been processing for <i>nn</i> seconds. After passes of <i>mm</i> seconds, becomes error condition.
00004743	When a monitored process that was unable to access (update) shared memory for a set time has recovered	<i>function-name</i> 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 <i>host-name</i> because <i>service-name</i> is not functioning.

Event ID	Occurrence	Message
00004749	When an error (host unreachable) is detected during monitoring of a remote host	Monitoring cannot be performed because a connection with <i>host-name</i> cannot be established. (<i>reason-message: detailed information</i>)
0000474A	When a remote host becomes able to be monitored. When a monitoring target that was stopped starts again.	<i>host-name</i> can now be monitored.
0000474B	When the shared memory is inaccessible	The shared memory is locked.
0000474C	When the monitoring target host stops.	The host <i>host-name</i> will not be monitored because it is not running.
0000474D	When the system cannot determine whether a monitoring target host has stopped or an error has occurred	Monitoring cannot be performed because a connection cannot be established with <i>host-name</i> , which is not receiving stop notifications. (<i>reason-message: detailed information</i>)
0000474E	When the system cannot reference the shared memory of one or more functions	The status of <i>function-name</i> cannot be confirmed.
0000474F	When the system continues to be unable to reference the shared memory of one or more functions	The status of <i>function-name</i> still cannot be confirmed.
00004750	When the system is able to reference the previously inaccessible shared memory of one or more functions	The status of <i>function-name</i> can now be confirmed.
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. (<i>action-execution-information</i>)
00004781	When command execution completed and the JP1 event (action end event) is registered	An action has completed. (<i>action-execution-information</i>)
00004782	When command execution is not completed and the JP1 event (action end event (not executable)) is registered	An action ended without being executed. (<i>action-execution-information</i>)
00004783	When command execution is canceled and the JP1 event (action end event (cancellation)) is registered	An action ended because it was cancelled. (<i>action-execution-information</i>)

#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 *15. 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 [4.3 Detecting abnormal process termination and authentication server switching](#).

#3: The log file trap or JP1/AJS log monitoring job issues the event.

#4: These JP1 events are forwarded to every destination host in the forwarding settings file (`forward`) even if they do not match the conditions of the event filter. If you do not want these events to be forwarded, define an exclusion condition or specify the `auto-forward-off` flag in the `options` parameter of the event server settings file (`conf`).

17.3 JP1 event details

This section lists JP1 event details by event ID.

17.3.1 JP1 event details by event ID

(1) Details about event ID 00001011

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00001011
		Message	--	Agent host (<i>agent-host-name</i>) has scale-out.
Extended attribute	Common information	Event level	SEVERITY	Information
	Program-specific information	OS type	OS_TYPE	OS name (Windows or Linux)
		Installation information	INSTALLPP_INFO	Whether linkage products (JP1/PFM) have been installed (PFM_Install or PFM_Not_Install)

(2) Details about event ID 00003D00

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003D00
		Message	--	Event DB was switched from <i>old-database-number</i> to <i>new-database-number</i> .
		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	<i>event-server-name</i> : <i>old-database-number</i>
		Occurrence	OCCURRENCE	SWITCH
	Program-specific information	Old event database number	E0	Old event database number

(3) Details about event ID 00003D04

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003D04

Attribute type		Item	Attribute name	Contents
		Message	--	The event service was recovered by restarting an internal function.
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

(4) Details about event ID 00003D05

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D05
		Message	B.MESSAGE	KAJP1087-W Suppression of event-forwarding by the jevagtfw command has continued for <i>total-suppression-time</i> seconds. (server = <i>host-name</i>)
Extended attribute	Common information	Event level	E.SEVERITY	Warning
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	JEVAGTFW
		Occurrence	E.OCCURRENCE	INTERVAL_PROGRESS
	Program-specific information	Suppression condition	E.HOST	Host name #
		Report interval	E.INTERVAL	Interval for reporting (seconds)
		Suppression time	E.SUPPRESSED_TIME	Time when the suppression was performed

#: All alphabetic characters must be capitalized.

(5) Details about event ID 00003D06

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D06
		Message	B.MESSAGE	KAJP1410-I Event-forwarding from <i>host-name</i> is now being suppressed.
Extended attribute	Common information	Event level	E.SEVERITY	Information
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice

Attribute type		Item	Attribute name	Contents
		Object ID	E.OBJECT_ID	JEVAGTFW
		Occurrence	E.OCCURRENCE	START_SUPPRESS
	Program-specific information	Suppression condition	E.HOST	Host name [#]

[#]: All alphabetic characters must be capitalized.

(6) Details about event ID 00003D07

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D07
		Message	B.MESSAGE	KAJP1421-I The suppression of event-forwarding from <i>host-name</i> was stopped.
Extended attribute	Common information	Event level	E.SEVERITY	Information
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	JEVAGTFW
		Occurrence	E.OCCURRENCE	END_SUPPRESS
	Program-specific information	Suppression condition	E.HOST	Host name [#]
		Suppression time	E.SUPPRESSED_TIME	Time when the suppression was performed

[#]: All alphabetic characters must be capitalized.

(7) Details about event ID 00003D08

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D08
		Message	B.MESSAGE	KAJP1430-I The events received from <i>host-name</i> are now being discarded.
Extended attribute	Common information	Event level	E.SEVERITY	Information
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	JEVAGTFW
		Occurrence	E.OCCURRENCE	START_DISPOSE
	Program-specific information	Suppression condition	E.HOST	Host name [#]

[#]: All alphabetic characters must be capitalized.

(8) Details about event ID 00003D09

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D09
		Message	B.MESSAGE	KAJP1424-I Discarding of events received from <i>host-name</i> was stopped.
Extended attribute	Common information	Event level	E.SEVERITY	Information
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	JEVAGTFW
		Occurrence	E.OCCURRENCE	END_DISPOSE
	Program-specific information	Suppression condition	E.HOST	Host name [#]
		Suppression time	E.SUPPRESSED_TIME	Time during which discarding was performed (seconds)

[#]: All alphabetic characters must be capitalized.

(9) Details about event ID 00003D0B

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D0B
		Message	B.MESSAGE	KAJP1083-W <i>host-name</i> will start the threshold-based suppression of event-forwarding. (suppression ID = <i>identifier</i>)
Extended attribute	Common information	Event level	E.SEVERITY	Warning
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	FORWARD_SUPPRESS
		Occurrence	E.OCCURRENCE	START
	Program-specific information	Suppression condition	E.SUPPRESS_ID	Identifier

Note: These JP1 events are forwarded to every destination host in the forwarding settings file (*forward*) even if they do not satisfy the event filter conditions. If you do not want these events to be forwarded, define an exclusion condition or specify the *auto-forward-off* flag in the *options* parameter of the event server settings file (*conf*).

(10) Details about event ID 00003D0C

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D0C
		Message	B.MESSAGE	KAJP1084-I <i>host-name</i> stopped the threshold-based suppression of event-forwarding. (suppression ID = <i>identifier</i>)
Extended attribute	Common information	Event level	E.SEVERITY	Information
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	FORWARD_SUPPRESS
		Occurrence	E.OCCURRENCE	END
	Program-specific information	Suppression condition	E.SUPPRESS_ID	Identifier

Note: These JP1 events are forwarded to every destination host in the forwarding settings file (`forward`) even if they do not satisfy the event filter conditions. If you do not want these events to be forwarded, define an exclusion condition or specify the `auto-forward-off` flag in the `options` parameter of the event server settings file (`conf`).

(11) Details about event ID 00003D0D

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D0D
		Message	B.MESSAGE	KAJP1085-I <i>host-name</i> stopped all threshold-based suppressions of event-forwarding.
Extended attribute	Common information	Event level	E.SEVERITY	Information
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	FORWARD_SUPPRESS
		Occurrence	E.OCCURRENCE	END_ALL
	Program-specific information	Suppression condition	E.SUPPRESS_ID	*

Note: These JP1 events are forwarded to every destination host in the forwarding settings file (`forward`) even if they do not satisfy the event filter conditions. If you do not want these events to be forwarded, define an exclusion condition or specify the `auto-forward-off` flag in the `options` parameter of the event server settings file (`conf`).

(12) Details about event ID 00003D0E

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	B.ID	00003D0E
		Message	B.MESSAGE	KAJP1086-W Suppression of event-forwarding by <i>host-name</i> has continued for <i>total-suppression-time</i> seconds. (suppression ID = <i>identifier</i>)
Extended attribute	Common information	Event level	E.SEVERITY	Warning
		Product name	E.PRODUCT_NAME	/HITACHI/JP1/IM
		Object type	E.OBJECT_TYPE	EVENT
		Object name	E.OBJECT_NAME	jevservice
		Object ID	E.OBJECT_ID	FORWARD_SUPPRESS
		Occurrence	E.OCCURRENCE	INTERVAL_PROGRESS
	Program-specific information	Suppression condition	E.SUPPRESS_ID	Identifier

Note: These JP1 events are forwarded to every destination host in the forwarding settings file (`forward`) even if they do not satisfy the event filter conditions. If you do not want these events to be forwarded, define an exclusion condition or specify the `auto-forward-off` flag in the `options` parameter of the event server settings file (`conf`).

(13) 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 = <i>process-ID</i> / <i>thread-ID</i> [<i>monitoring-target-name</i>])
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> jevlogstart command with <code>-p</code> option specified /HITACHI/JP1/NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. jevlogstart command with <code>-p</code> option unspecified /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> jevlogstart command with <code>-p</code> option specified

Attribute type		Item	Attribute name	Contents
				/HITACHI/JP1/ UX_LOGTRAP/ <i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. <ul style="list-style-type: none"> • 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	

(14) 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= <i>error-number</i> , file name= <i>log-file-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	In Windows: <ul style="list-style-type: none"> • jevlogstart command with -p option specified /HITACHI/JP1/ NT_LOGTRAP/ <i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. <ul style="list-style-type: none"> • jevlogstart command with -p option unspecified /HITACHI/JP1/NT_LOGTRAP In UNIX: <ul style="list-style-type: none"> • jevlogstart command with -p option specified /HITACHI/JP1/ UX_LOGTRAP/ <i>program-name</i>

Attribute type		Item	Attribute name	Contents
				<p><i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option.</p> <ul style="list-style-type: none"> jevlogstart command with <code>-p</code> 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	Monitoring stop time	WATCH_STOP_TIME	Time at which log file monitoring stopped (number of seconds since UTC 1970-01-01 00:00:00)

(15) Details about event ID 00003A21

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A21
		Message	--	<p>KAVA3644-E Monitoring will now stop because the specified number of retries was performed, but the relevant log file cannot be read. (code=<i>error-number</i>, file name=<i>log-file-name</i>)</p>
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> jevlogstart command with <code>-p</code> option specified /HITACHI/JP1/NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. jevlogstart command with <code>-p</code> option unspecified /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> jevlogstart command with <code>-p</code> option specified /HITACHI/JP1/UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. jevlogstart command with <code>-p</code> option unspecified /HITACHI/JP1/UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE

Attribute type		Item	Attribute name	Contents
		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)

(16) 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= <i>error-number</i> , file name= <i>log-file-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/NT_LOGTRAP/<i>program-name</i> <i>program-name</i> 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 <p>In UNIX:</p> <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/UX_LOGTRAP/<i>program-name</i> <i>program-name</i> 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

(17) Details about event ID 00003A25

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A25
		Message	--	KAVA3668-I The log file (<i>file-type</i>) will now be monitored. (<i>id=process-ID [monitored-target-name] / thread-ID [monitored-target-name] , file name=log-file-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	In Windows: <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/ NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. jevlogstart command without -p option specified /HITACHI/JP1/NT_LOGTRAP In UNIX: <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. jevlogstart command without -p option specified /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
		Monitoring start time	WATCH_START_TIME	Time at which the system started monitoring the log file (as a number of seconds since UTC 1970-01-01 00:00:00)
	Program-specific information			

(18) Details about event ID 00003A26

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A26
		Message	--	KAVA3669-I A different log file (<i>file-type</i>) is now being monitored. (<i>id=process-ID [monitored-target-name] / thread-ID [monitored-target-name] , file name=log-file-name</i>)

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	In Windows: <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. jevlogstart command without -p option specified /HITACHI/JP1/NT_LOGTRAP In UNIX: <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. jevlogstart command without -p option specified /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	Monitoring switch time	WATCH_CHANGE_TIME	Time at which the process started monitoring a different log file (as a number of seconds since UTC 1970-01-01 00:00:00)

(19) Details about event ID 00003A27

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A27
		Message	--	KAVA3670-E The log file (<i>file-type</i>) can no longer be properly monitored. (id= <i>process-ID</i> [<i>monitored-target-name</i>]/ <i>thread-ID</i> [<i>monitored-target-name</i>], code= <i>error-number</i> , file name= <i>log-file-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	In Windows: <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/NT_LOGTRAP/<i>program-name</i>

Attribute type		Item	Attribute name	Contents
				<p><i>program-name</i> is the name of the source program that output the log data, as specified in the -p option.</p> <ul style="list-style-type: none"> jevlogstart command without -p option specified /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/UX_LOGTRAP/<i>program-name</i> <p><i>program-name</i> is the name of the source program that output the log data, as specified in the -p option.</p> <ul style="list-style-type: none"> jevlogstart command without -p option specified /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 (as a number of seconds since UTC 1970-01-01 00:00:00)	

(20) Details about event ID 00003A28

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A28
		Message	--	KAVA3671-E Monitoring will now stop because the number of files corresponding to the monitoring file name exceeds the maximum. (id= <i>process-ID</i> [<i>monitored-target-name</i>] / <i>thread-ID</i> [<i>monitored-target-name</i>], FILETYPE= <i>file-type</i>)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/NT_LOGTRAP/<i>program-name</i> <p><i>program-name</i> is the name of the source program that output the log data, as specified in the -p option.</p> <ul style="list-style-type: none"> jevlogstart command without -p option specified /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p>

Attribute type		Item	Attribute name	Contents
				<ul style="list-style-type: none"> • jevlogstart command with -p option specified /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. • jevlogstart command without -p option specified /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	Monitoring stop time	WATCH_STOP_TIME	Time at which monitoring of the log file was stopped (as a number of seconds from UTC 1970-01-01 00:00:00)

(21) Details about event ID 00003A29

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A29
		Message	--	KAVA3672-E Monitoring will now stop because no log files can be identified for monitoring. (id= <i>process-ID</i> [<i>monitored-target-name</i>] / <i>thread-ID</i> [<i>monitored-target-name</i>], code= <i>error-number</i> , FILETYPE= <i>file-type</i>)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> • jevlogstart command with -p option specified /HITACHI/JP1/ NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. • jevlogstart command without -p option specified /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> • jevlogstart command with -p option specified /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option.

Attribute type		Item	Attribute name	Contents
				<ul style="list-style-type: none"> jevlogstart command without -p option specified /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	Monitoring stop time	WATCH_STOP_TIME	Time at which monitoring of the log file was stopped (as a number of seconds from UTC 1970-01-01 00:00:00)

(22) Details about event ID 00003A2A

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A2A
		Message	--	KAVA3673-W <i>number-of-files</i> files correspond to the monitoring file name. (id= <i>process-ID</i> [<i>monitored-target-name</i>]/ <i>thread-ID</i> [<i>monitored-target-name</i>] , FILETYPE= <i>file-type</i>)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/ NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. jevlogstart command without -p option specified /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> jevlogstart command with -p option specified /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the -p option. jevlogstart command without -p option specified /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	Number of files check time	WATCH_FILECHECK_TIME	Time at which the number of files was checked (as a number of seconds from UTC 1970-01-01 00:00:00)

(23) Details about event ID 00003A30

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A30
		Message	--	KAVA3909-W Log data from the termination previous to this startup might not be registered as JP1 events. (event server = <i>event-server-name</i> , target host = <i>monitored-host</i> , monitor name = <i>monitored-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> With the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/ NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. Without the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> With the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. Without the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	<p>When monitoring a log file: jelallog</p> <p>When monitoring the event log: jelalelt</p>
		Object ID	OBJECT_ID	ID number of remote monitoring log where the error was detected
Occurrence	OCCURRENCE	NOTICE		

Attribute type		Item	Attribute name	Contents
	Program-specific information	Monitored host name	MONITOR_HOST	Name of monitored host
		Monitor name	MONITOR_NAME	Monitored-name

(24) Details about event ID 00003A31

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A31
		Message	--	KAVA3910-E The remote monitor stopped due to an error that prevents processing. (event server = <i>event-server-name</i> , target host = <i>monitored-host</i> , monitor name = <i>monitored-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> With the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/ NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. Without the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> With the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. Without the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	<p>When monitoring a log file: jelallog</p> <p>When monitoring the event log: jelalelt</p>
		Object ID	OBJECT_ID	ID number of remote monitoring log where the error was detected
Occurrence	OCCURRENCE	NOTICE		

Attribute type		Item	Attribute name	Contents
	Program-specific information	Monitored host name	MONITOR_HOST	Name of monitored host
		Monitor name	MONITOR_NAME	Monitored-name

(25) Details about event ID 00003A32

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A32
		Message	--	KAVA3915-W Event issuance was delayed because the system retried the remote monitor. (event server = <i>event-server-name</i> , target host = <i>monitored-host</i> , monitor name = <i>monitored-name</i>)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	<p>In Windows:</p> <ul style="list-style-type: none"> With the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/ NT_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. Without the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/NT_LOGTRAP <p>In UNIX:</p> <ul style="list-style-type: none"> With the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/ UX_LOGTRAP/<i>program-name</i> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. Without the <code>-p</code> option specified as an additional option in the Display/Edit Profiles window of JP1/IM /HITACHI/JP1/UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	<p>When monitoring a log file: jelallog</p> <p>When monitoring the event log: jelalelt</p>
		Object ID	OBJECT_ID	ID number of remote monitoring log for which the retry operation took place
Occurrence	OCCURRENCE	RECONNECT		

Attribute type		Item	Attribute name	Contents
Program-specific information	Monitored host name	MONITOR_HOST		Name of monitored host
	Monitor name	MONITOR_NAME		Monitored- name
	Retry start time	RETRY_START_TIME		When the retry operation took place (as a number of seconds from UTC 1970-01-01 00:00:00)
	Reconnection time	RECONNECT_TIME		When reconnection to the event service was confirmed (as a number of seconds from UTC 1970-01-01 00:00:00).
	Number of held events	HOLD_EVENT		The number of JP1 events held during retry processing
	Number of deleted events	DELETE_EVENT		The number of JP1 events deleted during retry processing

(26) Details about event ID 00003A71 or the event ID specified in the filter of the action definition file for event log trapping

Attribute type		Item	Attribute name	Contents	
Basic attribute	Event ID		--	Event ID specified in the filter of the action definition file for event log trapping If no event ID is specified, 00003A71 is used by default.	
	Message		--	Windows event-log message ^{#1} . Maximum 1,023 bytes. Any excess is truncated.	
Extended attribute	Common information	Event level	SEVERITY	The value depends on the Windows log type: Value: Log type Critical: Critical Error: Error Warning: Warning Information: Information, Verbose, Other Notice: Audit_success, Audit_failure	
		Product name	PRODUCT_NAME	/HITACHI/JP1/ NTEVENT_LOGTRAP/ <i>source</i>	
		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/ Setup/Directory Service/DNS Server/File Replication

Attribute type		Item	Attribute name	Contents
				Service/Internet Explorer/Key Management Service/HardwareEvents Also, the content displayed in Log Name in the Event Viewer.
		NT log type	A3	Critical/Error/Warning/Information/Verbose/Audit_Success/Audit_Failure Also, the content displayed in Level in the Event Viewer. For the security log, the information displayed in Keyword in the Event Viewer window
		NT log category	A4	Category None if unidentifiable. The information displayed as Category under Task in the Event Viewer.
		NT event ID	A5	Windows event ID
		NT user name	A6	Windows user name. N/A if unidentifiable.
		NT log level ^{#2}	A7	The log level. The content of the Level field in the Event Viewer. Maximum 256 bytes. Any excess is truncated.
		NT log keyword ^{#2}	A8	Keywords. The content of the Keywords field in the Event Viewer. Maximum 256 bytes. Any excess is truncated.
		NT log opcode ^{#2}	A9	The opcode. The content of the OpCode field in the Event Viewer. Maximum 256 bytes. Any excess is truncated.
		Platform	PLATFORM	NT
		Program name	PPNAME	For a remote monitoring event log trap /HITACHI/JP1/IM/ REMOTE_MONITORING/ EVENTLOGTRAP For a JP1/Base event log trap /HITACHI/JP1/NTEVENT_LOGTRAP
		Windows version number ^{#2}	OS_VERSION	Major Windows version number
		Source host name ^{#3}	JP1_SOURCEHOST	The host that issues the JP1 event
		Trap name ^{#4}	JP1_TRAP_NAME	The trap name specified in the action definition file for event log trapping

#1: 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.

#2: This information is created if you specify the `ext-attr-option` parameter in the action definition file for event log trapping. It is not created if you do not specify the `ext-attr-option` parameter.

#3: This information is created when you specify 00000001 for the "ATTR_EVENT_LOGTRAP_SOURCEHOST" common definition attribute in a JP1/IM - Manager common definition settings file for a remote monitoring event log trap. For details on the common definition settings file for JP1/IM - Manager, see the manual *JP1/Integrated Management 3 - Manager Command and Definition File Reference*.

#4: This information is created if you specify the `trap-name` parameter in the filter of the action definition file for event log trapping. It is not created if you do not specify the `trap-name` parameter.

(27) Details about event IDs specified in the ACTDEF parameter in the action definition file for log file trapping

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	Value specified in the ACTDEF parameter
		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	<p>In Windows:</p> <ul style="list-style-type: none"> If the <code>-p</code> option is specified in the <code>jevlogstart</code> command or as an additional option in the Display/Edit Profiles window of JP1/IM: <code>/HITACHI/JP1/ NT_LOGTRAP/program-name</code> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. If the <code>-p</code> option is not specified in the <code>jevlogstart</code> command or as an additional option in the Display/Edit Profiles window of JP1/IM: <code>/HITACHI/JP1/NT_LOGTRAP</code> <p>In UNIX:</p> <ul style="list-style-type: none"> If the <code>-p</code> option is specified in the <code>jevlogstart</code> command or as an additional option in the Display/Edit Profiles window of JP1/IM: <code>/HITACHI/JP1/ UX_LOGTRAP/program-name</code> <i>program-name</i> is the name of the source program that output the log data, as specified in the <code>-p</code> option. If the <code>-p</code> option is not specified in the <code>jevlogstart</code> command or as an additional option in the Display/Edit Profiles window of JP1/IM: <code>/HITACHI/JP1/UX_LOGTRAP</code>
		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

Attribute type		Item	Attribute name	Contents
	Program-specific information	Platform	PLATFORM	In Windows: NT In UNIX: UNIX
		Program name	PPNAME	For a remote monitoring log file trap /HITACHI/JP1/IM/ REMOTE_MONITORING/LOGTRAP For a JP1/Base log file trap <ul style="list-style-type: none"> In Windows: /HITACHI/JP1/NT_LOGTRAP In UNIX: /HITACHI/JP1/UX_LOGTRAP
		Host name	JP1_SOURCEHOST	The host that generates the log entry
		Monitor ID	JP1_TRAP_ID	ID number of the log file trap
		Monitoring target name	JP1_TRAP_NAME	Monitoring target name [#]

[#]: This item is output only when the `-a` option is specified for the `jevlogstart` command.

(28) Details about event ID 00003FA0

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA0
		Message	--	KAVB2100-I [<i>host-name:JP1-user-name</i>] Command execution started.
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
		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

(29) Details about event ID 00003FA1

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA1

Attribute type		Item	Attribute name	Contents
		Message	--	KAVB2101-I [<i>host-name:JP-user-name</i>] 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
		Command execution	EXECCMD	Command executed

(30) Details about event ID 00003FA2

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA2
		Message	--	KAVB2102-E [<i>host-name:JP1-user-name</i>] 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
		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.

(31) Details about event ID 00003FA3

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA3
		Message	--	KAVB2402-W [<i>host-name</i>] The execution time of command execution exceeded the regulation value (<i>number</i> sec)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCOCMD

Attribute type		Item	Attribute name	Contents
		Object type	OBJECT_TYPE	<ul style="list-style-type: none"> 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
		Command ID	COMMANDID	Command ID
		Execution time	EXEC_TIME	Time when the command was executed

(32) Details about event ID 00003FA5

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA5
		Message	--	KAVB2071-W In <i>destination-host</i> , the number of queued commands requested from <i>source-host-name</i> has exceeded the threshold (<i>xx</i>).
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

(33) Details about event ID 00003FA6

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA6
		Message	--	KAVB2072-I In the <i>target-host</i> , the number of queued commands

Attribute type		Item	Attribute name	Contents
				requested from the <i>source-host</i> 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

(34) Details about event ID 00003FA7

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003FA7
		Message	--	KAVB2641-E Restoration of the command execution log file failed.
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCOCMD
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCOCMD
		Occurrence	OCCURRENCE	Error

(35) Details about event ID 00004700

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004700
		Message	--	KAVA1524-W <i>connection-sequence: authentication-server-name</i> was successfully blocked.
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

Attribute type		Item	Attribute name	Contents
	Program-specific information	Target host name for failed connection	AUTHSRV_NAME	Name of the authentication server which has been blocked

(36) Details about event ID 00004701

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004701
		Message	--	KAVA1525-I <i>connection-sequence: authentication-server-name</i> 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

(37) 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	

(38) Details about event ID 00004720

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004720
		Message	--	KAVB3737-E The <i>component-name management-target-process-name</i> terminated abnormally.
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/BASE/SPMD

Attribute type		Item	Attribute name	Contents
		Object type	OBJECT_TYPE	SPMD
		Object name	OBJECT_NAME	Name of the abnormally ended process
		Occurrence	OCCURRENCE	NOTICE

(39) Details about event ID 00004721

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004721
		Message	--	KAVB3613-W <i>component-name</i> timeout occurred in <i>management-target-process-name</i> . 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

(40) Details about event ID 00004722

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004722
		Message	--	KAVB3616-I Restart of the <i>component-name management-target-process-name</i> 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

(41) Details about event ID 00004724

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004724
		Message	--	KAVB3664-I JP1/Base has started on the host <i>host-name</i> .
Extended attribute	Common information	Event level	SEVERITY	Notice
		Product name	PRODUCT_NAME	/HITACHI/JP1/BASE/SPMD
		Object type	OBJECT_TYPE	SPMD

Attribute type		Item	Attribute name	Contents
		Object name	OBJECT_NAME	The host that was started
		Occurrence	OCCURRENCE	NOTICE

Note: This JP1 event is forwarded to every destination host in the forwarding settings file (`forward`) even if it does not match the conditions of the event filter. If you do not want this event to be forwarded, define an exclusion condition or specify the `auto-forward-off` flag in the `options` parameter of the event server settings file (`conf`).

(42) Details about event ID 00004725

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004725
		Message	--	KAVB3665-I JP1/Base will now end on the host <i>host-name</i> .
Extended attribute	Common information	Event level	SEVERITY	Notice
		Product name	PRODUCT_NAME	/HITACHI/JP1/BASE/SPMD
		Object type	OBJECT_TYPE	SPMD
		Object name	OBJECT_NAME	The host on which JP1/Base will stop
		Occurrence	OCCURRENCE	NOTICE

Note: This JP1 event is forwarded to every destination host in the forwarding settings file (`forward`) even if it does not match the conditions of the event filter. If you do not want this event to be forwarded, define an exclusion condition or specify the `auto-forward-off` flag in the `options` parameter of the event server settings file (`conf`).

(43) Details about event ID 00004740

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004740
		Message	--	KAVA7017-E <i>function-name</i> ended abnormally. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)
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

(44) Details about event ID 00004741

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004741
		Message	--	KAVA7014-E <i>function-name</i> has been processing for nn seconds. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)
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

(45) Details about event ID 00004742

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004742
		Message	--	KAVA7013-W <i>function-name</i> has been processing for nn seconds. After passes of mm seconds, becomes error condition. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)
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

Attribute type	Item	Attribute name	Contents
	Thread ID	THREAD_ID	Thread ID

(46) Details about event ID 00004743

Attribute type	Item	Attribute name	Contents	
Basic attribute	Event ID	--	00004743	
	Message	--	KAVA7016-I <i>function-name</i> has a normal status. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)	
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

(47) 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= <i>host-name</i>)	
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

(48) Details about event ID 00004748

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004748

Attribute type		Item	Attribute name	Contents
		Message	--	KAVA7222-E Monitoring notification cannot be performed at <i>host-name</i> because <i>service-name</i> 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

(49) 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 <i>host-name</i> cannot be established. (<i>reason-message: detailed information</i>)
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

(50) Details about event ID 0000474A

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0000474A
		Message	--	KAVA7224-I <i>host-name</i> 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

(51) 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 = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)
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

(52) Details about event ID 0000474C

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0000474C
		Message	--	KAVA7228-I The host <i>host-name</i> will not be monitored because it is not running.
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	Name of the host that will not be monitored
		Occurrence	OCCURRENCE	NOTICE

(53) Details about event ID 0000474D

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0000474D
		Message	--	KAVA7229-W Monitoring cannot be performed because a connection cannot be established with <i>host-name</i> , which is not receiving stop

Attribute type		Item	Attribute name	Contents
				notifications. (<i>reason-message: detailed information</i>)
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	Name of the host that cannot be monitored
		Occurrence	OCCURRENCE	NOTICE

(54) Details about event ID 0000474E

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0000474E
		Message	--	KAVA7032-W The status of <i>function-name</i> cannot be confirmed. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)
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	Name of the function
		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

(55) Details about event ID 0000474F

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0000474F
		Message	--	KAVA7033-E The status of <i>function-name</i> still cannot be confirmed. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)

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

(56) Details about event ID 00004750

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004750
		Message	--	KAVA7034-I The status of <i>function-name</i> can now be confirmed. (host name = <i>host-name</i> , process name = <i>process-name</i> , internal function name = <i>internal-function-name</i> , pid = <i>process-ID</i> , tid = <i>thread-ID</i>)
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

(57) 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.

Attribute type		Item	Attribute name	Contents
				(actno=action-number, actnm=action-name, host=execution-host-name, eventid=event-ID, eventseq=serial-number)
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)

#: A null character is used if not executed.

(58) 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)
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.

Attribute type		Item	Attribute name	Contents
		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)

[#]: A null character is used if not executed.

(59) 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)	

Attribute type	Item	Attribute name	Contents
	Error code	ERR_CODE	Error number of the cause of execution failure

#: A null character is used if the attribute is not used or is undefined.

(60) 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
	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)

#: A null character is used if the attribute is not used or is undefined.

18

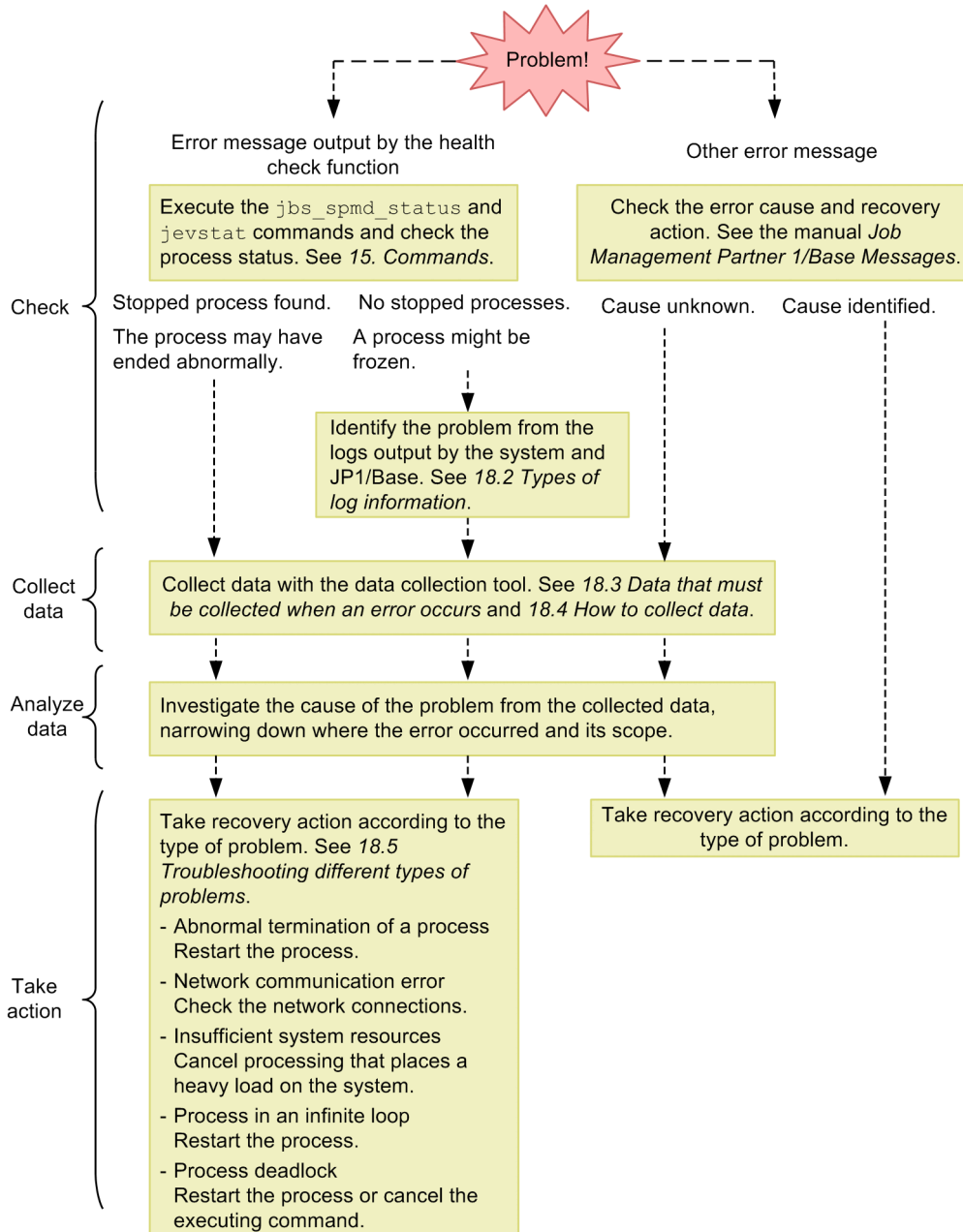
Troubleshooting

This chapter explains the type of problems that might occur in JP1/Base and how to recover from such problems.

18.1 Troubleshooting procedure

The figure below shows the recovery procedure if a problem occurs in JP1/Base.

Figure 18–1: Recovery procedure when a problem occurs



18.2 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.

18.2.1 Common message log information

The common message log information reports problems in the system for system administrators. This log information reports the minimum information about a problem.

The common message log information is output to syslog for UNIX and to the Windows event log for Windows.

Furthermore, in SUSE Linux 15 or later, by default, log information is to be output to log files known as journals only, not to syslog. To output common message log information to syslog, syslog output must be enabled. For details about how to enable syslog output, see [3.4.8 Syslog output when SUSE Linux 15 or later](#).

18.2.2 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 output destination for the integrated trace log is as follows:

In Windows:

```
system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log  
system-drive\Program Files\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log
```

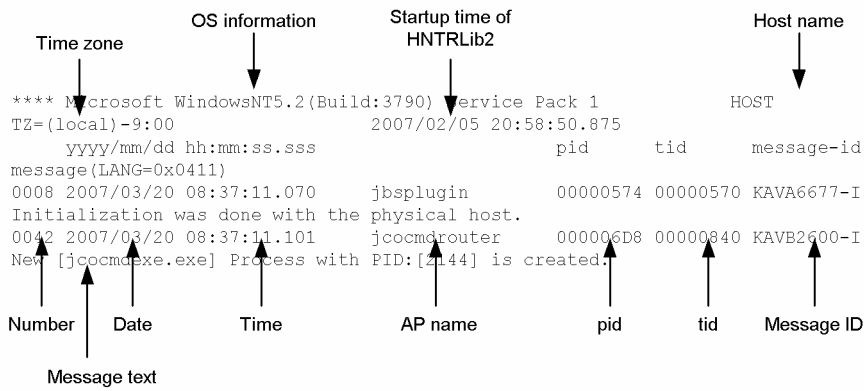
In UNIX:

```
/var/opt/hitachi/HNTRLib2/spool/hntr2{1|2|3|4}.log
```

You can use either the `hntr2utl2`, `hntr2conf`, or `hntr2getconf` command to view or change the log file destination or size. For details, see [hntr2utl2 \(Windows only\)](#), [hntr2utl2 \(UNIX only\)](#), [hntr2conf](#), or [hntr2getconf](#) in *15. 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 18–2: Output example of integrated trace log file



The following tables describe headers and items output to the integrated trace log file.

Table 18–1: Headers for the integrated trace log file

Header	Description
OS information	Information on the OS on which Hitachi Network Objectplaza Trace Library (HNTRLlib2) is running
host-name	Name of the host on which Hitachi Network Objectplaza Trace Library (HNTRLlib2) 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 (HNTRLlib2)	Time at which Hitachi Network Objectplaza Trace Library (HNTRLlib2) started

Table 18–2: 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: <i>yyyy/mm/dd</i> (year/month/day)
Time (12 bytes)	Trace acquisition time (local time): <i>hh:mm:ss.sss</i> (hour: minute: second. millisecond)
AP name (maximum of 16 bytes)	Application identification name. <ul style="list-style-type: none"> Process management JBS_SPM Startup control JP1ControlSvc Authentication access control jp1BsSess Operation access control jp1BsAcl Authentication server jbsessionmgr Configuration management jbsroute

Output item	Description
	<ul style="list-style-type: none"> • 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) jbsbcd • Health check (for other host monitoring) jbsbhostd • Event service jevservice • JP1/AJS-compatible process jevsessvc • Log file trap (Windows) jevtraplog • Log file trap (UNIX) jevlogd • Event log trap jevtrapevt • Other command names <i>Command name</i>
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.

Important

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.

18.2.3 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 [18.2.5 Log files and directories](#).

18.2.4 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 [I. Operation Log Output](#).

18.2.5 Log files and directories

(1) In Windows

For details on the type of log information output by JP1/Base for Windows, and a 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 a list of default log files, see [A.2\(2\) List of log files \(in UNIX\)](#).

18.3 Data that must be collected when a problem 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 15. *Commands*.

In the following tables, the data that can be collected using the initial settings of the data collection tool is indicated as such.

18.3.1 Data that must be collected when a problem occurs (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 <code>date /t</code> Execution result of <code>time /t</code>	<code>date.log</code>
Windows event log	Application log: <code>system-folder\system32\config\AppEvent.Evt</code> System log: <code>system-folder\system32\config\SysEvent.Evt</code>	<ul style="list-style-type: none">• <code>SysEvent (Backup).evt</code>• <code>AppEvent (Backup).evt</code>
Host names set on the machine	<code>system-folder\system32\drivers\etc\hosts</code>	<code>hosts</code>
Service ports set on the machine	<code>system-folder\system32\drivers\etc\services</code>	<code>services</code>
NICs installed	Execution result of <code>ipconfig /all</code>	<code>ipconfig.log</code>
List of services started	Execution result of <code>net start</code>	<code>netstart.log</code>
Machine environment variable	Execution result of <code>set</code>	<code>set.log</code>
Dr. Watson log file ^{#2}	<code>user-specified-folder\drwtsn32.log</code>	<code>drwtsn32.log</code>
Crash dump ^{#2}	<code>user-specified-folder\user.dmp</code>	<code>user.dmp</code>
Machine system information	Execution result of <code>msinfo32 /report file-name</code>	<code>msinfo32.log</code>
User right assignment	Execution result of <code>secedit /export /cfg file-name/areas USER_RIGHTS /quiet</code>	<code>secedit.log</code>
Group policy	Execution result of <code>gpresult /z</code>	<code>gpresult.log</code>
Range of the dynamic ports (IPv4)	Execution result of <code>netsh int ipv4 show dynamicporttcp</code>	<code>dynamicport_ipv4.log</code>
Range of the dynamic ports (IPv6)	Execution result of <code>netsh int ipv6 show dynamicporttcp</code>	<code>dynamicport_ipv6.log</code>
Routing information	Execution result of <code>netstat -rn</code>	<code>netstat_rn.log</code>

^{#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 about the specification method, see [4.7 Preparing to collect information when a problem occurs \(Windows only\)](#). For details on the setting, see [4.7 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 information	Required data	File name ^{#1}
Environment settings	All files in <i>installation-folder</i> \conf	Same as the name of the file from which the data is collected.
	All files in <i>installation-folder</i> \default\	Same as the name of the file from which the data is collected.
	All files in <i>installation-folder</i> \plugin\conf\	Same as the name of the file from which the data is collected.
	All files in <i>shared-folder</i> \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 <i>logical-host-name</i> ^{#2}	
Log information	All files in <i>installation-folder</i> \log\	Same as the name of the file from which the data is collected.
	All files in <i>shared-folder</i> \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}	Same as the name of the file from which the data is collected.
	All files in %ALLUSERSPROFILE%\Hitachi\jp1\ <i>logical-host-name</i> \JP1Base\log\ ^{#4}	Same as the name of the file from which the data is collected.
Log of installation	<i>Windows-installation-folder</i> \Temp\jp1common\jp1base\hliclib*.log	Same as the name of the file from which the data is collected.
	All files in <i>Windows-installation-folder</i> \TEMP\RF\	Same as the name of the file from which the data is collected
Service operating information	All files in <i>installation-folder</i> \sys\OPI\	Same as the name of the file from which the data is collected.
	All files in <i>shared-folder</i> \jp1base\sys\OPI\	Same as the name of the file from which the data is collected.
Event service settings	All files in <i>installation-folder</i> \sys\tmp\event\	Same as the name of the file from which the data is collected.
	All files in <i>shared-folder</i> \jp1base\event\ ^{#2}	Same as the name of the file from which the data is collected.
Event database	All files in <i>installation-folder</i> \sys\event\ ^{#3}	Same as the name of the file from which the data is collected.
	All files in <i>shared-folder</i> \jp1base\event\ ^{#2, #3}	Same as the name of the file from which the data is collected.
Command execution log	All files in <i>installation-folder</i> \log\COMMAND ^{#3}	Same as the name of the file from which the data is collected.

Type of information	Required data	File name#1
	All files in <i>shared-folder</i> \jplbase\log\Command\#2,#3	Same as the name of the file from which the data is collected.
Integrated trace log	<i>system-drive</i> \Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2*.log <i>system-drive</i> \Program Files\Hitachi\HNTRLib2\spool\hntr2*.log	Same as the name of the file from which the data is collected.
File list	Execution result of <code>dir /s installation-folder</code>	dir_jplbase.log
	Execution result of <code>dir /s shared-folder\jplbase</code>	dir_jplbase.log
Version information	<i>system-drive</i> \Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ilg, setup.ini	base_setup.ilg, base_setup.ini
Patch log	<i>installation-folder</i> \Patchlog.txt	Patchlog_jplbase.txt
JP1/Base binding status	Execution result of <code>netstat -nao</code>	netstat.log
Host name for resolving the network address	Execution result of <code>jbsgethostbyname</code>	jbsgethostbyname.log
Access permissions for folders	Execution result of <code>cacls-installation-folder</code>	cacls_jplbase.log
	Execution result of <code>cacls-shared-folder\jplbase</code>	
	Execution result of <code>cacls-installation-folder\log</code>	cacls_jplbase_log.log
	Execution result of <code>cacls-shared-folder\jplbase\log</code>	
	Execution result of <code>cacls-installation-folder\log\COMMAND</code>	cacls_jplbase_log_COMMAND.log
	Execution result of <code>cacls-shared-folder\jplbase\log\COMMAND</code>	
	Execution result of <code>cacls-installation-folder\sys</code>	cacls_jplbase_sys.log
	Execution result of <code>cacls-installation-folder\sys\event</code>	cacls_jplbase_sys_event.log
	Execution result of <code>cacls-installation-folder\sys\event\servers</code>	cacls_jplbase_sys_event_servers.log
	Execution result of <code>cacls-installation-folder\sys\event\servers\default</code>	cacls_jplbase_sys_event_servers_default.log
	Execution result of <code>cacls-shared-folder\jplbase\event</code>	cacls_jplbase_event.log
Hitachi Integrated Installer log files	All files in <i>Windows-installation-folder</i> \Temp\HCDINST\	Copies of the files that are shown in the left column
Product information log	<i>system-drive</i> \Program Files\Hitachi\jplcommon\jplbase\jplbase.dat	Same as the name of the file from which the data is collected.
jplhosts2 information	All files in <i>installation-folder</i> \sys\jplhosts2\	Same as the name of the file from which the data is collected.
	All files in <i>shared-folder</i> \jplbase\sys\jplhosts2\#2	Same as the name of the file from which the data is collected.

Type of information	Required data	File name#1
	Execution result of <code>jbshosts2export</code>	<code>jbshosts2export_JP1_DEF AULT.log</code>
Exclusive control type of the integrated trace log	Execution result of <code>hntr2getconf -t</code>	<code>hntr2conf_f.log</code> , <code>hntr2x64conf_f.log</code>
Settings of the integrated trace log	Execution result of <code>hntr2getconf -f -b -n -s -w</code>	<code>hntr2conf_f.log</code> , <code>hntr2x64conf_f.log</code>
Product number and version information	<code>installation-folder\Version.txt</code>	Same as the name of the file from which the data is collected
License type information	<code>installation-folder\ProductInfo.txt</code>	Same as the name of the file from which the data is collected
Common definition information backup file	All files in <code>Windows-installation-folder\Temp\JP1_COMDEF\</code>	Same as the name of the file from which the data is collected

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.

(3) JP1/Base processes

Use the Windows task manager to check the operation status of processes.

(4) Operation data

If a problem 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

If the JP1/Base process stops due to an application error, collect the user dumps.

(7) Collecting problem reports

If the JP1/Base process stops due to an application error, collect the problem reports.

18.3.2 Data that must be collected when a problem occurs (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 (AIX)#2 /var/log/messages (Linux)#2#3	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
Network interface status information	Execution result of <code>-ip link</code> (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15) Execution result of <code>netstat -in</code> (for OSs other than the above)	jp1_default_base_1st.tar.Z, netstat_in.log
List of processes	Execution result of <code>ps -elfa</code>	jp1_default_base_1st.tar.Z, ps.log
Machine environment variable	Execution result of <code>env</code>	jp1_default_base_1st.tar.Z, env.log
Kernel parameter information	AIX: Execution result of <code>lsattr -E -l sys0</code> Execution result of <code>ulimit -a</code> /etc/security/limits#3 Linux: Execution result of <code>/sbin/sysctl -a</code> Execution result of <code>ulimit -a</code>	jp1_default_base_1st.tar.Z AIX: lsatt.log ulimit.log limits Linux: sysctl.log ulimit.log
Page size information	Execution result of <code>pagesize</code> (AIX) Not collected in Linux	jp1_default_base_1st.tar.Z, pagesize.log
Shared memory information	Execution result of <code>ipcs -a</code>	jp1_default_base_1st.tar.Z, ipcs.log

Type of information	Required data	File name ^{#1}
Memory information	Execution result of <code>lspcs -s</code> (AIX) <code>cat /proc/meminfo</code> (Linux)	jp1_default_base_1st.tar.Z, swapinfo.log
Disk information	Execution result of <code>df -k</code>	jp1_default_base_1st.tar.Z, df.log
System diagnostics	Execution result of <code>/usr/bin/alog -o -t boot</code> (AIX) ^{#3} Execution result of <code>/bin/dmesg</code> (Linux)	jp1_default_base_1st.tar.Z, sys_info.log
OS patches implemented	AIX: <code>lslpp -l -a</code> <code>/usr/bin/instfix -a -icv</code> Linux: <code>/bin/rpm -qa</code>	jp1_default_base_1st.tar.Z, patch_info.log
OS version information	Execution result of <code>uname -a</code>	jp1_default_base_1st.tar.Z, uname_a.log
Installed Hitachi products	<code>/etc/.hitachi/pplistd/pplistd</code>	jp1_default_base_1st.tar.Z, pplistd
Host name for resolving the network address	Execution result of <code>jbsgethostbyname</code>	jp1_default_base_1st.tar.Z, jbsgethostbyname.log
Linux release information	<code>/etc/redhat-release</code> (Linux) [#] #: Only collected if it exists.	jp1_default_base_1st.tar.Z, redhat-release
	<code>/etc/os-release</code> (Linux)	jp1_default_base_1st.tar.Z, os-release
Name service settings file	<code>/etc/netsvc.conf</code> (AIX) <code>/etc/nsswitch.conf</code> (Linux)	jp1_default_base_1st.tar.Z, netsvc.conf (AIX), nsswitch.conf (Linux)
DNS server settings file	<code>/etc/resolv.conf</code>	jp1_default_base_1st.tar.Z, resolv.conf
Network interface settings	Execution result of <code>ifconfig -a</code>	jp1_default_base_1st.tar.Z, ifconfig.log
Routing information	Execution result of <code>ip route</code> (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15) Execution result of <code>netstat -rn</code> (for OSs other than the above)	jp1_default_base_1st.tar.Z, netstat_rn.log
journal	Result of executing the <code>journalctl -l --no-pager</code> command ^{#4}	jp1default_base_1st.tar.Z, journal.log

#1: Names of the compressed file and expanded file after execution of the data collection tool (listed in that order). In Linux, the extension is `gz`.

#2: The syslog file might have a different name.

#3: The data collection tool does not have sufficient rights to collect this information when executed by a user with JP1/Base administrator privileges.

#4: Journal logs are output as text.

`-l` option : Output is not truncated.

`--no-pager` option: Output is not piped to a pager.

(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	Collected information	File name
Environment settings	All files in <code>/etc/opt/jp1base/conf/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>/etc/opt/jp1base/default/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>/opt/jp1base/plugin/conf/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>shared-directory/jp1base/conf#1</code>	<code>logical-host-name_1st.tar.Z</code> , same as the name of the file from which data is collected
Common definition information	<code>/opt/jp1/hcclibcnf/</code> (can also be checked from the <code>jbgsgetcnf</code> command execution result)	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>/etc/opt/jp1base/default/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
Log information	All files in <code>/var/opt/jp1base/log/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	<code>shared-directory/jp1base/log#1#2</code>	<code>logical-host-name_base_1st.tar.Z</code> , same as the name of the file from which data is collected
Log of installation	<code>/tmp/HITACHI_JP1_INST_LOG/</code> <code>jp1base_inst{1 2 3 4 5}.log</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	<code>/etc/.hitachi/.hliclog/</code> <code>hliclib*{1 2 3 4 5}.log</code>	Same as the name of the file from which data is collected
	<code>/etc/.hitachi/.hliclog/hliccmd{1 2 3 4 5}.log</code>	Same as the name of the file from which data is collected
	<code>/tmp/rf/</code> <code>hrf4securityinstall{1 2}.log</code>	Same as the name of the file from which data is collected
	All files in <code>/tmp/rf/</code>	Same as the name of the file from which data is collected
Service operating information	All files in <code>/var/opt/jp1base/sys/OPI/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>shared-directory/</code> <code>jp1base/sys/OPI/</code>	<code>logical-host-name_base_1st.tar.Z</code> , same as the name of the file from which data is collected
Event service settings	All files in <code>/var/opt/</code> <code>jp1base/sys/tmp/event/</code>	<code>jp1_default_base_1st.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>shared-directory/event/#1</code>	<code>logical-host-name_base_1st.tar.Z</code> , same as the name of the file from which data is collected
Event database	All files in <code>/var/opt/</code> <code>jp1base/sys/event/</code>	<code>jp1_default_base_2nd.tar.Z</code> , same as the name of the file from which data is collected
	All files in <code>shared-directory/event/#1</code>	<code>logical-host-name_base_2nd.tar.Z</code> , same as the name of the file from which data is collected

Type of information	Collected information	File name
Command execution log	All files in /var/opt/ jplbase/log/COMMAND	jpl_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	All files in <i>shared-directory</i> / jplbase/log/COMMAND	jpl_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_spmc_status	jpl_default_base_1st.tar.Z, jbs_spmc_status.log
	Execution result of jbs_spmc_status - h <i>logical-host-name</i> ^{#1}	jpl_default_base_1st.tar.Z, jbs_spmc_status_ <i>logical-host-name</i> .log
Process operating status of event service	Execution result of jevstat command	jpl_default_base_1st.tar.Z, jevstat.log
	Execution result of jevstat <i>logical-host-name</i> ^{#1}	jpl_default_base_1st.tar.Z, jevstat_ <i>logical-host-name</i> .log
Integrated trace log file	/var/opt/hitachi/HNTRLib2/ spool/hntr2*.log	jpl_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/jplbase/log/COMMAND Logical host specified: <i>shared-directory</i> /jplbase/log/COMMAND	Physical host specified: jpl_default_base_1st.tar.Z, com.jischk.log Logical host specified: jpl_default_base_1st.tar.Z, com.jischk_ <i>logical-host-name</i> .log
Core file diagnostics ^{#3, #5, #6}	Execution result of car command (results of analyzing core files in /var/opt/jplbase/ and /opt/jplbase/)	jpl_default_base_2nd.tar.Z, core_ <i>module-name</i> .log jpl_default_base_2nd.tar.Z, core_ <i>module-name</i> _car.tar.Z (core_ <i>module-name</i> _car.tar in Linux 9 and later)
File list	Execution result of ls command ls -lRa /opt/jplbase ls -lRa /etc/opt/jplbase ls -lRa /var/opt/jplbase	jpl_default_base_1st.tar.Z, inst_dir.log
	Execution result of ls command ^{#1} ls -lRa <i>shared-directory</i> /jplbase ls -lRa <i>shared-directory</i> /event	jpl_default_base_1st.tar.Z, share_dir.log
Patch log	/opt/jplbase/PatchInfo	jpl_default_base_1st.tar.Z, PatchInfo
Patch log information	/opt/jplbase/PatchLog	jpl_default_base_1st.tar.Z, PatchLog
JP1/Base binding status	Execution result of ss -nap (for Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15) Execution result of netstat -na (for AIX)	jpl_default_base_1st.tar.Z, netstat_na.log
jplhosts2 information	All files in /var/opt/ jplbase/sys/jplhosts2/	jpl_default_base_1st.tar.Z, same as the name of the file from which data is collected
	All files in <i>shared-directory</i> /jplbase/sys/ jplhosts2/ ^{#1}	<i>logical-host-name</i> _base_1st.tar.Z, same as the name of the file from which data is collected

Type of information	Collected information	File name
	Execution result of <code>jbshosts2export</code>	<code>jp1_default_base_1st.tar.Z</code> , <code>jbshosts2export_JP1_DEFAULT.log</code>
	Execution result of <code>jbshosts2export -h logical-host-name#1</code>	<code>logical-host-name_base_1st.tar.Z</code> , <code>jbshosts2export_logical-host-name.log</code>
JP1/Base administrator settings#4	Execution result of <code>jbssetadmingrp -v</code>	<code>jp1_default_base_1st.tar.Z</code> , <code>jbssetadmin.log</code>
Exclusive control type of the integrated trace log	Execution result of <code>hntr2getconf -t</code>	<code>hntr2getconf_t.log</code>
Settings of the integrated trace log	Execution result of <code>hntr2getconf -f -b -n -s -w</code>	<code>hntr2getconf_f.log</code>
Common definition information backup file	All files in <code>/tmp/JP1_COMDEF/</code>	Same as the name of the file from which data is collected

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.

```
jbbs_log.sh (any-option) [directory-specified-in-the-index-file]
```

```
jbbs_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: Note the following when using Linux:

In Linux, the maximum size for core file dumps will sometimes be set to 0 by default. In this case, the system will not output a core dump file. To avoid this issue, the `jbbs_start` and `jbbs_start.cluster` scripts contain the following standard setting:

```
if [ 'uname' = Linux ]; then
ulimit -c unlimited
fi
```

If this setting contravenes the security policy of the system on which the script is executed, comment it out by placing a hash mark (#) at the beginning of each line. This invalidates the setting. However, it also means that the system will not create a core dump file when an event such as a segmentation fault or bus error that would usually trigger a core dump occurs in the JP1/Base process, denying you information you might use to investigate the cause.

```
#if [ 'uname' = Linux ]; then
#ulimit -c unlimited
#fi
```

#4: The data collection tool does not have sufficient rights to collect this information when executed by a user with JP1/Base administrator privileges.

#5: As for the core dump file related ABRT settings (Linux only), note the following:

Under the Linux where an automated bug reporting tool (ABRT) is installed, if the ABRT settings constrain processes, OS account users, or user groups from creating a core dump file, no core dump file will be created when an event such as a segmentation fault or bus error that would usually trigger the creation of a core dump file occurs in a JP1/Base process. Hence, no investigation can be made.

Review your ABRT settings to meet your operation not to constrain OS account users, user groups, or processes to run JP1/Base from creating a core dump file. For details, see *the documentation for your Linux*.

#6: When collecting data in an environment of Red Hat Enterprise Linux 8 or later, by the default settings the analysis information of the core file output before restarting the system cannot be collected. If you want to collect the analysis information of the core file output before restarting the system, use the following procedure to make the journal persistent before starting JP1/Base.

1. Open the `/etc/systemd/journald.conf` file in an editor.

```
[...]
[Journal]
Storage=persistent
#Compress=yes
:
```

2. Restart `systemd-journald`.

```
systemctl restart systemd-journald
```

(3) Operation data

If a problem 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.)

18.4 How to collect data

18.4.1 How to collect data (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 value. 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*\jplbase\log\ (maximum 45 MB^{#1})

f

Data size of *shared-folder*\jplbase\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 value. 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 *jp1_default* folder is created in the directory you specified in *data-folder*. If you specify the *-h* option, in addition to the *jp1_default* 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 *15. Commands*.

(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 ^{#1}	--	--
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 <i>jbssessionmgr</i> when the

Parent process name	Function	Child process name	Function
			jbs_spm�_status command is executed.
		jbsroute.exe (1)	Configuration management ^{#1, #3} The displayed name is jbsroute when the jbs_spm�_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_spm�_status command is executed.
		jbsplugind.exe	Plug-in service ^{#1, #3} The displayed name is jbsplugin when the jbs_spm�_status command is executed.
		jbshcd.exe (1)	Health check (for local host monitoring) ^{#1, #3} The displayed name is jbshcd when the jbs_spm�_status command is executed.
		jbshchostd.exe (1)	Health check (for remote host monitoring) ^{#1, #3} The displayed name is jbshchostd when the jbs_spm�_status command is executed.
		jbssrvmgr.exe (1)	Service management control function ^{#1, #3} The displayed name is jbssrvmgr when the jbs_spm�_status command is executed.
		jbslact.exe (1)	Local action function ^{#1, #3} The displayed name is jbslact when the jbs_spm�_status command is executed.
		jbscomd.exe (1) jbscomd_api.exe (1) 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_spm�_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}	--	--
jevtraplog.exe (1)	Log file trap	--	This process is generated only when the log file trapping function is used.

Parent process name	Function	Child process name	Function
jevtrapevt.exe (1)	Event log trap	--	This process is generated only when the event log trapping function 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: $(number-of-logical-hosts + 1) \times number-of-processes$

#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:

```
jbsessionmgr
jbsroute
jcocmd
jbsplugin
jbshcd
jbshchostd
jbsrvmgr
jbslcact
jbscomd
```

- If an authentication server has not been set:

```
jbsroute
jcocmd
jbsplugin
jbshcd
jbshchostd
jbsrvmgr
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 a problem 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 problem reports

When an application error causes the JP1/Base process to stop, perform the following actions to collect a problem report:

1. In the Control Panel, click **Action Center**.
2. Click **Maintenance**.
3. Under **Check for solutions to problem reports**, click **View reliability history**.
4. Click **View all problem report**.
5. Click the appropriate problem.
6. Click **Copy to clipboard**.
7. Paste the clipboard into a file such as a text file, and then save the file.

18.4.2 How to collect data (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:

$$\text{Data size} = 3 + a + b + (60 \times c) \text{ MB}$$

a

Size of all the files in `/var/opt/jplbase/` (maximum 508 MB^{#1, #2})

b

Size of the core files under `/` (only if output)

c

Number of core files under `/`, and in the `/var/opt/jplbase/` or `/opt/jplbase/` directory

#1: An extra 254 MB is required if you are running JP1/IM - Manager on the same host.

#2: This is the default value. 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:

$$\text{Data size} = 3 + a + b + (60 \times c) + d + e \text{ (MB)}$$

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 value. 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 *15. Commands*.

(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}	jbsessionmgr (1)	Authentication server ^{#1, #4} This process exists only on the host that is set as the authentication server. The displayed name is jbsessionmgr 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)	Command execution ^{#1, #4}

Parent process name	Function	Child process name	Function
		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)	The displayed name is jcocmd when the jbs_spmc_status command is executed.
		jbsplugind#5	Plug-in service#1, #4 The displayed name is jbsplugin when the jbs_spmc_status command is executed.
		jbshcd (1)	Health check (for local host monitoring)#1, #4 The displayed name is jbshcd when the jbs_spmc_status command is executed.
		jbshchostd (1)	Health check (for remote host monitoring)#1, #4 The displayed name is jbshchostd when the jbs_spmc_status command is executed.
		jbssrvmgr (1)	Service management control function#1, #4 The displayed name is jbssrvmgr when the jbs_spmc_status command is executed.
		jbslcact (1)	Local action function#1, #4 The displayed name is jbslcact when the jbs_spmc_status command is executed.
		jbscomd (1) jbscomd_api (1) jbscomd_ses (1) jbscomd_snd (1) jbscomd_rcv (1)	Inter-process communication#1, #4 The displayed name is jbscomd when the jbs_spmc_status command is executed.
jevservice (1)	Event service#1, #6	jevservice (5 to 9,999)	Event service
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.

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: $(\text{number-of-logical-hosts} + 1) \times \text{number-of-processes}$

#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_spmc_status command to check the status of these processes. If the processes are running normally, the jbs_spmc_status command returns the following information.

- If an authentication server has been set:
 - jbssessionmgr
 - jbsroute
 - jcocmd

```
jbsplugin  
jbsbcd  
jbsbhostd  
jbsbrvmgr  
jbslcact  
jbscomd
```

- If an authentication server has not been set:

```
jbsroute  
jcoamd  
jbsplugin  
jbsbcd  
jbsbhostd  
jbsbrvmgr  
jbslcact  
jbscomd
```

#5: The process name displayed by the `ps-e1` 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
```

(3) Check the operation data

If a problem 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.

18.5 Troubleshooting different types of problems

This section describes how to troubleshoot different types of problems.

18.5.1 Problems in Windows or UNIX

(1) A large number of 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 the occurrence of large numbers of events causes too much load on the system or affects job processing, it might be absolutely necessary to stop the JP1 events from being forwarded. In such cases, use the event-forwarding suppression command (`jevagtfw`) to suppress forwarding of the JP1 events. For details on event forwarding suppression using the `jevagtfw` command, see [2.5.3 Using a manager to suppress event forwarding from an agent with large numbers of JP1 events](#). For details on the `jevagtfw` command, see [jevagtfw in 15. Commands](#).

If the event-forwarding suppression command (`jevagtfw`) cannot be used in your environment, initialize the event database on the event server from which the JP1 events were forwarded. 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 [10.2 Initializing the event database](#).

To prevent the generation of large numbers of JP1 events, adjust the JP1 event forwarding conditions in the forwarding settings file (`forward`). You can also set a threshold to detect large numbers of events, and automatically suppress event forwarding. For details on the threshold-based suppression of event-forwarding, see [2.5.4 Setting a threshold to automatically suppress forwarding of large numbers of events](#).

(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 [10.2 Initializing the event database](#).

(3) The event database is deleted from the source event server, resulting in delays in JP1 event registration on the target event server.

If the event database is lost from the source event server due to, for example, server replacement or disk failure, and the event database serial number is reset to 0 on the source event server, the source event database serial number of a forwarded JP1 event becomes smaller than the maximum value for the source event database serial number of the source event server that is recorded in the duplication prevention table on the target event server. Therefore, when a JP1 event is forwarded, an event database search is performed on the source event server to check for duplications. This might result in delaying JP1 event addition on the target event server. If the event database is lost from the source event server for a reason such as server replacement or disk failure, recover the event database by using the procedure described in the following subsections:

- [3.5.2\(4\) Recovering the event database](#)
- [3.5.3\(4\) Recovering an event database](#)

If the source event server is not available for operation, but you have added a JP1 event for clearing the duplication prevention table (user event) on the target event server, you can clear the maximum value for the source event database serial number of the source event server in the duplication prevention table.

Procedure:

```
jevsend -i 7FFF8001 -m "DPT CLEAR EVENT" -e OBJECT_NAME=source-event-server-name
```

Notes

- This procedure is applicable only to file-format duplication prevention tables.
- If the duplication prevention table is re-created by the `jevdbmkrep` command when no JP1 events have been received from the source event server since a JP1 event for clearing the duplication prevention table was issued, the maximum value for the source event database serial number of the source event server is not cleared. After you have executed the `jevdbmkrep` command, issue a JP1 event for clearing the duplication prevention table again.

(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 [15. Commands](#).

18.5.2 Problems in Windows

(1) The Event Console window for JP1/IM - View displays incorrect times for JP1 events.

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.

(2) The authentication server fails to start.

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.

(3) The JP1/Base EventlogTrap service fails to start, and the following message is displayed: "Service specific error 3004."

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 [9. Setting the Service Start and Stop Sequences \(Windows Only\)](#).

(4) The startup control function (JP1/Base Control Service) could not start or stop a service normally.

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`).

(5) The startup control function (JP1/Base Control Service) could not stop a system when the system terminated.

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.

(6) 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.

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 16. *Definition Files*.

(7) 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."

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.

(8) 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 the specified service is running

Review the settings as follows:

If the `Wait=` parameter is not set in the section applicable to the service:

The service takes longer than 60 seconds to start. 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.

When the specified service is not running

Investigate why the service failed to start by consulting with the developers.

(9) 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.

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 [9.3 Setting the timing for starting services](#).

(10) Cannot log in when the directory server linkage function is enabled.

Examine the contents of the integrated trace log. If any of the following error messages is included, see the manual *JP1/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



Note

- Action on a login authentication failure when using the directory server linkage function Even if you log in with a correct JP1 user (linkage user) and password, an error might occur during authentication in a directory server and authentication might fail.
- The messages above are output before the next message:
KAVA1691-W An attempt to authenticate the linkage user JP1-user-name has failed.

18.5.3 Problems in UNIX

(1) Failure to start the authentication server

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 `jbssetusrsv` command.

Action

Use the `jbssetusrsv` command to specify the local host in *authentication-server*, and then perform the following:

```
cd /etc/opt/jplbase/conf
cp -p jplbs_spmd.conf.session.model jplbs_spmd.conf
```

(2) Failure to start the event service because an error such as KAJP1005-E or KAJP1852-E occurred

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.

18.5.4 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.

No.	Function	Process name		Recovery action
2	Authentication server	jbsessionmgr		In Windows: Restart the JP1/Base services (process management including user management). In UNIX: Restart JP1/Base.#
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	Restart the log-file trap management service (daemon).
			jevlogd	In Windows: Restart the JP1/Base LogTrap service. In UNIX: Restart the log-file trap management daemon.#
		jelparentim	jelchildim	Using the <code>jevlogstart</code> command, restart the log file trap that has the ID indicated in the error message.
				In Windows: Restart the log file trap whose thread ID is the same as the ID indicated in the message. In UNIX: Restart the log file trap whose process ID is the same as the ID indicated in the message.
8	Event log trap	jevtrapevt		Restart the event log trapping service (JP1/Base EventlogTrap).
9	Health check	jbsbcd		Restart JP1/Base.
		jbsbchostd		In Windows: Restart the JP1/Base services (process management including user management). In UNIX: Restart JP1/Base.#
10	Service management control	jbsbrvmgr		In UNIX: Restart JP1/Base.#
11	Local action	jbslact		
12	Inter-process communication	jbscomd		

#: 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.

18.6 Notes on using JP1/Base

18.6.1 Notes on starting the system

- If you execute the commands below 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`
- In JP1/Base versions 11-10 and later, if a manager host is using a JP1/IM - Manager remote command or automated action, it may take time to start JP1/Base due to the function to automatically re-organize the command execution log file. For the details about the function to automatically re-organize the command execution log file, see [4.9 Function for automatically re-organizing the command execution log file](#).

18.6.2 Notes on starting the system operation

- Do not use the following commands when JP1/Base is active:
 - `jbs_setup_cluster` (Windows only)
 - `jbshostsimport`
 - `jbssetadmingrp` (UNIX only) with any option other than `-v`
 - `jbsunsetcnf`
 - `jevdbinit`
 - `jevdbmkrep`
 - `jplbase_setup` (UNIX only)
 - `jplbase_setup_cluster` (UNIX only)
 - `jplbshasetup` (Windows only)
 - `Jischk`
 - `Jiscond`
 - `Jisconv`
 - `Jiscpy`
 - `Jisext`
 - `Jiskeymnt`
 - `Jislckext`
 - `Jisprt`
 - `Jislckreg` (UNIX only)
 - `Jisrsdel` (UNIX only)
- If there are no JP1 products using JP1/Base user authentication, you can change the following environment settings while JP1/Base is active:

- JP1 user settings[#]
- Authority level for JP1 resource groups (for Windows)[#]
- JP1 user operating permission settings (for UNIX)
- Authentication server change

#:

For the case of operation to use a DS user, the settings can be changed even when a function to use user authentication is operating.

Exercise caution when changing these environment settings while JP1/Base is active.

- On Windows, folders and files referenced by JP1/Base cannot be the folders or files on a network drive. If folders and file on a network drive are specified operation is not guaranteed.
- On UNIX, folders and files referenced by JP1/Base cannot be the folders or files on a mounted NFS. If folders and file on a mounted NFS are specified operation is not guaranteed.
- JP1/Base does not support the 3rd and 4th level JIS characters.
- On Windows, when performing an operation that requires processing efficiency, the following configuration is recommended:

Select **Control Panel - Performance Information and Advanced Tools - Adjust the appearance and performance of Windows - Advanced** tab - **Processor scheduling**, and then select **background services**.

- Do not specify Windows reserved device file names (AUX, CON, NUL, PRN, CLOCK\$, COM[0-9], and LPT[0-9]) in JP1/Base commands or in JP1/Base definition files.
- The accessing of files and folders of JP1/Base by antivirus software might cause JP1/Base to behave unexpectedly. If you are using antivirus software, do not set the software to scan any of the files and folders in the following folders:

- Installation-folder (The following is the default path in Windows.)

On a physical host:

- *system-drive*\Program Files (x86)\Hitachi\JP1Base
- %ALLUSERSPROFILE%\Hitachi\JP1\jpl_default\JP1Base

On a logical host:

- *shared-folder*\jplbase\conf\
- *shared-folder*\jplbase\log\
- *shared-folder*\jplbase\event\
- %ALLUSERSPROFILE%\Hitachi\JP1*logical-host-name*\JP1Base

- Installation-directory (In UNIX)

On a physical host:

- /opt/jplbase
- /etc/opt/jplbase
- /var/opt/jplbase
- /usr/tmp/jpl_ses
- /usr/lib/jpl_ses
- /opt/jpl/hcclibcnf/regdir

On a logical host:

- *shared-directory*/jplbase
- *shared-directory*/event

- The integrated trace log folder (The following is the default path in Windows.)
 - *system-drive*\Program Files (x86)\Hitachi\HNTRLib2
- The integrated trace log directory (In UNIX)
 - /opt/hitachi/HNTRLib2
 - /var/opt/hitachi/HNTRLib2
- Folders that are specified in the index file
 - The default path is *installation-folder*\conf\event\ in Windows, /etc/opt/jp1base/conf/event/ in UNIX.
- Log files monitored by using the log file trapping function

18.6.3 Notes on user authentication

- When a large amount of login activity is concentrated on a single authentication server, the system might output the message KAVB0109-E, KAVB0105-E, KAVB0106-E, or KAVB0108-E and prevent further login attempts. If this error occurs, wait a while and then retry the login.
For details on these messages, see the manual *JP1/Integrated Management 3 - Manager Messages*.
- When you log in from JP1/AJS - View, spaces after a password are ignored.

18.6.4 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.

18.6.5 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 List of files and directories (in Windows)

In the following tables, the *Base_Path* indicates the *installation-folder* in this manual. The default location of *Base_Path* is as follows:

system-drive\Program Files (x86)\Hitachi\jplbase

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	<i>Base_Path</i> \bin\ <i>Base_Path</i> \bin\ext
Environment settings folder ^{#1}	<i>Base_Path</i> \conf\ <i>shared-folder</i> \jplbase\conf\
Language type settings file	<i>Base_Path</i> \conf\jplbs_param.conf <i>shared-folder</i> \jplbase\conf\jplbs_param.conf
Configuration definition file	<i>Base_Path</i> \conf\route\jbs_route.conf <i>shared-folder</i> \jplbase\conf\route\jbs_route.conf
Startup process definition file	<i>Base_Path</i> \cconf\jplbs_spm�.conf <i>Base_Path</i> \cconf\conf\jplbs_spm�.conf.model (No authentication server startup (2038-non compliant)) <i>Base_Path</i> \conf\conf\jplbs_spm�.conf.session.model (Authentication server startup (2038-non compliant)) <i>Base_Path</i> \cconf\conf\jplbs_spm�.conf.2038_model (No authentication server startup (2038 compliant)) <i>Base_Path</i> \cconf\conf\jplbs_spm�.conf.session.2038_model (Authentication server startup (2038 compliant))
JP1/IM function header file	<i>Base_Path</i> \include\JevApi.h
Log folder ^{#2}	<i>Base_Path</i> \log\ <i>shared-folder</i> \jplbase\log\
Folder for plug-in	<i>Base_Path</i> \plugin\
Operating information storage folder	<i>Base_Path</i> \sys\OPI\ <i>shared-folder</i> \jplbase\sys\OPI\
Readme file	<i>Base_Path</i> \readme.txt
Product number and version information	<i>Base_Path</i> \Version.txt
License type information	<i>Base_Path</i> \ProductInfo.txt
Event database storage folder ^{#3}	<i>Base_Path</i> \sys\event\servers\ ^{#4} <i>shared-folder</i> \jplbase\event\ ^{#4}

Contents	File name/folder name
jplhosts2 information	<i>Base_Path</i> \sys\jplhosts2\hostdb{0 1}.bin <i>shared-folder</i> \jplbase\sys\jplhosts2\hostdb{0 1}.bin
Log and temporary folder ^{#2}	<i>Base_Path</i> \sys\tmp\event\servers ^{#4}
	Event ID save file <ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\ereb.backup^{#4} • <i>shared-folder</i>\jplbase\event\ereb.backup^{#4}
	Internal action file for the log file trapping function <ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\logtrap\conftbl.ID-number
Tool folder	<i>Base_Path</i> \tools\
	Data collection tool sample batch file <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\jbs_log.bat
	Function sample source file that issues and collects JP1 events <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\event\receiver.c • <i>Base_Path</i>\tools\event\sender.c
	AR System linkage sample batch file <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\helpdesk\register_ars.bat
	Model file for Active Directory schema extension <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\schema\JP1_UserLevel_schema.ldf.model
Integrated trace log folder	[32bit] <i>system-drive</i> \Program Files (x86)\Hitachi\HNTRLib2\spool\ [64bit] <i>system-drive</i> \Program Files\Hitachi\HNTRLib2\spool\
IT Report Utility (system information collection tool) folder	File used to link with IT Report Utility <ul style="list-style-type: none"> • %ProgramFiles%\Hitachi\systoru\pattern\!830_HNTRLIB2^{#5}
Forwarding suppression status management folder	<i>Base_Path</i> \conf\event\servers\default\suppress ^{#4}
Forwarding suppression information folder for each agent	<i>Base_Path</i> \conf\event\servers\default\suppress\agent-host-name ^{#4}
Auto-scaling linkage script folder ^{#1}	<i>Base_Path</i> \tools\cloud\
	Script files <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\cloud\jbsas_setup_agent.ps1 • <i>Base_Path</i>\tools\cloud\jbsas_add_agent.ps1 • <i>Base_Path</i>\tools\cloud\jbsas_add_agent_cli.ps1 • <i>Base_Path</i>\tools\cloud\jbsas_del_agent.ps1 • <i>Base_Path</i>\tools\cloud\jbsas_del_agent_cli.ps1
	Model files for script files <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\cloud\jbsas_setup_agent.ps1.model • <i>Base_Path</i>\tools\cloud\jbsas_add_agent.ps1.model • <i>Base_Path</i>\tools\cloud\jbsas_add_agent_cli.ps1.model • <i>Base_Path</i>\tools\cloud\jbsas_del_agent.ps1.model • <i>Base_Path</i>\tools\cloud\jbsas_del_agent_cli.ps1.model
	Internal files <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\cloud\jbsas_util.ps1 • <i>Base_Path</i>\tools\cloud\jbsas_hosts

Contents	File name/folder name
	Model file for internal files <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\cloud\jbsas_util.ps1.model
Common definition information backup file output folder	<i>Windows-installation-folder</i> \Temp\JP1_COMDEF\
	Common definition information (except JP1/Base) backup file (physical host) <ul style="list-style-type: none"> • comdef_JP1_DEFAULT.conf
	Common definition information (except JP1/Base) backup file (logical host) <ul style="list-style-type: none"> • comdef_logical-host-name.conf
	Internal files <ul style="list-style-type: none"> • logical.list

#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 *2.3.2 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).

#5: For a server OS that is Windows Server 2012 or later.

(1) List of definition files (in Windows)

Table A–2: List of definition files (in Windows)

Function	File name/folder name
Startup control	Start sequence definition file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\boot\JP1SVPRM.DAT • <i>Base_Path</i>\conf\boot\JP1SVPRM.DAT.MODEL
	Service startup delay time / timer monitoring period definition file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\boot\jplsvprm_wait.dat • <i>Base_Path</i>\conf\boot\jplsvprm_wait.dat.sample
Event service	Event server index file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\index
	Event server settings file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\conf#1 • <i>shared-folder</i>\jplbase\event\conf#1
	Forwarding settings file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\forward#1 • <i>shared-folder</i>\jplbase\event\forward#1
	Forwarding settings file for event-forwarding suppression <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\suppress\forward_suppress#1
	Any forwarding suppression definition file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\suppress\forwarding-suppression-definition-file-name#1
	API settings file <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\api
	Additional extended attribute settings file for transfer reception <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\recv_add_extattr#1

Function	File name/folder name
	<ul style="list-style-type: none"> • <i>shared-folder</i>\jplbase\event\recv_add_extattr#1
	<p>Additional extended attribute settings file for event registration</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\send_add_extattr#1 • <i>shared-folder</i>\jplbase\event\send_add_extattr#1
Event conversion	<p>Log file trap definition file You can specify any folder and any file.</p>
	<p>Log-file trap startup definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\jevlog_start.conf
	<p>Log information definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\jevlogd.conf
	<p>Event log trap definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\ntevent.conf
Event service definition information collection and distribution	<p>Distribution definition file (forwarding settings file)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\[jev_forward.conf <i>any-file</i>]^{#2} • <i>shared-folder</i>\jplbase\event\[jev_forward.conf <i>any-file</i>]^{#2}
	<p>Distribution definition file (log file trap definition file)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\[jev_logtrap.conf <i>any-file</i>]^{#2}
	<p>Distribution definition file (event log trap definition file)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\[jev_ntevent.conf <i>any-file</i>]^{#2}
User management	<p>Password definition file You can specify any folder and any file.</p>
	<p>User permission level file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\user_acl\JP1_UserLevel • <i>shared-folder</i>\jplbase\conf\user_acl\JP1_UserLevel
	<p>Directory server modification file You can specify any folder and any file.</p>
	<p>Directory server linkage definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\ds\jplbs_ds_setup.conf • <i>Base_Path</i>\conf\ds\jplbs_ds_setup.conf.model • <i>shared-folder</i>\jplbase\conf\ds\jplbs_ds_setup.conf • <i>shared-folder</i>\jplbase\conf\ds\jplbs_ds_setup.conf.model
	<p>User mapping definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\user_acl\jplBsUmap.conf • <i>shared-folder</i>\jplbase\conf\user_acl\jplBsUmap.conf
	<p>Password policy definition files</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\passwdpolc\jplbs_passwdpolc.conf • <i>shared-folder</i>\jplbase\conf\passwdpolc\jplbs_passwdpolc.conf
Health check function	<p>Health check definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jbshc\jbshc.conf • <i>shared-folder</i>\jplbase\conf\jbshc\jbshc.conf
	<p>Model file for the common definition settings file (health check function)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jbshc\jbshc_setup.conf.model

Function	File name/folder name
	<ul style="list-style-type: none"> • <i>shared-folder</i>\jplbase\conf\jbshc\jbshc_setup.conf.model <p>Model file for the common definition settings file (health check function) (for upgrade from version 07-00 or earlier)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\default\jbshc_com.conf.model • <i>shared-folder</i>\jplbase\default\jbshc_com.conf.model
Plugin service	<p>Request transmission settings file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\plugin\reqforward.conf • <i>shared-folder</i>\jplbase\conf\plugin\reqforward.conf
Operation log output function	<p>Operation log definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jplbs_base\log_setup.conf • <i>Base_Path</i>\conf\jplbs_base\log_setup.conf.model
Process management	<p>JP1/Base parameter definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jplbs_param_v7.conf • <i>shared-folder</i>\jplbase\conf\jplbs_param_v7.conf <p>Extended startup process definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jplbs_service_0700.conf • <i>shared-folder</i>\jplbase\conf\jplbs_service_0700.conf
Communication settings	<p>jp1hosts definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jp1hosts • <i>shared-folder</i>\jplbase\conf\jp1hosts <p>jp1hosts2 definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jp1hosts2.conf • <i>shared-folder</i>\jplbase\conf\jp1hosts2.conf <p>Communication protocol settings file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\physical_ipany.conf • <i>Base_Path</i>\conf\logical_ipany.conf • <i>Base_Path</i>\conf\physical_recovery_0651.conf • <i>Base_Path</i>\conf\logical_recovery_0651.conf • <i>Base_Path</i>\conf\physical_anyany.conf • <i>Base_Path</i>\conf\physical_ipip.conf • <i>Base_Path</i>\conf\logical_ipip.conf • <i>shared-folder</i>\jplbase\conf\physical_ipany.conf • <i>shared-folder</i>\jplbase\conf\logical_ipany.conf • <i>shared-folder</i>\jplbase\conf\physical_recovery_0651.conf • <i>shared-folder</i>\jplbase\conf\logical_recovery_0651.conf • <i>shared-folder</i>\jplbase\conf\physical_anyany.conf • <i>shared-folder</i>\jplbase\conf\physical_ipip.conf • <i>shared-folder</i>\jplbase\conf\logical_ipip.conf <p>Host access control definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jbsdfts\jbsdfts_srv.conf <p>SSL communication definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jplbs_ssl.conf • <i>shared-folder</i>\jplbase\conf\jplbs_ssl.conf <p>Non-SSL communication host configuration file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jplbs_nosslhost.conf

Function	File name/folder name
	<p>File to which to write SSL definitions</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\ssl.conf • <i>shared-folder</i>\jplbase\event\ssl.conf
	<p>File to which to save the non-SSL communication host configuration file (JP1/Base)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\sys\nossl_base.conf • <i>Base_Path</i>\sys\nossl_base{1 2 3}.conf • <i>shared-folder</i>\jplbase\sys\nossl_base.conf • <i>shared-folder</i>\jplbase\sys\nossl_base{1 2 3}.conf
	<p>File to which to save the non-SSL communication host configuration file (event service)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\nossl_evt.conf • <i>Base_Path</i>\sys\tmp\event\servers\default\nossl_evt{1 2 3}.conf • <i>shared-folder</i>\jplbase\event\nossl_evt.conf • <i>shared-folder</i>\jplbase\event\nossl_evt{1 2 3}.conf
Local action function	<p>Local action environment variable file You can specify any folder and any file.</p>
	<p>Local action execution definition file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\lcact\jbslcact.conf • <i>shared-folder</i>\jplbase\conf\lcact\jbslcact.conf
	<p>Common definition settings file (local action function)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\lcact\jplbs_lcact_setup.conf.model • <i>shared-folder</i>\jplbase\conf\lcact\jplbs_lcact_setup.conf.model
Collection of JP1/Base setup information in a single operation	<p>Collection information file</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\jbsparamdump.conf
Configuration management functionality	<p>Common definition settings file (configuration management functionality)</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\conf\route\jbsrt_setup.conf.model • <i>shared-folder</i>\jplbase\conf\route\jbsrt_setup.conf.model
Auto-scaling linkage scripts	<p>Script definition files</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\cloud\jbsas_setup_agent.ini • <i>Base_Path</i>\tools\cloud\jbsas_setup_manager.ini • <i>Base_Path</i>\tools\cloud\jbsas_setup_manager_cli.ini
	<p>Model files for script definition files</p> <ul style="list-style-type: none"> • <i>Base_Path</i>\tools\cloud\jbsas_setup_agent.ini.model • <i>Base_Path</i>\tools\cloud\jbsas_setup_manager.ini.model • <i>Base_Path</i>\tools\cloud\jbsas_setup_manager_cli.ini.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: This file does not exist unless definition information distribution is used.

(2) List of log files (in Windows)

The table below lists the log files that JP1/Base outputs by default.

! Important

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.

File name/folder name indicates the full path of the log file name when JP1/Base is installed using the default settings, and the log file name when JP1/Base is used in a cluster system.

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)

Log type	File name/folder name	Max. disk space	File changing timing
Process management log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBS_SPMD{1 2 3}.log • <i>shared-folder</i>\jplbase\log\JBS_SPMD{1 2 3}.log 	384 KB	128 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBS_SPMD_COMMAND{1 2 3}.log • <i>shared-folder</i>\jplbase\log\JBS_SPMD_COMMAND{1 2 3}.log 	384 KB	128 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBS_SERVICE{1 2 3}.log • <i>shared-folder</i>\jplbase\log\JBS_SERVICE{1 2 3}.log 	384 KB	128 KB
Authentication server log	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jpl_default\JP1Base\log\jbsessionapi.log{1 2 3 4 5 6 7 8}.log#1 • %ALLUSERSPROFILE%\Hitachi\JP1\logical-host-name\JP1Base\log\jbsessionapi.log{1 2 3 4 5 6 7 8}.log#1 	5 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsessionmgr{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\jbsessionmgr{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsessionmgr_trace{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\jbsessionmgr_trace{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
Log of the authentication server setting command	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBSSESS{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\JBSSESS{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBS_SETUP\JBSSETUPSRV{1 2}.log 	128 KB	64 KB
Log of the environment settings program	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jplbssetup{1 2}.log • <i>shared-folder</i>\jplbase\log\jplbssetup{1 2}.log 	128 KB	64 KB

Log type	File name/folder name	Max. disk space	File changing timing
Log of the logical host setting program	• <i>Base_Path</i> \log\jplhassetup.{log log.old}	2,000 KB	1,000 KB
	• <i>Base_Path</i> \log\JBS_SETUP\JBSSETUPCLUSTER{1 2}.log	128 KB	64 KB
Command execution log (ISAM) ^{#2}	• <i>Base_Path</i> \log\COMMAND\ACTISAMLOGV8.DRF • <i>shared-folder</i> \jplbase\log\COMMAND\ ACTISAMLOGV8.DRF	1.2 GB ^{#3}	None
	• <i>Base_Path</i> \log\COMMAND\ACTISAMLOGV8.K01 • <i>shared-folder</i> \jplbase\log\COMMAND\ ACTISAMLOGV8.K01	2 MB ^{#3}	None
	• <i>Base_Path</i> \log\COMMAND\ACTISAMLOGV8.KDF • <i>shared-folder</i> \jplbase\log\COMMAND\ ACTISAMLOGV8.KDF	1 KB	When the command is executed
	• <i>Base_Path</i> \log\COMMAND\CMDISAMLOGV8.DRF • <i>shared-folder</i> \jplbase\log\COMMAND\ CMDISAMLOGV8.DRF	1.2 GB ^{#3}	None
	• <i>Base_Path</i> \log\COMMAND\CMDISAMLOGV8.K01 • <i>shared-folder</i> \jplbase\log\COMMAND\ CMDISAMLOGV8.K01	2 MB ^{#3}	None
	• <i>Base_Path</i> \log\COMMAND\CMDISAMLOGV8.KDF • <i>shared-folder</i> \jplbase\log\COMMAND\ CMDISAMLOGV8.KDF	1 KB	When the command is executed
	• <i>Base_Path</i> \log\COMMAND\CMDISAMLOGV8.DRF • <i>shared-folder</i> \jplbase\log\COMMAND\ CMDISAMLOGV8.DRF	1.2 GB ^{#3}	None
Common definition information log	• <i>Base_Path</i> \log\JBSCNFCMD\JBSCNFCMD{1 2}.log	128 KB	64 KB
Log of jplhosts information command	• <i>Base_Path</i> \log\JBSCNFCMD\JBSCOMMCMD{1 2}.log	128 KB	64 KB
User mapping command log	• <i>Base_Path</i> \log\JBSUMAPCMD\JBSUMAPCMD{1 2}.log • <i>shared-folder</i> \jplbase\log\JBSUMAPCMD\JBSUMAPCMD{1 2}.log	128 KB	64 KB
Remote command log ^{#2}	• <i>Base_Path</i> \log\JCOCMD\jcocmd_result{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i> \jplbase\log\JCOCMD\jcocmd_result{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB
	• <i>Base_Path</i> \log\JCOCMD\jcocmdapi{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i> \jplbase\log\JCOCMD\jcocmdapi{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB
	• <i>Base_Path</i> \log\JCOCMD\jcocmdapi_trace{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i> \jplbase\log\JCOCMD\jcocmdapi_trace{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB
	• <i>Base_Path</i> \log\JCOCMD\jcocmdcom{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i> \jplbase\log\JCOCMD\jcocmdcom{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB
	• <i>Base_Path</i> \log\JCOCMD\jcocmdcom_trace{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i> \jplbase\log\JCOCMD\jcocmdcom_trace{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB
	• <i>Base_Path</i> \log\JCOCMD\jcocmddex{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB
	• <i>Base_Path</i> \log\JCOCMD\jcocmddex_trace{1 2 3 4 5 6 7 8}.log	20 MB	2.5 MB

Log type	File name/folder name	Max. disk space	File changing timing
	<ul style="list-style-type: none"> • <i>shared-folder</i>\jplbase\log\JCOCMD\jcocmdexe{1 2 3 4 5 6 7 8}.log 		
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JCOCMD\jcocmdexe_trace{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\JCOCMD\jcocmdexe_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JCOCMD\jcocmdrouter{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\JCOCMD\jcocmdrouter{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JCOCMD\jcocmdrouter_trace{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\JCOCMD\jcocmdrouter_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JCOCMD\JCOCMDCMD{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\JCOCMD\JCOCMDCMD{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
Plug-in service log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\plugin\jbsplugin{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\plugin\jbsplugin{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\plugin\jbsplugincom_{0 1 2 3 4 5 6 7 8 9}#4_{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\plugin\jbsplugincom_{0 1 2 3 4 5 6 7 8 9}#4_{1 2 3 4 5 6 7 8}.log 	50 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\plugin\jbsplugincmd{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\plugin\jbsplugincmd{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\plugin\jbsplugincmdapi{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\plugin\jbsplugincmdapi{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\plugin\jbspluginhcshm{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\plugin\jbspluginhcshm{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jpl_default\JP1Base\log\plugin\jbsrmtcmd{1 2 3 4 5 6 7 8}.log^{#1} 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\plugin\jbspluginremotecmd{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\plugin\jbspluginremotecmd{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB

Log type	File name/folder name	Max. disk space	File changing timing
	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbsrmtapi{1 2 3 4 5 6 7 8}.log^{#1} 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbspluginmgrapi{1 2 3 4 5 6 7 8}.log^{#1} • %ALLUSERSPROFILE%\Hitachi\JP1\logical-host-name\JP1Base\log\plugin\jbspluginmgrapi{1 2 3 4 5 6 7 8}.log^{#1} 	5 MB	640 KB
	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbsplugincomapi{1 2 3 4 5 6 7 8}.log^{#1} • %ALLUSERSPROFILE%\Hitachi\JP1\logical-host-name\JP1Base\log\plugin\jbsplugincomapi{1 2 3 4 5 6 7 8}.log^{#1} 	5 MB	640 KB
Configuration management log ^{#2}	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\route\JBSRT{1 2 3 4 5}.log • <i>shared-folder</i>\jp1base\log\route\JBSRT{1 2 3 4 5}.log 	20 MB	4 MB
Start sequence control log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\boot\ContServ{1 2}.log 	128 KB	64 KB
Event log trap trace log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\ntevtrap\trace{1 2}.log 	1,024 KB	512 KB
Trap log for event log traps	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\ntevtrap\trap{1 2 3 4}.log 	4,096 KB	1,024 KB
Log of the health check function (local host monitoring)	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbshc\jbshc{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jp1base\log\jbshc\jbshc{1 2 3 4 5 6 7 8}.log 	50 MB	6.25 MB
Log of the health check function (remote host monitoring)	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbshc\jbshc{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jp1base\log\jbshc\jbshc{1 2 3 4 5 6 7 8}.log 	50 MB	6.25 MB
Health check command log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbshc\jbshcstatus{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jp1base\log\jbshc\jbshcstatus{1 2 3 4 5 6 7 8}.log 	50 MB	6.25 MB
Log of the health check API	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbshc\jbshcapi{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jp1base\log\jbshc\jbshcapi{1 2 3 4 5 6 7 8}.log 	50 MB	6.25 MB
Application error log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsdump.log 	5 MB	5 MB
Operation log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\BASE\base_log[{1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16}].log 	68 MB ^{#5}	1,024 KB ^{#5#6}
Trace log for the event setting, centralized management, and acquisition command	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\jevdef_get.{000 001 002}^{#7} • <i>shared-folder</i>\jp1base\event\jevdef_get.{000 001 002}^{#7} 	192 KB	When the command is executed

Log type	File name/folder name	Max. disk space	File changing timing
Trace log for event setting, centralized management, and distribution command	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\jevdef_distrib.{000 001 002}#7 • <i>shared-folder</i>\jplbase\event\jevdef_distrib.{000 001 002}#7 	192 KB	When the command is executed
Trace log of the event service	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\trace.{000 001 002 003 004}#7#8 • <i>shared-folder</i>\jplbase\event\trace.{000 001 002 003 004}#7#8 	12.5 MB ^{#8}	When the event service starts
	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\imevterr.{000 001 002 003 004}#7#8 • <i>shared-folder</i>\jplbase\event\imevterr.{000 001 002 003 004}#7#8 	5 MB ^{#8}	When the event service starts
Transfer error log of the event service	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\fderr.{000 001 002 003 004}#7#8 • <i>shared-folder</i>\jplbase\event\fderr.{000 001 002 003 004}#7#8 	5 MB ^{#8}	When the event service starts
Error log of the event service	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\error.{000 001 002 003 004}#7#8 • <i>shared-folder</i>\jplbase\event\error.{000 001 002 003 004}#7,#8 	2,500 KB ^{#8}	When the event service starts
Log of the event service API.	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jpl_default\JP1Base\log\event\IMEvapi.{000 001 002 003 004}#9#10 	5 MB ^{#9}	1 MB ^{#9}
Log of the event service	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jpl_default\JP1Base\log\event\IMEvenc.{000 001 002 003 004}#10 	5 MB	1 MB
Event service message settings change log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jevmessage\jevmessageid{1 2}.log 	10 KB	5 KB
Error log of the log file trap	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\logtrap\.errorfile.ID-number 	A few hundred bytes ^{#12}	When the log file trap starts
Log of the log file trap	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\logtrap\jevtraplog\jevtraplog.{000 001 002 003 004} 	5 MB ^{#13}	1 MB ^{#13}
Log-file trap startup execution results log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jevlog_start\jevlog_start{1 2 3}.log^{#15#16} 	3 MB	1 MB
Remote monitoring log (log-file trap)	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\logtrap\jelallog\jelallog{1-5}.log^{#15} 	5 MB	1 MB
Remote monitoring log (event log trap)	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\logtrap\jelalelt\jelalelt{1-5}.log^{#15} 	5 MB	1 MB
Installation log	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\jplcommon\jplbase\hliclibtrc{1 2 3 4 5}.log 	1 MB	200 KB
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\jplcommon\jplbase\hliclibmgrtrc{1 2 3 4 5}.log 	1 MB	200 KB

Log type	File name/folder name	Max. disk space	File changing timing
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\jplcommon\jplbase\hlicliberr{1 2 3 4 5}.log 	50 KB	10 KB
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\jplcommon\jplbase\hliclibmgrerr{1 2 3 4 5}.log 	50 KB	10 KB
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\HCDINST\product-number[_{1 2 3 4 5}].LOG <p>The output destination in the remote desktop service (formerly known as the terminal service) of the server OS changes as follows:</p> <ul style="list-style-type: none"> • %USERPROFILE%\WINDOWS\Temp\HCDINST\product-number[_{1 2 3 4 5}].LOG 	25 KB	At installation
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\HCDINST\NETMINST.LOG 	256 KB	256 KB
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\RF\HRF4SECURITYINSTALL{1 2 3 4}.LOG 	1,024 KB	256 KB
	<ul style="list-style-type: none"> • <i>Windows-installation-folder</i>\Temp\RF\HRF4INSTALL{1 2 3 4}.LOG 	1,024 KB	256 KB
Trace log for inter-process communication	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBSCOM\jbscmd{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\JBSCOM\jbscmd{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBSCOM\jbscmd_api{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\JBSCOM\jbscmd_api{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBSCOM\jbscmd_snd{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\JBSCOM\jbscmd_snd{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBSCOM\jbscmd_rcv{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\JBSCOM\jbscmd_rcv{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBSCOM\command{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\JBSCOM\command{1 2 3 4}.log 	10 MB	2.5 MB
Error log of the command for collecting operating information	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsopi\jbsopi_cmd{1 2 3 4 5}.log 	5 MB	1 MB
Log for the operating information API	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsopi\jbsopi_api{1 2 3 4 5}.log • <i>shared-folder</i>\jplbase\log\jbsopi\jbsopi_api{1 2 3 4 5}.log 	5 MB	1 MB
Service management control log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsrvmgr\jbsrvmgr{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\jbsrvmgr\jbsrvmgr{1 2 3 4}.log 	10 MB	2.5 MB
Trace log of the service management control	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbsrvmgr\jbsrvmgr_trace{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\jbsrvmgr\jbsrvmgr_trace{1 2 3 4}.log 	10 MB	2.5 MB

Log type	File name/folder name	Max. disk space	File changing timing
Log of the service management control API	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbssrvmgr\jbssrvmgr_api{1 2 3 4}.log • <i>shared-folder</i>\jplbase\log\jbssrvmgr\jbssrvmgr_api{1 2 3 4}.log 	10 MB	2.5 MB
Local action execution log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\lcact\localact{1-n}#14.log • <i>shared-folder</i>\jplbase\log\lcact\localact{1-n}#14.log 	1,024 KB#14	256 KB#14
Local action log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbslcact\jbslcact{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\jbslcact\jbslcact{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbslcact\jbslcact_list{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\jbslcact\jbslcact_list{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\jbslcact\jbslcact_cancel{1 2 3 4 5 6 7 8}.log • <i>shared-folder</i>\jplbase\log\jbslcact\jbslcact_cancel{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
Product information log	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\hliclib\hliclib*.log 	5 MB	1 MB
JP1/Base communications base log	<ul style="list-style-type: none"> • %ALLUSERSPROFILE%\Hitachi\JP1\jpl_default\JP1Base\log\jplBsComm\error{1 2 3 4 5}.log #10 	5 MB	1 MB
Individual log for the setup information collection command	<ul style="list-style-type: none"> • <i>Base_Path</i>\log\JBS_SETUP\JBSPARAMDUMP{1 2}.log 	2 MB	1 MB
Log for recording starting and stopping of forwarding suppression	<ul style="list-style-type: none"> • <i>Base_Path</i>\conf\event\servers\default\suppress\agent-host-name\{log log.old}#7 	128 KB	64 KB
Trace log for the event-forwarding suppression command	<ul style="list-style-type: none"> • <i>Base_Path</i>\sys\tmp\event\servers\default\jevagtfw.{000 001 002 003 004}#7 	5 MB	1 MB

#1: The value set in the environment variable %ALLUSERSPROFILE% at installation is used.

#2: Log file for JP1/IM - Manager

#3: You can use the jccomddef 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 records is 20,000 (the default setting)
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

#4: Indicates a jbsplugincom process identification number.

#5: You can use the operation log definition file (jplbs_base_log_setup.conf) to change the number of files and the maximum disk space. For details on the range of specifiable values, see [1.5 Settings for outputting operation logs](#).

#6: You can specify whether to automatically switch files at JP1/Base startup in the operation log definition file (jplbs_base_log_setup.conf).

- #7: This file or folder is stored in a different folder if you specify another path in the event server index file (`index`).
- #8: 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 *16. Definition Files*.
- #9: 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 *16. Definition Files*.
- #10: The value set in the environment variable `%ALLUSERSPROFILE%` at execution is used.
- #11: One line equals approximately 100 bytes.
- #12: 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.
- #13: 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 *16. Definition Files*.
- #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 *16. Definition Files*.
- #15: Logs are output in HNTRLib2 format (multi-process trace).
- #16: When deleting this log data, also delete the `mmap` folder at the output destination.

A.2 List of files and directories (in UNIX)

Table A–4: List of files and directories of JP1/Base (in UNIX)

Contents	File name/directory name
Command storage directory	<code>/opt/jplbase/bin/</code> <code>/opt/jplbase/bin/ext/#1</code>
Environment setting directory ^{#2}	<code>/etc/opt/jplbase/conf/</code> <code>shared-directory/jplbase/conf/</code>
Language type settings file	<code>/etc/opt/jplbase/conf/jplbs_param.conf</code> <code>shared-directory/jplbase/conf/jplbs_param.conf</code>
Configuration definition file	<code>/etc/opt/jplbase/conf/route/jbs_route.conf</code> <code>shared-directory/jplbase/conf/route/jbs_route.conf</code>
Startup process definition file	<ul style="list-style-type: none"> <code>/etc/opt/jplbase/cconf/jplbs_spm�.conf</code> <code>/etc/opt/jplbase/cconf/jplbs_spm�.conf.model</code> (No authentication server startup (2038-non compliant)) <code>/etc/opt/jplbase/cconf/jplbs_spm�.conf.session.model</code> (Authentication server startup (2038-non compliant)) <code>/etc/opt/jplbase/cconf/jplbs_spm�.conf.2038_model</code> (No authentication server startup (2038 compliant)) <code>/etc/opt/jplbase/cconf/jplbs_spm�.conf.session.2038_model</code> (Authentication server startup (2038 compliant))
Character code mapping definition file	<ul style="list-style-type: none"> <code>/opt/jplbase/lib/eventenc.dat</code> <code>/opt/jplbase/lib/eventenc.dat.model</code>
Language type mapping definition file	<ul style="list-style-type: none"> <code>/opt/jplbase/lib/eventlng.dat</code> <code>/opt/jplbase/lib/eventlng.dat.model</code>
JP1/IM function header file	<code>/opt/jplbase/include/JevApi.h</code>
Log directory ^{#3}	<code>/var/opt/jplbase/log/</code> <code>shared-directory/jplbase/log/</code>
Directory for plug-in	<code>/opt/jplbase/plugin/</code>

Contents	File name/directory name
Directory for storing operating information	<code>/var/opt/jplbase/sys/OPI/</code> <i>shared-directory</i> / <code>/jplbase/sys/OPI/</code>
Event DB storage directory ^{#4}	<code>/var/opt/jplbase/sys/event/servers/#5</code> <i>shared-directory</i> / <code>/event/#5</code>
jplhosts2 information	<code>/var/opt/jplbase/sys/jplhosts2/hostdb{0 1}.bin</code> <i>shared-directory</i> / <code>/jplbase/sys/jplhosts2/hostdb{0 1}.bin</code>
Log and temporary directory ^{#3}	<code>/var/opt/jplbase/sys/tmp/event/servers/#5</code>
	Event ID save file <ul style="list-style-type: none"> <code>/var/opt/jplbase/sys/tmp/event/servers/default/ereb.backup#5</code>
	Internal action file for the log file trapping function <ul style="list-style-type: none"> <code>/var/opt/jplbase/sys/tmp/event/logtrap/conftbl.ID-number</code>
Tool directory	<code>/opt/jplbase/tools/</code>
	Data collection tool sample script file <ul style="list-style-type: none"> <code>/opt/jplbase/tools/jbs_log.sh</code>
	Function sample source file that issues and collects JP1 events <ul style="list-style-type: none"> <code>/opt/jplbase/tools/event/receiver.c</code> <code>/opt/jplbase/tools/event/sender.c</code>
	AR System linkage sample script file <ul style="list-style-type: none"> <code>/opt/jplbase/tools/helpdesk/register_ars.sh</code>
Integrated trace log directory	<code>/var/opt/hitachi/HNTRLlib2/spool/</code>
IT Report Utility (system information collection tool) folder	File used to link with IT Report Utility <ul style="list-style-type: none"> <code>/etc/opt/hitachi/systoru/pattern/!830_HNTRLIB2</code>
Forwarding suppression status management directory	<code>/etc/opt/jplbase/conf/event/servers/default/suppress#5</code>
Forwarding suppression information directory for each agent	<code>/etc/opt/jplbase/conf/event/servers/default/suppress/agent-host-name#5</code>
Auto-scaling linkage script directory ^{#2}	<code>/opt/jplbase/tools/cloud/</code>
	Script files <ul style="list-style-type: none"> <code>/opt/jplbase/tools/cloud/jbsas_setup_agent.sh</code> <code>/opt/jplbase/tools/cloud/jbsas_add_agent.sh</code> <code>/opt/jplbase/tools/cloud/jbsas_add_agent_cli.sh</code> <code>/opt/jplbase/tools/cloud/jbsas_del_agent.sh</code> <code>/opt/jplbase/tools/cloud/jbsas_del_agent_cli.sh</code>
	Model files for script files <ul style="list-style-type: none"> <code>/opt/jplbase/tools/cloud/jbsas_setup_agent.sh.model</code> <code>/opt/jplbase/tools/cloud/jbsas_add_agent.sh.model</code> <code>/opt/jplbase/tools/cloud/jbsas_add_agent_cli.sh.model</code> <code>/opt/jplbase/tools/cloud/jbsas_del_agent.sh.model</code> <code>/opt/jplbase/tools/cloud/jbsas_del_agent_cli.sh.model</code>
	Internal files <ul style="list-style-type: none"> <code>/opt/jplbase/tools/cloud/jbsas_util.sh</code>

Contents	File name/directory name
	<ul style="list-style-type: none"> • /opt/jplbase/tools/cloud/jbsas_hosts
	Model file for internal files <ul style="list-style-type: none"> • /opt/jplbase/tools/cloud/jbsas_util.sh.model
Common definition information backup file output directory	/tmp/JP1_COMDEF/
	Common definition information (except JP1/Base) backup file (physical host) <ul style="list-style-type: none"> • comdef_JP1_DEFAULT.conf
	Common definition information (except JP1/Base) backup file (logical host) <ul style="list-style-type: none"> • comdef_logical-host-name.conf
	Internal files <ul style="list-style-type: none"> • logical.list

#1: This is created for Linux.

#2: For details on definition files, see [A.2\(1\) List of definition files \(in UNIX\)](#).

#3: For details on log files, see [A.2\(2\) List of log files \(in UNIX\)](#).

#4: For details on event database file name, see [2.3.2 Event database](#).

#5: 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)

Table A–5: List of definition files (in UNIX)

Function	File name/directory name
Event service	Event server index file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/index
	Event server settings file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/conf^{#1} • <i>shared-directory</i>/event/conf^{#1}
	Forwarding settings file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/forward^{#1} • <i>shared-directory</i>/event/forward^{#1}
	Forwarding settings file for event-forwarding suppression <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/suppress/forward_suppress^{#1}
	Any forwarding suppression definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/suppress/<i>forwarding-suppression-definition-file-name</i>^{#1}
	API settings file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/api
	Additional extended attribute settings file for transfer reception <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/recv_add_extattr^{#1} • <i>shared-directory</i>/event/recv_add_extattr^{#1}
	Additional extended attribute settings file for event registration <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/send_add_extattr^{#1} • <i>shared-directory</i>/event/send_add_extattr^{#1}

Function	File name/directory name
Event conversion	Log file trap definition file You can specify any folder and any file.
	Log-file trap startup definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/jevlog_start.conf
	Log information definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/jevlogd.conf
Event service definition information collection and distribution	Distribution definition file (forwarding settings file) <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/[jev_forward.conf any-file]#2 • shared-directory/event/[jev_forward.conf any-file]#2
	Distribution definition file (log file trap definition file) <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/[jev_logtrap.conf any-file]#2
	Distribution definition file (event log trap definition file) <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/[jev_ntevent.conf any-file]#2
User management	User permission level file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/user_acl/JP1_UserLevel • shared-directory/jplbase/conf/user_acl/JP1_UserLevel
	User mapping definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/user_acl/jplBsUmap.conf • shared-directory/jplbase/conf/user_acl/jplBsUmap.conf
	Password policy definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/passwdpolc/jplbs_passwdpolc.conf • shared-directory/jplbase/conf/passwdpolc/jplbs_passwdpolc.conf
Health check function	Health check definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jbshc/jbshc.conf • shared-directory/jplbase/conf/jbshc/jbshc.conf
	Model file for the common definition settings file (health check function) <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jbshc/jbshc_setup.conf.model • shared-directory/jplbase/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) <ul style="list-style-type: none"> • /etc/opt/jplbase/default/jbshc_com.conf.model • shared-directory/jplbase/default/jbshc_com.conf.model
Plugin service	Request transmission settings file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/plugin/reqforward.conf • shared-directory/jplbase/conf/plugin/reqforward.conf
Operation log output function	Operation log definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplbs_base_log_setup.conf • /etc/opt/jplbase/conf/jplbs_base_log_setup.conf.model
Process management	JP1/Base parameter definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplbs_param_v7.conf • shared-directory/jplbase/conf/jplbs_param_v7.conf

Function	File name/directory name
	<p>Extended startup process definition file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplbs_service_0700.conf • <i>shared-directory</i>/jplbase/conf/jplbs_service_0700.conf
Communication settings	<p>jplhosts definition file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplhosts • <i>shared-directory</i>/jplbase/conf/jplhosts
	<p>jplhosts2 definition file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplhosts2.conf • <i>shared-directory</i>/jplbase/conf/jplhosts2.conf
	<p>Communication protocol settings file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/physical_ipany.conf • /etc/opt/jplbase/conf/logical_ipany.conf • /etc/opt/jplbase/conf/physical_recovery_0651.conf • /etc/opt/jplbase/conf/logical_recovery_0651.conf • /etc/opt/jplbase/conf/physical_anyany.conf • /etc/opt/jplbase/conf/physical_ipip.conf • /etc/opt/jplbase/conf/logical_ipip.conf • <i>shared-directory</i>/jplbase/conf/physical_ipany.conf • <i>shared-directory</i>/jplbase/conf/logical_ipany.conf • <i>shared-directory</i>/jplbase/conf/physical_recovery_0651.conf • <i>shared-directory</i>/jplbase/conf/logical_recovery_0651.conf • <i>shared-directory</i>/jplbase/conf/physical_anyany.conf • <i>shared-directory</i>/jplbase/conf/physical_ipip.conf • <i>shared-directory</i>/jplbase/conf/logical_ipip.conf
	<p>Host access control definition file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jbsdfts/jbsdfts_srv.conf
	<p>SSL communication definition file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplbs_ssl.conf • <i>shared-directory</i>/jplbase/conf/jplbs_ssl.conf
	<p>Non-SSL communication host configuration file</p> <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/jplbs_nosslhost.conf
	<p>File to which to write SSL definitions</p> <ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/ssl.conf • <i>shared-directory</i>/jplbase/event/ssl.conf
	<p>File to which to save the non-SSL communication host configuration file (JP1/Base)</p> <ul style="list-style-type: none"> • /var/opt/jplbase/sys/nossl_base.conf • /var/opt/jplbase/sys/nossl_base{1 2 3}.conf • <i>shared-directory</i>/jplbase/sys/nossl_base.conf • <i>shared-directory</i>/jplbase/sys/nossl_base{1 2 3}.conf
	<p>File to which to save the non-SSL communication host configuration file (event service)</p> <ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/nossl_evt.conf • /var/opt/jplbase/sys/tmp/event/servers/default/nossl_evt{1 2 3}.conf • <i>shared-directory</i>/event/nossl_evt.conf • <i>shared-directory</i>/event/nossl_evt{1 2 3}.conf

Function	File name/directory name
Local action function	Local action environment variable file You can specify any folder and any file.
	Local action execution definition file <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/lcact/jbslcact.conf • <i>shared-directory</i>/jplbase/conf/lcact/jbslcact.conf
	Common definition settings file (local action function) <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/lcact/jplbs_lcact_setup.conf.model • <i>shared-directory</i>/jplbase/conf/lcact/jplbs_lcact_setup.conf.model
Collection of JP1/Base setup information in a single operation	Collection information file <ul style="list-style-type: none"> • /etc./opt/jplbase/conf/jbsparamdump.conf
Configuration management functionality	Common definition settings file (configuration management functionality) <ul style="list-style-type: none"> • /etc/opt/jplbase/conf/route/jbsrt_setup.conf.model • <i>shared-directory</i>/jplbase/conf/route/jbsrt_setup.conf.model
Auto-scaling linkage scripts	Script definition files <ul style="list-style-type: none"> • /opt/jplbase/tools/cloud/jbsas_setup_agent.ini • /opt/jplbase/tools/cloud/jbsas_setup_manager.ini • /opt/jplbase/tools/cloud/jbsas_setup_manager_cli.ini
	Model files for script definition files <ul style="list-style-type: none"> • /opt/jplbase/tools/cloud/jbsas_setup_agent.ini.model • /opt/jplbase/tools/cloud/jbsas_setup_manager.ini.model • /opt/jplbase/tools/cloud/jbsas_setup_managerr_cli.ini.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: This file does not exist unless definition information distribution is used.

(2) List of log files (in UNIX)

The table below lists the log files that JP1/Base outputs by default.

Important

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.

File name/directory name indicates the full path of the log file name when JP1/Base is installed using the default settings, and the log file name when JP1/Base is used in a cluster system.

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	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBS_START/jbs_start.log[.old] • <i>shared-directory</i>/jplbase/log/JBS_START/jbs_start.log[.old] 	128 KB	When the command is executed
JP1/Base shutdown log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBS_STOP/jbs_stop.log[.old] • <i>shared-directory</i>/jplbase/log/JBS_STOP/jbs_stop.log[.old] 	128 KB	When the command is executed
Process management log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBS_SPMD{1 2 3}.log • <i>shared-directory</i>/jplbase/log/JBS_SPMD{1 2 3}.log 	384 KB	128 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBS_SPMD_COMMAND{1 2 3}.log • <i>shared-directory</i>/jplbase/log/JBS_SPMD_COMMAND{1 2 3}.log 	384 KB	128 KB
Authentication server log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jbssessionapi.log{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/jbssessionapi.log{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jbssessionmgr{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/jbssessionmgr{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jbssessionmgr_trace{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/jbssessionmgr_trace{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
Log of the authentication server setting command	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBSSESS{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JBSSESS{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
Command execution log (ISAM) ^{#1}	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/actisamlogv8.DAT • <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.DAT 	1.2 GB ^{#2}	None
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/actisamlogv8.K01 • <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.K01 	2 MB ^{#2}	None
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/actisamlogv8.DEF • <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.DEF 	1 KB	When the command is executed
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/cmdisamlogv8.DAT • <i>shared-directory</i>/jplbase/log/COMMAND/cmdisamlogv8.DAT 	1.2 GB ^{#2}	None
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/cmdisamlogv8.K01 • <i>shared-directory</i>/jplbase/log/COMMAND/cmdisamlogv8.K01 	2 MB ^{#2}	None

Log type	File name/directory name	Max. disk space	File changing timing
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/cmdisamlogv8.DEF • <i>shared-directory</i>/jplbase/log/COMMAND/cmdisamlogv8.DEF 	1 KB	When the command is executed
Common definition information log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBSCNFCMD/JBSCNFCMD{1 2}.log 	128 KB	64 KB
Log of jplhosts information command	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBSCNFCMD/JBSCOMMCMD{1 2}.log 	128 KB	64 KB
User mapping command log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBSUMAPCMD/JBSUMAPCMD{1 2}.log • <i>shared-directory</i>/jplbase/log/JBSUMAPCMD/JBSUMAPCMD{1 2}.log 	128 KB	64 KB
Remote command log ^{#1}	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmd_result{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmd_result{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdapi{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdapi{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdapi_trace{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdapi_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdcmc{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdcmc{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdcmc_trace{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdcmc_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdcom{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdcom{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdcom_trace{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdcom_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdexe{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdexe{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdexe_trace{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdexe_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB

Log type	File name/directory name	Max. disk space	File changing timing
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdrouter{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdrouter{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/jcocmdrouter_trace{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/jcocmdrouter_trace{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JCOCMD/JCOCMDCMD{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/JCOCMD/JCOCMDCMD{1 2 3 4 5 6 7 8}.log 	20 MB	2.5 MB
Plug-in service log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsplugin{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbsplugin{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsplugincom_{0 1 2 3 4 5 6 7 8 9}#3_{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbsplugincom_{0 1 2 3 4 5 6 7 8 9}#3_{1 2 3 4 5 6 7 8}.log 	50 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsplugincmd{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbsplugincmd{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbspluginmgrapi{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbspluginmgrapi{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsplugincomapi{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbsplugincomapi{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsplugincmdapi{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbsplugincmdapi{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbspluginhcshm{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbspluginhcshm{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsrmtcmd{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbspluginremotecmd{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/plugin/jbspluginremotecmd{1 2 3 4 5 6 7 8}.log 	5 MB	640 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/plugin/jbsrmtapi{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
Installation log	• /tmp/HITACHI_JP1_INST_LOG/jp1base_inst{1 2 3 4 5}.log	128 KB	At installation
	• /etc/.hitachi/.hliclog/hliclibtrc{1 2 3 4 5}.log	10 MB	2 MB
	• /etc/.hitachi/.hliclog/hliclibmgrtrc{1 2 3 4 5}.log	10 MB	2 MB
	• /etc/.hitachi/.hliclog/hlicliberr{1 2 3 4 5}.log	50 KB	10 KB
	• /etc/.hitachi/.hliclog/hliclibmgrerr{1 2 3 4 5}.log	50 KB	10 KB
	• /etc/.hitachi/.hliclog/hliccmd{1 2 3 4 5}.log	1 MB	At startup of Hitachi Program Product Installer
	• /tmp/rf/hrf4securityinstall{1 2}.log	4 MB	If 1 MB is exceeded when installation is executed
	• /tmp/rf/hrf4installhitachi.log	10 MB	At installation
	• /tmp/rf/hrf4unknowninstall{1 2}.log	4 MB	If 1 MB is exceeded when installation is executed
Setup log	• /var/opt/jp1base/log/JBS_SETUP/jbs_setup.log	--	None ^{#15}
Configuration management log ^{#1}	• /var/opt/jp1base/log/route/JBSRT{1 2 3 4 5}.log • <i>shared-directory</i> /jp1base/log/route/JBSRT{1 2 3 4 5}.log	20 MB	4 MB
Log of the health check function (local host monitoring)	• /var/opt/jp1base/log/jbshc/jbshc{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i> /jp1base/log/jbshc/jbshc{1 2 3 4 5 6 7 8}.log	50 MB	6.25 MB
Log of the health check function (remote host monitoring)	• /var/opt/jp1base/log/jbshc/jbshc{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i> /jp1base/log/jbshc/jbshc{1 2 3 4 5 6 7 8}.log	50 MB	6.25 MB
Log of the health check commands	• /var/opt/jp1base/log/jbshc/jbshcstatus{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i> /jp1base/log/jbshc/jbshcstatus{1 2 3 4 5 6 7 8}.log	50 MB	6.25 MB
Log of the health check API	• /var/opt/jp1base/log/jbshc/jbshcapi{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i> /jp1base/log/jbshc/jbshcapi{1 2 3 4 5 6 7 8}.log	50 MB	6.25 MB
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 • <i>shared-directory</i> /jp1base/log/jbshc/jbshcshmctl{1 2 3 4 5 6 7 8}.log	50 MB	6.25 MB

Log type	File name/directory name	Max. disk space	File changing timing
Operation log	<ul style="list-style-type: none"> • /var/opt/jplbase/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	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/jevdef_get.{000 001 002}^{#6} • <i>shared-directory</i>/event/jevdef_get.{000 001 002}^{#6} 	192 KB	When the command is executed
Trace log for event setting, centralized management, and distribution command	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/jevdef_distrib.{000 001 002}^{#6} • <i>shared-directory</i>/event/jevdef_distrib.{000 001 002}^{#6} 	192 KB	When the command is executed
Trace log of the event service	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/trace.{000 001 002 003 004}^{#6, #7} • <i>shared-directory</i>/event/trace.{000 001 002 003 004}^{#6, #7} 	12.5 MB ^{#7}	When the event service starts
	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/imevterr.{000 001 002 003 004}^{#6, #7} • <i>shared-directory</i>/event/imevterr.{000 001 002 003 004}^{#6, #7} 	5 MB ^{#7}	When the event service starts
	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/imses.{log old}^{#6} • <i>shared-directory</i>/event/imses.{log old}^{#6} 	2 MB	When the event service starts
Transfer error log of the event service	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/fwderr.{000 001 002 003 004}^{#6, #7} • <i>shared-directory</i>/event/fwderr.{000 001 002 003 004}^{#6, #7} 	5 MB ^{#7}	When the event service starts
Error log of the event service	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/error.{000 001 002 003 004}^{#6, #7} • <i>shared-directory</i>/event/error.{000 001 002 003 004}^{#6, #7} 	2,500 KB ^{#7}	When the event service starts
Log of the event service API.	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/IMEvapi.{000 001 002 003 004}^{#8} 	5 MB ^{#8}	1 MB ^{#8}
Log of the event service	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/IMEvenc.{000 001 002 003 004} 	5 MB	1 MB
Error information generated during communication between the event registration/reception process and the event service	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/sock.log 	1 KB	1 KB
Error log of the log file trap	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/logtrap/.errorfile.ID-number 	A few hundred bytes ^{#9}	When the log file trap starts
Log of the log file trap	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/logtrap/jevtraplog/jevtraplog.{000 001 002 003 004} 	5 MB ^{#10}	1 MB ^{#10}
Log-file trap startup execution results log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jevlog_start/jevlog_start{1 2 3}.log^{#13#14} 	3 MB	1 MB

Log type	File name/directory name	Max. disk space	File changing timing
Remote monitoring log (log-file trap)	<ul style="list-style-type: none"> /var/opt/jplbase/sys/tmp/event/logtrap/jelallog/jelallog{1-5}.log 	5 MB	1 MB
Trace log of the jbs_killall.cluster command ^{#11}	<ul style="list-style-type: none"> shared-directory/jplbase/log/ jbs_killall.cluster[{1 2 3 4}] 	256 KB	When the command is executed
Trace log for inter-process communication	<ul style="list-style-type: none"> /var/opt/jplbase/log/JBSCOM/jbscomd {1 2 3 4}.log shared-directory/jplbase/log/JBSCOM/jbscomd{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> /var/opt/jplbase/log/JBSCOM/jbscomd_api {1 2 3 4}.log shared-directory/jplbase/log/JBSCOM/jbscomd_api{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> /var/opt/jplbase/log/JBSCOM/jbscomd_snd{1 2 3 4}.log shared-directory/jplbase/log/JBSCOM/jbscomd_snd{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> /var/opt/jplbase/log/JBSCOM/jbscomd_rcv{1 2 3 4}.log shared-directory/jplbase/log/JBSCOM/jbscomd_rcv{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> /var/opt/jplbase/log/JBSCOM/command {1 2 3 4}.log shared-directory/jplbase/log/JBSCOM/command{1 2 3 4}.log 	10 MB	2.5 MB
	<ul style="list-style-type: none"> /var/opt/jplbase/log/JBSCOM/command {1 2 3 4}.log shared-directory/jplbase/log/JBSCOM/command{1 2 3 4}.log 	10 MB	2.5 MB
Error log of the command for collecting operating information	<ul style="list-style-type: none"> /var/opt/jplbase/log/jbsopi/jbsopi_cmd{1 2 3 4 5}.log 	5 MB	1 MB
Log for the operating information API	<ul style="list-style-type: none"> /var/opt/jplbase/log/jbsopi/jbsopi_api{1 2 3 4 5}.log shared-directory/jplbase/log/jbsopi/jbsopi_api{1 2 3 4 5}.log 	5 MB	1 MB
Log of the service management control	<ul style="list-style-type: none"> /var/opt/jplbase/log/jbssrvmgr/jbssrvmgr{1 2 3 4}.log shared-directory/jplbase/log/jbssrvmgr/jbssrvmgr{1 2 3 4}.log 	10 MB	2.5 MB
Trace log of the service management control	<ul style="list-style-type: none"> /var/opt/jplbase/log/jbssrvmgr/jbssrvmgr_trace{1 2 3 4}.log shared-directory/jplbase/log/jbssrvmgr/jbssrvmgr_trace{1 2 3 4}.log 	10 MB	2.5 MB
Log of the service management control API	<ul style="list-style-type: none"> /var/opt/jplbase/log/jbssrvmgr/jbssrvmgr_api{1 2 3 4}.log shared-directory/jplbase/log/jbssrvmgr/jbssrvmgr_api{1 2 3 4}.log 	10 MB	2.5 MB
Local action execution log	<ul style="list-style-type: none"> /var/opt/jplbase/log/lcact/localact{1-n}^{#12}.log shared-directory/jplbase/log/lcact/localact{1-n}^{#12}.log 	1,024 KB ^{#12}	256 KB ^{#12}

Log type	File name/directory name	Max. disk space	File changing timing
Local action log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jbslcact/jbslcact{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/jbslcact/jbslcact{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jbslcact/jbslcact_list{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/jbslcact/jbslcact_list{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jbslcact/jbslcact_cancel{1 2 3 4 5 6 7 8}.log • <i>shared-directory</i>/jplbase/log/jbslcact/jbslcact_cancel{1 2 3 4 5 6 7 8}.log 	2,048 KB	256 KB
JP1/Base administrator settings command log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBS_SETUP/jbssetadmingrp{1 2}.log 	128 KB	64 KB
JP1/Base communications base log	<ul style="list-style-type: none"> • /var/opt/jplbase/log/jp1BsComm/error{1 2 3 4 5}.log 	5 MB	1 MB
Individual log for the setup information collection command	<ul style="list-style-type: none"> • /var/opt/jplbase/log/JBS_SETUP/JBSPARAMDUMP{1 2}.log 	2 MB	1 MB
Log for recording starting and stopping of forwarding suppression	<ul style="list-style-type: none"> • /etc/opt/jplbase/conf/event/servers/default/suppress/<i>agent-host-name</i>/{log log.old}^{#6} 	128 KB	64 KB
Trace log for the event-forwarding suppression command	<ul style="list-style-type: none"> • /var/opt/jplbase/sys/tmp/event/servers/default/jevagtfw.{000 001 002 003 004}^{#6} 	5 MB	1 MB

#1: Log file for JP1/IM - Manager

#2: You can use the `jccocmdef` 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 records is 20,000 (the default setting)
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 [1.5 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 16. 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 16. Definition Files](#).

#9: 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.

#10: 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 16. Definition Files](#).

#11: A log file output when the `jbs_killall.cluster` command executes in a cluster system.

#12: 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 *16. Definition Files*.

#13: Logs are output in HNTRLib2 format (multi-process trace).

#14: When deleting this log data, also delete the `mmap` directory at the output destination.

#15: Log data is output only when an environment is configured, for example, at the time of installation.

B. List of Processes

This appendix describes the processes for JP1/Base.

B.1 List of processes (in Windows)

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 (2)	Starts the Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
hntr2mon.exe (2)	Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
jbs_service.exe (1)	Starts the JP1/Base process management ^{#1}	--	--
jbs_spmd.exe (1)	JP1/Base process management ^{#1}	jbsessionmgr.exe (1) ^{#2, #3}	Authentication server ^{#1#6} This process exists only on the host that is set as the authentication server. The displayed name is jbsessionmgr when the jbs_spmd_status command is executed.
		jbsroute.exe (1) ^{#2}	Configuration management ^{#1#6} 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)) jcocmdcom.exe (1) ^{#5}	Command execution ^{#1#6} The displayed name is jcocmd when the jbs_spmd_status command is executed.
		jbsplugind.exe (1) ^{#2}	Plug-in service ^{#1#6} The displayed name is jbsplugin when the jbs_spmd_status command is executed.
		jbshcd.exe (1)	Health check (for local host monitoring) ^{#1#6} The displayed name is jbshcd when the jbs_spmd_status command is executed.
		jbshchostd.exe (1)	Health check (for remote host monitoring) ^{#1#6}

Parent process name	Function	Child process name	Function
			The displayed name is jbschostd when the jbs_spm�_status command is executed.
		jbsrvmgr.exe (1)	Service management control function#1#6 The displayed name is jbsrvmgr when the jbs_spm�_status command is executed.
		jbslcact.exe (1)	Local action function#1#6 The displayed name is jbslcact when the jbs_spm�_status command is executed.
		jbscmd.exe (1) jbscmd_api.exe (1) jbscmd_ses.exe (1) jbscmd_snd.exe (1) jbscmd_rcv.exe (1)	Inter-process communication#1#6 The displayed name is jbscmd when the jbs_spm�_status command is executed.
jbpmsrvcecon.exe (1)#3	Startup control	powendar.exe (1)	Power control This sub-process is generated when JP1/Power Monitor is installed.
jevservice.exe (1)	Event service#1#7	--	--
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.

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: $(\text{number-of-logical-hosts} + 1) \times \text{number-of-processes}$

#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 [4. 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: This process was added in 08-00.

#6: You can use the jbs_spm�_status command to check the status of these processes. If the processes have started normally, the jbs_spm�_status command returns the following information.

- If an authentication server has been set:

```
jbsessionmgr
jbsroute
jcccmd
jbsplugin
jbsbcd
```

```

jbschostd
jbsrvmgr
jbslcact
jbscmd

```

- If an authentication server has not been set:

```

jbsroute
jccmd
jbsplugin
jbscd
jbschostd
jbsrvmgr
jbslcact
jbscmd

```

#7: 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 List of processes (in UNIX)

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)	--	--
jbs_spmd (1)	Process management ^{#1}	jbsessionmgr (1) ^{#2}	Authentication server ^{#1#5} This process exists only on the host that is set as the authentication server. The displayed name is <code>jbsessionmgr</code> when the <code>jbs_spmd_status</code> command is executed.
		jbsroute (1 to 9) ^{#2}	Configuration management ^{#1#5} The displayed name is <code>jbsroute</code> when the <code>jbs_spmd_status</code> command is executed.
		jccmd (1) ^{#2} jccmdexe (1) jccmdapi (Execute Command window count ^{#3} + 1 (when JP1/IM - Manager is installed)) jccmdcmc (0 to the command count ^{#4}) jccmdcom (1) ^{#8}	Command execution ^{#1#5} The displayed name is <code>jccmd</code> when the <code>jbs_spmd_status</code> command is executed.
		jbsplugind (1) ^{#2, #7}	Plug-in service ^{#1#5} The displayed name is <code>jbsplugin</code> when the <code>jbs_spmd_status</code> command is executed.
		jbscd (1)	Health check (for local host monitoring) ^{#1#5}

Parent process name	Function	Child process name	Function
			The displayed name is jbsbcd when the jbs_spmd_status command is executed.
		jbshchostd (1)	Health check (for remote host monitoring) ^{#1#5} The displayed name is jbschostd when the jbs_spmd_status command is executed.
		jbssrvmgr (1)	Service management control function ^{#1#5} The displayed name is jbsrvmgr when the jbs_spmd_status command is executed.
		jbslact (1)	Local action function ^{#1#5} The displayed name is jbslact when the jbs_spmd_status command is executed.
		jbsscmd (1) jbsscmd_api (1) jbsscmd_ses (1) jbsscmd_snd (1) jbsscmd_rcv (1)	Inter-process communication ^{#1#5} The displayed name is jbscmd when the jbs_spmd_status command is executed.
jevservice (1)	Event service ^{#1#6}	jevservice (5 to 9,999)	--
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.
		jelalog (0 to the number of times a log file trapping process has been started)	The jelalog process is generated for each remote monitoring log file trap process started from the Display/Edit Profiles window of JP1/IM. When the process is stopped, the jelalog process disappears.

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: $(\text{number-of-logical-hosts} + 1) \times \text{number-of-processes}$

#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 [4. 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:

```

jbsessionmgr
jbsroute
jcccmd
jbsplugin
jbsbcd
jbschostd

```

jbssrvmgr
jbslcact
jbscomd

- If an authentication server has not been set:

jbstroute
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-ef` command is `jbsplugin`.

#8: This process was added in version 07-51.

C. List of Port Numbers

JP1/Base uses the TCP/IP protocol for communication. These port numbers are set by default when the product ships.

Note:

When JP1/Base is used in an environment in which the Windows firewall is enabled, you must register the port number used by JP1/Base to the exception list. For details about settings for the Windows firewall, see [C.4 Settings for the Windows firewall](#).

C.1 Port numbers for JP1/Base

When a connection is established, the connection destination uses a port number in the table below. The connection source, which tries to connect to the port number, uses a port number that is assigned by the OS from free port numbers (ephemeral ports). The range of port numbers available depends on the OS.

Table C–1: Port numbers for JP1/Base

Service name	Port number	Purpose
jplimevt	20098/tcp	Transferring JP1 events to another host
jplimevtapi	20099/tcp	All the products that register and obtain JP1 events, and functions for issuing and acquiring JP1 events
jplimrt	20237/tcp	Configuration management (when using JP1/IM - Manager)
jplimcmda	20238/tcp	Command execution (when using JP1/IM - Manager)
jplimcmdc	20239/tcp	Command execution (when using JP1/IM - Manager)
jplbsuser	20240/tcp	User authentication server
jplbsplugin	20306/tcp	Used to collect and distribute JP1/IM definition information, used by the JP1/Base health check function, and used by the <code>jevagt fw</code> command for event forwarding suppression
jplbscom	20600/tcp	Used for communication between JP1/IM configuration management and service management control
ldap	389/tcp [#]	Used for linkage with a directory server
ldaps	636/tcp [#]	

[#]: 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

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
jplimevt	20098/tcp	JP1/Base that transfers JP1 events -> JP1/Base that receives JP1 events
jplimevtapi	20099/tcp	A program such as JP1/IM - Manager that obtains JP1 events -> JP1/Base

Service name	Port number	Direction in which data passes through the firewall
jplimrt	20237/tcp	JP1/IM - Manager -> JP1/Base Upper-layer JP1/IM - Manager -> lower-layer JP1/IM - Manager
jplimcmda	20238/tcp	JP1/IM - View -> JP1/Base on the host where JP1/IM - Manager is installed JP1/IM - Manager -> JP1/Base
jplimcmdc	20239/tcp	JP1/Base on the host running JP1/IM - Manager <--> JP1/Base on the host that executes the command
jplbsuser	20240/tcp	JP1/IM - Manager -> JP1/Base JP1/AJS - Manager -> JP1/Base JP1/AJS - Agent -> JP1/Base
jplbsplugin	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
jplbscom	20600/tcp	JP1/IM - Manager <--> JP1/Base on a different host Upper-layer JP1/IM - Manager <--> lower-layer JP1/IM - Manager
ldap	389/tcp [#]	JP1/Base (authentication server) -> Directory server
ldaps	636/tcp [#]	
ICMP	--	JP1/Base (jplping) -> JP1/Base on a different host

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).
- : None

[#]: 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

Table C-3: Connection status

Service name	Port number	Connection status
jplimevt	20098/tcp	When <code>keep-alive</code> is specified in the <code>remote-server</code> parameter in the event server settings file (<code>conf</code>), the connection is maintained. To forcibly close the connection, specify <code>close</code> in this parameter.
jplimevtapi	20099/tcp	When <code>keep-alive</code> is specified in the <code>server</code> parameter in the API settings file (<code>api</code>), the connection is maintained. To forcibly close the connection, specify <code>close</code> in this parameter.
jplimrt	20237/tcp	A connection is established only when required.

Service name	Port number	Connection status
jplimcmda	20238/tcp	The connection is maintained. If the connection is forcibly terminated, you must re-execute the command.
jplimcmdc	20239/tcp	The connection is maintained. ^{#1} If the connection is forcibly terminated, the service is automatically reconnected.
jplbsuser	20240/tcp	A connection is established only when required.
jplbspplugin	20306/tcp	A connection is established only when required.
jplbscom	20600/tcp	A connection is established only when required.
ldap	389/tcp ^{#2}	A connection is established only when required.
ldaps	636/tcp ^{#2}	A connection is established only when required.

#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.

C.4 Settings for the Windows firewall

Port numbers and programs required by the system must be registered in the exceptions list, or Windows Firewall needs to be turned off, to prevent JP1/Base communications from being blocked by Windows Firewall.

Register the port numbers and programs in the exceptions list using procedure (a) or (b) below.

(a) From the Control Panel, choose **Windows Firewall** and the **Exceptions** page. Then register the following programs or ports.

Program registration:

In the **Add a Program** dialog box, click **Browse** and add the following information:

- File name: (installation-directory) `jbssessionmgr.exe`
- File name: (installation-directory) `jbsroute.exe`
- File name: (installation-directory) `jcocmd.exe`
- File name: (installation-directory) `jcocmdapi.exe`
- File name: (installation-directory) `jevservice.exe`
- File name: (installation-directory) `jbsplugind.exe`
- File name: (installation-directory) `jbscomd_snd.exe`
- File name: (installation-directory) `jbscomd_rcv.exe`

Note:

To send and receive events using the pre-Version 6 products JP1/SES and JP1/AJS, or products such as JP1/OJE that use JP1/SES protocol, you must add the following information:

- File name: (installation-directory) `jevsessvc.exe`

Port number registration:

Click **Add Port** and register the following information:

- Port number: `tcp jplimevt, 20098`

- Port number: tcp jplimevtapi, 20099
- Port number: tcp jplimrt, 20237
- Port number: tcp jplimcmda, 20238
- Port number: tcp jplimcmdc, 20239
- Port number: tcp jplbsuser, 20240
- Port number: tcp jplbsplugin, 20306
- Port number: tcp jplbscom, 20600
- Name : JP1 Base

Note:

To send and receive events using the pre-Version 6 JP1/SES or JP1/AJS, or products such as JP1/OJE that use JP1/SES protocol, you must add the following information:

- Port number: tcp JP1AutoJob, user-specified port
- Name : JP1 Base

(b) Register the above information using the following commands. Note that you need administrator permissions to execute this command.

Program registration:

```
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jbsessionmgr.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jbsroute.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jcocmd.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jcocmdapi.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jevservice.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jbsplugind.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jbscomd_snd.exe" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jbscomd_rcv.exe" enable=yes
```

Note:

To send and receive events using the pre-Version 6 JP1/SES or JP1/AJS, or products such as JP1/OJE that use JP1/SES protocol, you must register the following information:

```
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow program="(installation-directory)\bin\jevsessvc.exe" enable=yes
```

Port number registration:

```
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow protocol=TCP localport=20098 description="jplimevt" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow protocol=TCP localport=20099 description="jplimevtapi" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow protocol=TCP localport=20237 description="jplimrt" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow protocol=TCP localport=20238 description="jplimcmda" enable=yes
```

```
otocol=TCP localport=20238 description="jplimcmda" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow pr
otocol=TCP localport=20239 description="jplimcmdc" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow pr
otocol=TCP localport=20240 description="jplbsuser" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow pr
otocol=TCP localport=20306 description="jplbsplugin" enable=yes
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allow pr
otocol=TCP localport=20600 description="jplbscom" enable=yes
```

Note:

To send and receive events using the pre-Version 6 JP1/SES or JP1/AJS, or products such as JP1/OJE that use JP1/SES protocol, you must register the following information:

```
netsh advfirewall firewall add rule name="JP1/Base" dir=in action=allo
w protocol=TCP localport=user-specified-port description="JP1AutoJob" e
nable=yes
```

Registration is completed if the above information appears in the Programs and Services list and the check box of each service is selected. To remove a registered program or service from the exceptions, select it in the Programs and Services list and then click the **Delete** button. To temporarily remove a registered program or service from the exceptions, clear its check box.

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, forwarding settings file, and distribution definition file)	1,023 bytes
Maximum length of a filter for a forwarding settings file	64 kilobytes
Maximum length of an event server name	If you do not use the encryption function (<code>jp1bsagent</code> is not configured to <code>BASESSL</code> in the SSL communication definition file). 240 bytes for Windows 255 bytes for Linux 255 bytes for AIX If you use the encryption function (<code>jp1bsagent</code> is not configured to <code>BASESSL</code> in the SSL communication definition file). 240 bytes for Windows 63 bytes for Linux 61 bytes for AIX
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.)
OS user password	1 to 64 bytes
Information-search-user-name	8 to 64 bytes (including <code>aduser/</code>)
Maximum length of a server host name	255 bytes
Maximum length of a logical host name	180 bytes for Windows [#] 32 bytes for Linux [#] 32 bytes for AIX [#] If you use the <code>jbs_killall.cluster</code> command (UNIX only): 32 bytes
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 OS users that can be registered	2,048 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
Maximum file size of a forwarding setting file or an additional extended attribute settings file	2 gigabytes

#: 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. Do not exceed the limitation of the higher-level products such as JP1/IM-Manager or JP1/AJS3 if you install the JP1/Base and the higher-level products in the same server.

E. Estimating memory and disk space requirements

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 describes the regular expressions that can be used by default in 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 [3.4.5 Extending regular expressions to be used](#). AIX use extended regular expressions that conform to the XPG4 standard, and Linux uses extended regular expressions that conform to the POSIX1003.2 standard. 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.

`string$`

Signifies that the specified string is at the end of a line. 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 among regular expressions that can be used

The following table lists major items for regular expressions usable with the initial settings, and regular expressions usable in extended regular expressions.

Method	Meaning	In Windows: (JP1-specific regular expressions)	In UNIX: (basic regular expressions)#1	In Windows: (extended regular expressions)#3	In UNIX: (extended regular expressions)#2
Character string	Signifies the line with the specified string.	Y	Y	Y	Y
<i>^string</i>	Signifies that the specified string is at the beginning of a line.	Y	Y	Y	Y
<i>string\$</i>	Signifies that the specified string is at the end of a line.	Y	Y	Y	Y
<i>^string\$</i>	Signifies the line that contains the specified string only.	Y	Y	Y	Y
<i>^\$</i>	Signifies a blank line.	Y	Y	Y	Y
(period)	Signifies any single character.	Y	Y	Y	Y
. *	Combination of a period (.) and asterisk (*). Matches any character string.	Y	Y	Y	Y
[<i>string</i>]	Signifies any of the characters specified in the string enclosed by [and].	N	Y	Y	Y
[<i>^string</i>]	Signifies characters other than those specified in the string enclosed by [and].	N	Y	Y	Y
[<i>character-character</i>]	Signifies a single character within the range, in the ascending order of character codes.	N	Y	Y	Y
[<i>^character-character</i>]	Signifies a single character out of the range, in the ascending order of character codes.	N	Y	Y	Y
<i>character*</i>	Signifies the string in which the immediately preceding character is repeated at least zero times.	Y	Y	Y	Y
<i>character+</i>	Signifies the string in which the immediately preceding character is repeated at least one time.	N	N	Y	Y
<i>character?</i>	Signifies the string in which the immediately	N	N	Y	Y

Method	Meaning	In Windows: (JP1-specific regular expressions)	In UNIX: (basic regular expressions) ^{#1}	In Windows: (extended regular expressions) ^{#3}	In UNIX: (extended regular expressions) ^{#2}
	preceding character is not repeated or only one time.				
<i>Character{n}</i>	Signifies the string in which the immediately preceding character is repeated at least n times.	N	N	Y	Y
<i>Character{n,}</i>	Signifies the string in which the immediately preceding character is repeated at least n times.	N	N	Y	Y
<i>Character{n,m}</i>	Signifies the string in which the immediately preceding character is repeated at least n times, but m times or less.	N	N	Y	Y
<i>regular-expression regular-expression</i>	Signifies either the right or left regular expressions.	N	N	Y	Y
<i>\special-character</i>	Handles a special character as an ordinary character.	Y	Y	Y	Y
<i>(regular-expression)</i>	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. For details on the regular expressions that other products use by default, see the manual for each product.

#2: If regular expressions are extended, the extended regular expressions that are applied differ by OS. AIX uses extended regular expressions that conform to the XPG4 standard, and Linux uses extended regular expressions that conform to the POSIX1003.2 standard. 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

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

Specification	Meaning	String specified as a regular expression	Example character string	Match
<i>character-string</i>	Match lines containing the specified string.	spring	spring has come.	Yes
			winter-summer-autumn- spring	Yes
			---- spring -----	Yes
^ <i>character-string</i>	Match lines beginning with the specified string.	^spring	spring has come.	Yes
			winter-summer-autumn-spring	--
			-----spring-----	--
<i>character-string</i> \$	Match lines ending with the specified string.	spring\$	spring has come.	--
			winter-summer-autumn- spring	Yes
			-----spring-----	--
^ <i>character-string</i> \$	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	winter has come.	Yes
			mother of in vention	Yes
			life is in everything	Yes
			eight nine ten	--
			increasing population	--
		s..ing	picnic in spring	Yes
	skiing in winter	Yes		
[<i>character-string</i>]	Signifies any of the characters specified in the string enclosed by [and].	[pr]	spring has come.	Yes
			today is Monday.	--
[<i>character-character</i>]	Signifies a single character within the range, in the ascending order of character codes.	[a-i]	spring has come .	Yes
[<i>character-character</i>]	Signifies a single character out of the range, in the ascending order of character codes.	[^a-i]	spring has come .	Yes
<i>character</i> *	Match strings containing zero or	ro*m	terminal	Yes
			cd- rom	Yes

Specification	Meaning	String specified as a regular expression	Example character string	Match
	more repetitions of the preceding characters.		living room	Yes
		h.*n	This is a pen.	Yes
			That is an apple.	Yes
<i>regular-expression</i> <i>regular-expression</i>	Signifies either of the right and left regular expressions.	[0-9]+ apple	That is an apple.	Yes
			spring in 2003	Yes
<i>\ special-character</i>	Handles a special character as an ordinary character.	o\.h	<stdi o.h >	Yes
			another man	--
<i>(regular-expression)</i>	Groups regular expressions.	i(n.e ng)	w inter has come.	Yes
			interesting 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.

The following describes the kernel parameters you must add or adjust to run JP1/Base.

In the *Parameters to be added* tables, to each parameter add the estimated values (total) for all programs used in the system.

In the *Parameters to be adjusted* tables, for each parameter check the estimate for all programs used in the system, and then optimize the value so that no problems will occur with JP1/Base or any other program.

G.1 List of Kernel Parameters (in AIX)

Kernel parameters do not need to be adjusted in AIX.

G.2 List of Kernel Parameters (in Linux)

(1) Adjusting the Default System Resource Settings

The table below shows the estimated values for the default system resource settings that need to be adjusted to run JP1/Base.

(a) Parameters to be added

System resource	Parameter	Estimate
File system	fs.file-max	For the event service #1 : $180 + \text{Number of transfer destination hosts} \times 6 + \text{Number of hosts that transfer an event} \times 6 + \text{Number of simultaneously issued events}^{\#2} \times 6 + \text{Number of programs that acquire an event}^{\#3} \times 6 + \text{Number of event service operation commands to be simultaneously executed} \times 10$
		For log file trapping: $\text{Number of operating log file traps} \times 9 + \text{Total number of files to be monitored by one log file trap} \times 9 + \text{Number of log file trap operation commands to be simultaneously executed} \times 10 + \text{Number of profiles for remote monitoring in IM-Configuration Management} \times 10$
		For processes others than the event service and log file trapping: $60 + \text{Number of command execution for JP1/Base} \times 10$

#1:

For logical hosts, get an estimate by using the following formula:

$180 + \text{number-of-transfer-destination-hosts} \times 6 + \text{number-of-hosts-that-transfer-events} \times 6 + \text{number-of-simultaneously-issued-events} \times 6 + \text{number-of-programs-that-acquire-events} \times 6$

#2:

An event is issued using a `jevsend` command, a `jevsendd` command, a JP1/AJS event-sending job, other programs in a JP1 series, and user programs created using the JP1/Base extension function. The number of simultaneously issued events is the maximum number of events

obtained when these programs are executed simultaneously. The time in which programs are simultaneously executed varies depending on the performance of the machine. Assume that the time is approximately one second.

#3:

An event is acquired using a JP1/AJS event-receiving job and a user program created using the JP1/Base extension function. The number of programs that acquire an event is the number of these programs that are running.

Notes:

See the manual for the operating system you are using, and estimate the value that is described in the manual. If the kernel parameters cannot be set, then this setting is not necessary.

(b) Parameters to be adjusted

System resource	Parameter	Estimate
Socket backlog	<code>net.core.somaxconn</code> [#]	1,024 or greater

#: For the `net.core.somaxconn` parameter, specify 1024 or more if the system is running as an agent of JP1/IM Configuration Management.

(2) When using the command execution function

The tables below show the estimated values for the kernel parameters that need to be adjusted to run JP1/Base when using remote commands and automated actions issued from JP1/IM - Manager.

(a) Parameters to be added

System resource	Parameter	Estimate
File system	<code>fs.file-max</code>	<i>Number of remote commands to be simultaneously executed using JP1/IM - Manager</i> × 16
Shared memory	<code>kernel.shmall</code>	<i>Estimated value of kernel.shmmni</i> × <i>Estimated value of kernel.shmmax</i>
	<code>kernel.shmmni</code>	1 + <i>Number of concurrently executable remote commands</i> [#]
Semaphore	The fourth field in <code>kernel.sem (SEMMNI)</code>	3
	The second field in <code>kernel.sem (SEMMNS)</code>	3

#: If the total estimate exceeds 256, assume 256 in the calculations. Estimate this value for the host on which commands are executed.

(b) Parameters to be adjusted

System resource	Parameter	Estimate
Shared memory	<code>kernel.shmmax</code>	143,468 or greater

(3) When using the health check function

The tables below show the estimated values for the system resource settings that need to be adjusted to run JP1/Base when using the JP1/Base health check function.

(a) Parameters to be added

System resource	Parameter	Estimate
Shared memory	<code>kernel.shmall</code>	<i>Estimated value of <code>kernel.shmmni</code> × Estimated value of <code>kernel.shmmax</code></i>
	<code>kernel.shmmni</code>	<i>10 + 10 × Number of logical hosts</i>

(b) Parameters to be adjusted

System resource	Parameter	Estimate
Shared memory	<code>kernel.shmmax</code>	215,644 or greater

(4) When a local action function is used

The estimated value of system resources that must be adjusted as JP1/Base when a local action function is used is shown below.

(a) Parameters to be added

System resource	Parameter	Estimate
File system	<code>fs.file-max</code>	Number of concurrently executable local actions

H. Handling Changes in Communication Settings

The JP1/Base communication settings can be changed according to the network configuration, so that JP1/Base supports various network configurations. You might need to change the communication protocol to suit your network environment and the manner in which you use JP1/Base. The following describes the files and parameters that define the communication settings for JP1/Base.

H.1 Changing the settings in the `jp1hosts2` definition file

A `jp1hosts2` definition file contains hosts information specific to JP1. Reasons you might use a `jp1hosts2` definition file include being unable to use the operating system's name resolution process, wanting JP1/Base to communicate using a specific LAN in an environment with multiple LAN connections, and wanting the local host in a cluster system to use multiple IP addresses for reception. This file also allows JP1/Base to communicate using IPv6 addresses.

JP1/Base uses the name resolution process of the OS for host names not defined in the hosts information. Depending on your network environment, you might need to configure a communication protocol settings file. For details on the `jp1hosts2` definition file, see *jp1hosts2 definition file* in *16. Definition Files*.

Examples of situations where communication settings need to be changed:

- The name resolution process of the operating system cannot resolve the destination host name, or obtains an address that is not the preferred IP address
- You want JP1/Base to use multiple LANs for receiving in a cluster system environment with multiple LAN connections
- You want JP1/Base to use a specific LAN for receiving in an environment with multiple LAN connections
- In a Windows environment, you want to run JP1/Base services on physical and logical hosts on the same host
- You want JP1/Base to use a specific LAN for sending in an environment with multiple LAN connections
- You want JP1/Base to communicate using IPv6 addresses

H.2 Changing the settings in the `jp1hosts` definition file

A `jp1hosts` definition file contains hosts information specific to JP1. You might use a `jp1hosts` definition file when you cannot use the operating system's name resolution process, you want JP1/Base to communicate using a specific LAN in an environment with multiple LAN connections, or you want the local host in a cluster system to use multiple IP addresses for reception.

JP1/Base uses the name resolution process of the OS for host names not defined in the hosts information. Depending on your network environment, you might need to configure a communication protocol settings file. For details on the `jp1hosts` definition file, see *jp1hosts definition file* in *16. Definition Files*.

Example situations where communication settings need to be changed:

- The name resolution process of the operating system cannot resolve the destination host name, or obtains an IP address that is not the preferred IP address
- You want JP1/Base to use multiple LANs for receiving in a cluster system environment with multiple LAN connections
- You want JP1/Base to use a specific LAN for receiving in an environment with multiple LAN connections

- In a Windows environment, you want to run JP1/Base services on physical and logical hosts on the same host
- You want JP1/Base to use a specific LAN for sending in an environment with multiple LAN connections

H.3 Changing the settings in the communication protocol settings files

Use communication protocol settings files when you want to change the transmission setting to the ANY binding method in a cluster system, or use a specific LAN to communicate in an environment with multiple LAN connections. To perform name resolution, you might need to set a `jp1hosts` definition file or `jp1hosts2` definition file. For details on communication protocol settings files, see [6.3.2\(2\) Communication protocol settings files](#).

Example situations where communication settings need to be changed:

- You want JP1/Base to communicate using multiple LANs in a cluster system environment with multiple LAN connections
- You want JP1/Base to communicate using a specific LAN in an environment with multiple LAN connections
- You create an environment of only physical hosts by deleting logical hosts from a cluster system

H.4 Changing the settings for the ports parameter in the event server settings file (conf)

This parameter sets the IP address used by the event server to receive JP1 events. If you omit the `client-bind` parameter from the event server settings file, the event service uses the IP address of the event server. For details on the event server settings file, see [Event server settings file](#) in *16. Definition Files*.

Example situations where settings need to be changed (changes are not required when using `jp1hosts2` information):

- You want JP1/Base to use multiple LANs for receiving in a cluster system environment with multiple LAN connections
- You want JP1/Base to communicate using a specific LAN in an environment with multiple LAN connections

H.5 Changing the settings for the client-bind parameter in the event server settings file (conf)

This parameter sets the IP address used by the event server to forward JP1 events. If you omit the `client-bind` parameter, JP1/Base uses the IP address specified in the `ports` parameter of the event server settings file as the source IP address for JP1 events. JP1/Base uses the name resolution process of the OS to resolve event server names not explicitly specified in hosts information. For details on the event server settings file, see [Event server settings file](#) in *16. Definition Files*.

Example situations where settings need to be changed (changes are not required when using `jp1hosts2` information):

- You want JP1/Base to use multiple LANs for sending in a cluster system environment with multiple LAN connections (specify `0.0.0.0`)
- You want JP1/Base to use a specific LAN for sending in an environment with multiple LAN connections

H.6 Changing the settings for the remote-server parameter in the event server settings file (conf)

Use this parameter to resolve the name of the destination event server when forwarding JP1 events. Specify the IP address specified in the `ports` parameter on the destination event server. If you do not specify an event server name, JP1/Base uses the name resolution process of the OS. For details on the event server settings file, see *Event server settings file* in *16. Definition Files*.

Example situations where settings need to be changed (changes are not required when using `jp1hosts2` information):

- The name resolution process of the operating system cannot resolve the destination host name
- The obtained IP address is not the preferred IP address

H.7 Changing the settings for the server parameter in the API settings file (api)

Use this parameter to allow name resolution locally when an application program registers an event on an event server, or when searching for events on a remote host. JP1/Base uses the name resolution process of the OS for host names not defined in this parameter. For details on the API settings file, see *API settings file* in *16. Definition Files*.

Example situations where settings need to be changed (changes are not required when using `jp1hosts2` information):

- An IP address that is not the preferred IP address is specified in the `ports` parameter of the event server settings file
- The OS cannot natively resolve the IP address of an event server specified when searching for events in JP1/IM - View
- The obtained IP address is not the preferred IP address

H.8 Changing the settings for the client parameter in the API settings file (api)

Use this parameter to set the IP address an application program uses to connect to the event server. If you omit this parameter, the OS allocates an IP address automatically. For details on the API settings file, see *API settings file* in *16. Definition Files*.

Example situation where settings need to be changed:

You want JP1/Base to communicate using use a specific LAN for sending in an environment with multiple LAN connections

For details on the communication settings for JP1/Base, see *6. JP1/Base Communication Settings According to Network Configurations*.

H.9 Functionality supported in communication settings

The table below describes the communication settings available for the functionality offered by JP1/Base. When you change the communication settings, you need to restart JP1/Base, products for which JP1/Base is a prerequisite, and programs that have dependency relationships with JP1/Base.

Products such as JP1/IM and JP1/AJS for which JP1/Base is a prerequisite use the communication settings of JP1/Base. For details on the compatibility of these products with JP1/Base communication settings, see the manuals for each product.

Table H-1: Supported functionality in communication settings

Function		Communication settings			
		jp1hosts definition file, jp1hosts2 definition file	Communication protocol settings file	conf file	API settings file
User management	User authentication function	Yes [#]	Yes	--	Yes
	User mapping function	--	--	--	--
Startup control for services	Start sequence control	--	--	--	--
	Stop sequence control	--	--	--	--
Event service		Yes	Yes	Yes	Yes
Event conversion	Log file trap	Yes [#]	--	--	Yes
	Event log trap	Yes [#]	--	--	Yes
Collecting and distributing definitions for the event service		Yes	Yes	--	--
Process management		Yes [#]	--	--	Yes
Health check function		Yes [#]	Yes	--	Yes
Local actions		Yes [#]	--	--	Yes
ISAM utility commands		--	--	--	--
Hitachi Network Objectplaza Trace Library (HNTRLib2)		--	--	--	--
Programs created by users to extend the functionality of JP1/Base		Yes [#]	--	--	Yes

Legend:

Yes: Can be used

--: Cannot be used

[#]: When a JP1 event is registered or obtained, only the jp1hosts2 information is referenced.

H.10 Parameters defined in the communication protocol settings file

The following table lists the meanings of parameters defined in the communication protocol settings file.

Table H-2: Communication settings parameters

Parameter	Description	Value	Meaning
JP1_COM_VERSION	Determines whether to use the communication protocols of JP1/Base 06-51 or earlier, or those of JP1/Base 06-71 or later.	0	Communication protocol of JP1/Base 06-51 or earlier
		1	Communication protocol of JP1/Base 06-71 or later

Parameter	Description	Value	Meaning
JP1_BIND_ADDR	Determines the server-binding method (for receiving data).	ANY	Bind to all the IP addresses
		IP	Bind to a specified IP address
JP1_CLIENT_BIND_ADDR	Determines the client-binding method (for sending data).	ANY	Let the OS determine the IP address to bind to.
		IP	Bind to a specified IP address
COM_LISTEN_ALL_ADDR	Determines whether a service listens on multiple IP addresses	0	Bind to the IP address with the highest priority
		1	Bind to multiple IP addresses
COM_MAX_LISTEN_NUM	When COM_LISTEN_ALL_ADDR=1 is set, specify the number of IP addresses on which a service listens.	4	Bind to four IP addresses

H.11 Differences between communication protocols of JP1/Base 06-51 or earlier and JP1/Base 06-71 or later

You can check which of the communication protocols is used, JP1/Base 06-51 or earlier or JP1/Base 06-71 or later, by referring to the JP1_COM_VERSION value in the common definition information. If JP1_COM_VERSION is set to 0, the system uses the communication protocol of JP1/Base 06-51 or earlier. If JP1_COM_VERSION is set to 1, the system uses the communication protocol of JP1/Base 06-71 or later.

For details on how to check the JP1/Base communication protocol, see [6.3.4 Checking the JP1/Base communication protocol](#).

Depending on the JP1_COM_VERSION setting, during communication, JP1/Base functionalities behave differently according to the value specified in each communication setting item.

The following table shows the behavior of each function during communication when the communication protocol of JP1/Base 06-51 or earlier is used.

Table H-3: Behavior during communication when the communication protocol of JP1/Base 06-51 or earlier is used (JP1_COM_VERSION is 0)

Functionality	Communication setting item					
	JP1_BIND_ADDR	JP1_CLIENT_BIND_ADDR	COM_LISTEN_ALL_ADDR	COM_MAX_LISTEN_NUM	jp1hosts information	jp1hosts2 information
Configuration management	Yes	..#1	..#2	..#3	Yes	Yes
Command execution	Yes	..#1	..#2	..#3	Yes	Yes
User management	Yes	..#1	--	--	Yes	Yes
Collecting and distributing definitions	Yes	..#1	--	--	Yes	Yes
Health check	Yes	..#1	--	--	Yes	Yes

Functionality	Communication setting item					
	JP1_BIND_ADDR	JP1_CLIENT_BIND_ADDR	COM_LISTEN_ALL_ADDR	COM_MAX_LISTEN_NUM	jp1hosts information	jp1hosts2 information
Service management control	Yes	--#1	--	--	Yes	Yes
Inter-process communication	Yes	--#1	--	--	Yes	Yes
Event service#4	Yes	Yes	Yes	Yes	Yes	Yes
Event API (client)#5	--	--#6	--	--	--	Yes

Legend:

Yes: The value of the setting item is referenced.

--: The value of the setting item is not referenced.

#1: The functionality depends on the value specified in JP1_BIND_ADDR.

#2: The value 1 (bind to multiple IP addresses) is assumed.

#3: The value 16 (bind to 16 IP addresses) is assumed.

#4: The value of the setting item shown in the above table is referenced when <jp1hosts2> is specified in the address component of the ports and remote-server parameters of the event server settings file (conf).

#5: This functionality is used when registering and obtaining JP1 events to and from JP1/Base and other products such as JP1/IM. The value of the setting item shown in the above table is referenced when <jp1hosts2> is specified in the address component of the server parameter of the API settings file (api).

#6: The source IP address can be specified by using only the client parameter in the API settings file (api).

The following table shows the behavior of each function during communication when the communication protocol of JP1/Base 06-71 or later is used.

Table H-4: Behavior during communication when the communication protocol of JP1/Base 06-71 or later is used (JP1_COM_VERSION is 1)

Functionality	Communication setting item					
	JP1_BIND_ADDR	JP1_CLIENT_BIND_ADDR	COM_LISTEN_ALL_ADDR	COM_MAX_LISTEN_NUM	jp1hosts information	jp1hosts2 information
Configuration management	Yes	Yes	Yes	Yes	Yes	Yes
Command execution	Yes	Yes	Yes	Yes	Yes	Yes
User management	Yes	Yes	Yes	Yes	Yes	Yes
Collecting and distributing definitions	Yes	Yes	Yes	Yes	Yes	Yes
Health check	Yes	Yes	Yes	Yes	Yes	Yes
Service management control	Yes	Yes	Yes	Yes	Yes	Yes
Inter-process communication	Yes	Yes	Yes	Yes	Yes	Yes
Event service#1	Yes	Yes	Yes	Yes	Yes	Yes
Event API (client)#2	--	--#3	--	--	--	Yes

Legend:

Yes: Setting is referenced.

--: Setting is not referenced.

#1: The value of the setting item shown in the above table is referenced when <jp1hosts2> is specified in the address component of the `ports` and `remote-server` parameters of the event server settings file (`conf`).

#2: This functionality is used when registering and obtaining JP1 events to and from JP1/Base and other products such as JP1/IM. The value of the setting item shown in the above table is referenced when <jp1hosts2> is specified in the address component of the `server` parameter of the API settings file (`api`).

#3: The source IP address can be specified by using only the `client` parameter in the API settings file (`api`).

H.12 Communication protocols in a cluster setup

When JP1/Base is set up for use in a cluster system, the communication protocol is automatically set up as shown in the following table.

Table H-5: Communication protocol in a cluster setup

Parameter	Specified value
JP1_COM_VERSION	0
JP1_BIND_ADDR	IP
JP1_CLIENT_BIND_ADDR	ANY
COM_LISTEN_ALL_ADDR	0
COM_MAX_LISTEN_NUM	4

I. 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.

At the initial settings, output to the operation log is disabled.

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.

In this case, if you use JP1/Audit to collect data that is output to the operation log, you can centrally manage the collected data.

This appendix describes what information can be output to the operation log, and how to specify JP1/Base for operation log output.

I.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 I-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.	<ul style="list-style-type: none">• When adding or deleting a JP1 user• Changing the password of a JP1 user• When adding, changing, or deleting JP1 user operating permission• When registering or deleting a JP1 resource group• When registering, deleting, or changing JP1 resource group operating permission• When executing the <code>jbs_spm�_reload</code> command• When executing the <code>jbsaclreload</code> command

I.2 Storage format of operation log output

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 (`jplbs_base_log_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 [1.5 Settings for outputting operation logs](#).

1.3 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 (`jplgroup1` and `jplgroup2`) registered by a JP1 user are changed, a record for each JP1 resource group (`jplgroup1` and `jplgroup2`) 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/jplbase/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

Table I–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	--	<i>x.x</i>	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	KAJP6xxx-x	Product message ID
5	Date and time	date	yyyy-mm-ddThh:mm:ss.sssTZD ^{#1}	Data and time the operation log record is output, and the time zone
6	Source program name	progid	JPlBase	Name of the program where the event occurred
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	<ul style="list-style-type: none"> • StartStop • ConfigurationAccess 	Category name used to classify events recorded in the operation log
11	Event result	result	<ul style="list-style-type: none"> • Success • Failure 	Event result
12	Subject identification	subj:euid	<ul style="list-style-type: none"> • 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_spmc_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

Table I–3: Fixed output items for the operation log

No.	Output item		Value	Contents
	Item name	Output attribute name		
1	Object information	obj	<ul style="list-style-type: none"> • JPluser • Permission • Process • Password 	Operation target
2	Operation information	op	<ul style="list-style-type: none"> • Add • Apply • Update • Delete • Start • Stop 	Operation type
3	Object location information: <i>authentication-server-name</i>	objloc:authsv	<i>authentication-server-name</i> ^{#1}	Name of the authentication server where the operated resource exists
4	Object location information: <i>JPI-user-name</i>	objloc:user	<i>JPI-user-name</i> ^{#1}	Name of the JP1 user that has the operated resource
5	Pre-change information: <i>JPI-resource-group-name</i>	before:rsrcgrp	<i>JPI-resource-group-name</i> ^{#1}	Deleted information output as pre-change information
6	Post-change information: <i>JPI-resource-group-name</i>	after:rsrcgrp	<i>JPI-resource-group-name</i> ^{#1}	Post-change information output
7	Post-change information: <i>JPI-authority-level-name</i>	after:prmsn	<i>JPI-authority-level-name</i> ^{#1}	Post-change information output
8	Authority information	auth	<ul style="list-style-type: none"> • Windows Administrator • UNIX SuperUser 	Authority of the operating OS user
9	Requesting host	from:ipv4 or from:ipv6	<i>IP-address-of-the-command-executing-host</i> ^{#1#2}	IP address of the command executing host
10	Optional description	msg	For details on messages ^{#2} , see I.6 Operation log messages .	Message describing the event

#1: Output of these values depend on the operation log message. See [Table I-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 I-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
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
KAJP6024-I	Y	N	N	N	N	N
KAJP6025-I	Y	N	N	N	N	N

Legend:

Y: Output

N: Not output

(4) Output example

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=server1,
```

```
objloc:user=jpluser1,auth=Administrator,from:ipv4=206.aa.bb.ccc,
msg=The JP1 user was added successfully
```

I.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 *1.6 Operation log messages*.

Table I–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	<ul style="list-style-type: none"> 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
		KAJP6024-I or KAJP6025-I	
	Startup failed	Startup of the authentication server failed.	KAJP6013-E
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_spm�_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

Trigger condition			Message ID
Operation	Result	Recorded "Failed" event description	
	Command succeeded	--	KAJP6022-I
	Command failed	The <code>jbs_spmc_reload</code> command execution failed.	KAJP6023-W
When reloading the user permission levels (or executing <code>jbsaclreload</code> 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_spmc_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.

I.5 Settings for outputting operation logs

Use the operation log definition file (`jp1bs_baselog_setup.conf`) to configure JP1/Base to output operation log data.

(1) Setup

(a) On a physical host

1. Edit the operation log definition file (`jp1bs_baselog_setup.conf`).

1-1 Set the `ENABLE` parameter.

Open the operation log definition file (`jp1bs_baselog_setup.conf`) in an editor, and change the `ENABLE` parameter as follows:

- Before (default)
"ENABLE"=dword:00000000
- After
"ENABLE"=dword:00000001

1-2 To change the output destination for operation log data, set the `LOGFILEDIR` parameter.

Change the `LOGFILEDIR` parameter as follows:

In Windows:

- Before (default)
"LOGFILEDIR"="*installation-folder*\log\BASE"

- After
"LOGFILEDIR"="*output-destination*"

In UNIX:

- Before (default)
"LOGFILEDIR"="/var/opt/jp1base/log/BASE"
- After
"LOGFILEDIR"="*output-destination*"

2. Execute the `jbssetcnf` command.

The new settings are added to the common definition information.

3. Enable the new settings.

Enable the new settings by restarting JP1/Base or executing the `jbs_spm�_reload` command.

(b) On a logical host

1. Edit the operation log definition file (`jp1bs_baselog_setup.conf`) on the shared disk.

1-1 Set the `[JP1_DEFAULT\JP1BASE\BASE_LOG]` parameter.

Open the operation log definition file (`jp1bs_baselog_setup.conf`) in an editor, and change the `[JP1_DEFAULT\JP1BASE\BASE_LOG]` parameter as follows:

- Before (default)
`[JP1_DEFAULT\JP1BASE\BASE_LOG]`
- After
`[logical-host-name\JP1BASE\BASE_LOG]`

1-2 Set the `ENABLE` parameter.

Change the `ENABLE` parameter as follows:

- Before (default)
"ENABLE"=`dword:00000000`
- After
"ENABLE"=`dword:00000001`

1-3 Set the output destination for operation log data.

Specify the `LOGFILEDIR` parameter as follows. On logical hosts, we recommend that you specify a location on the shared disk.

In Windows:

- Before (default)
"LOGFILEDIR"="*installation-folder*\log\BASE"
- After
"LOGFILEDIR"="*shared-folder*\jp1base\log\BASE"

In UNIX:

- Before (default)
"LOGFILEDIR"="/var/opt/jp1base/log/BASE"
- After
"LOGFILEDIR"="*shared-directory*/jp1base/log/BASE"

2. Execute the `jbssetcnf` command on the primary node.

The contents of the definition file are added to the common definition information.

3. Carry the settings over to the secondary node.

When using JP1/Base in a cluster environment, you need to make the common definition information consistent on each server. For details, see [5.6.1\(1\) When common definition information is added or changed](#).

4. Enable the new settings.

Enable the new settings by restarting JP1/Base from the cluster software, or executing the `jbs_spm�_reload` command.

(2) Operation log definition file (`jp1bs_base_log_setup.conf`) details

(a) Storage destination directory

In Windows:

`installation-folder\conf\
shared-folder\jp1base\conf\`

In UNIX:

`/etc/opt/jp1base/conf/
shared-directory/jp1base/conf/`

(b) Format

In the operation log definition file (`jp1bs_base_log_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

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`). For the operation log file in a logical host, we recommend that you specify a path for a shared disk.

- Initial value
In Windows: `installation-folder\log\BASE`
In UNIX: `/var/opt/jp1base/log/BASE`
- Example output path for logical hosts

In Windows: *shared-folder\jp1base\log\BASE*

In UNIX: *shared-directory/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

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
```

I.6 Operation log messages

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.

KAJP6024-I

SSL communication is enabled for the authentication server.

KAJP6025-I

SSL communication is disabled for the authentication server.

J. Operating JP1/Base as a JP1/Base Administrator (UNIX Only)

In an environment where the users of JP1/Base include a JP1/Base system administrator and JP1/Base administrators, by clarifying the responsibilities of each party, users can use JP1/Base without needing to know what OS user privileges they have. JP1/Base administrators cannot operate JP1/Base unless the system is configured to allow this. JP1/Base processes operate using root permission in either case. When you enable the settings that allow JP1/Base administrators to perform operations, the JP1/Base system administrator is able to keep using JP1/Base as normal.

This appendix describes the division of roles between the JP1/Base system administrator and the JP1/Base administrator, and the settings that allow JP1/Base administrators to use JP1/Base. For an overview of how to operate JP1/Base in the role of a JP1/Base administrator, see [2.11 Managing JP1/Base as a JP1/Base administrator \(UNIX only\)](#).

J.1 Division of roles when operating JP1/Base

To change the environment settings of JP1/Base or execute certain commands, users need to have the right permissions for the OS and products related to JP1/Base. This means that JP1/Base administrators cannot perform every task traditionally performed by the JP1/Base system administrator. The division of roles is as follows:

JP1/Base system administrator

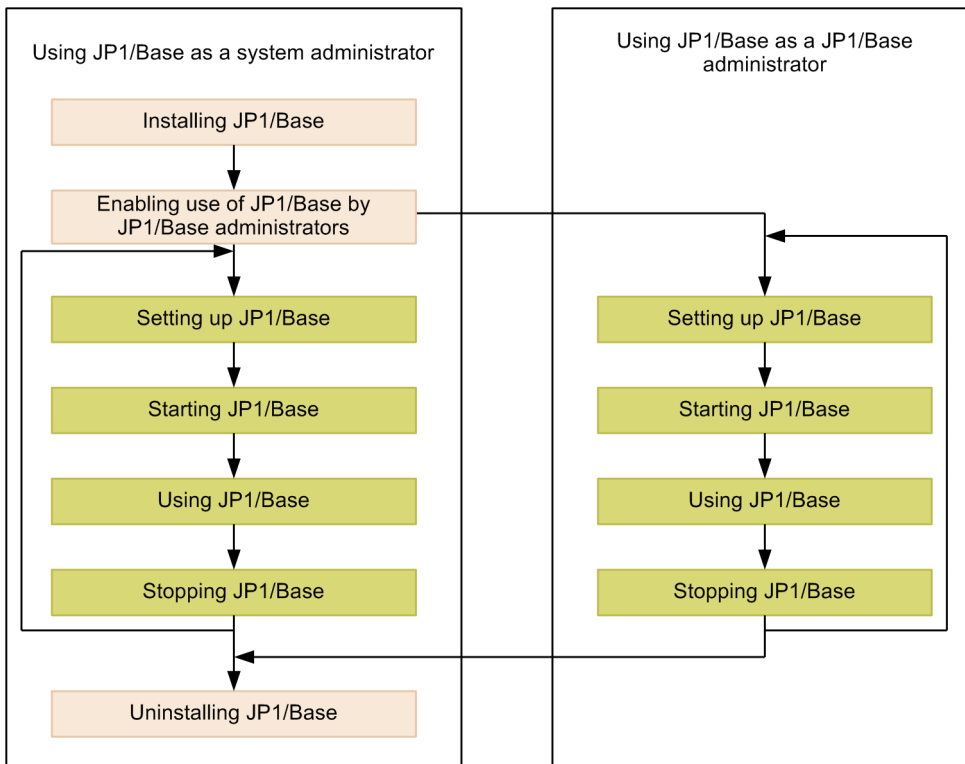
- Working with the operating system
- Setting up the JP1/Base environment
- Troubleshooting JP1/Base

JP1/Base administrator

- Tasks related to JP1/Base operation that are not the responsibility of the JP1/Base system administrator

The following figure shows how JP1/Base is used when the settings that allow JP1/Base administrators to perform operations are enabled.

Figure J–1: JP1/Base operation with JP1/Base administrators enabled



Legend:

- : Tasks only the JP1/Base system administrator can perform.
- : Tasks JP1/Base administrators can perform on behalf of the system administrator.

The following tables describe the roles of the JP1/Base system administrator and JP1/Base administrators in detail.

Table J–1: Role of JP1/Base system administrator

No.	Function	
1	OS operations	Network-related settings such as hosts information
2		Allocating shared directories and assigning the appropriate update permissions to JP1/Base administrators (when using JP1/Base on a logical host)
3		Registering JP1/Base with cluster software (when using JP1/Base in a cluster environment)
4	Settings that allow JP1/Base administrators to perform operations	Creating the JP1 administrators group
5		Assigning OS users to the JP1 administrators group
6	Setting up the JP1/Base environment	Installing JP1/Base
7		Uninstalling JP1/Base
8		Migrating command execution log files (<code>jcocmdconv</code> command)
9		Enabling the JP1/Base administrator role (<code>jbsetadmingrp</code> command)
10		Executing commands managed by HNTRLlib that are intended for root users
11		Deleting resources used by ISAM (<code>Jisrsdel</code> command)
12		Increasing or decreasing the number of entries in lock tables (<code>Jislckext</code> command)

No.	Function	
13	Troubleshooting JP1/Base	Forcibly shutting down all logical hosts (<code>jbs_killall.cluster</code> command)
14		Collecting resources (<code>jbs_log.sh</code> command) [#]

#: The `jbs_log.sh` command for collecting data can also be executed by a JP1/Base administrator. However, the data collection tool does not have sufficient rights to collect the following information when executed by a user with JP1/Base administrator privileges:

- **syslog**
/var/log/messages (in Linux)
- **Kernel parameter information**
/etc/security/limits (in AIX)
- **System diagnostics**
Execution result of `/usr/bin/alog -o -t boot` (in AIX)

When the data collection tool fails to collect data, the following message is output to the console:

Can not get *resource-for-which-collection-failed*.

Table J–2: Role of JP1/Base administrator

No.	Function		
1	Operating JP1/Base	Starting and stopping JP1/Base	
2		User management	User authentication
3			User mapping
4		Event service	
5		Event conversion	Log file traps
6		Collecting and distributing definitions	Managing definition information using IM configuration management and managing the operating status of services
7			Collecting and distributing definitions for the event service
8			Collecting definition information for JP1 products
9		Process management	
11		Health check function	
11		Local actions	
12		Adding primary and secondary logical hosts	
13		ISAM utility commands With the exception of the following: <ul style="list-style-type: none"> • Deleting resources used by ISAM (<code>Jisrsdel</code> command) • Increasing or decreasing the number of entries in lock tables (<code>Jislckext</code> command) 	

JP1/Base administrators cannot use the following features of JP1/Base. These remain the responsibility of the JP1/Base system administrator.

- **Mapping users to the superuser**
If a JP1/Base administrator adds a mapping definition that maps to the superuser (the root OS user), an error occurs accompanied by an error message.
- **Automatic startup**
Automatic startup is not supported for JP1/Base administrators.

J.2 Setting up an environment in which JP1/Base administrators can use JP1/Base

The JP1/Base system administrator needs to perform the following tasks to allow JP1/Base administrators to operate JP1/Base:

- Create the JP1 administrators group (an OS user group)
You can use an existing OS group as the JP1 administrators group.
- Set the primary group for JP1/Base administrators
Set the JP1 administrators group as the primary group for users who are to act as JP1 administrators.
- Set up an environment in which JP1/Base administrators can use JP1/Base[#]
You can do so by executing the `jbssetadmingrp` command. You can also use this command to check whether JP1/Base administrators are able to use JP1/Base. For details on the `jbssetadmingrp` command, see [jbssetadmingrp \(UNIX only\)](#) in *15. Commands*.

#

If you have enabled the JP1/Base administrator role, you cannot disable it again without uninstalling and then reinstalling JP1/Base. Uninstalling JP1/Base means that you also need to uninstall products for which JP1/Base is a prerequisite, so consider carefully before setting up such an environment.

(1) Additional setup tasks for specific functionality

In an environment where JP1/Base administrators can use JP1/Base, additional setup is required before JP1/Base administrators can use the functionality below. These tasks must be performed by the JP1/Base system administrator.

- Setting the shared directory for logical hosts, the output destination for operation log data, and the directory used by the event service
- Executing ISAM-related utility commands

(a) Setting shared directories for logical hosts, output destinations for operation log data, and directories used by event services

To allow JP1/Base administrators use of shared directories for logical hosts, output destinations for operation log data, and the directories used by the event service, JP1/Base administrators must be given access to all higher-level directories. Assign read and execute permission in the `others` category for all higher-level directories of the following directories:

- Shared directory for each logical host
- Output destination for operations log data (if the location was changed from the default)
- Any directories other than default specified in the event server index file (`index`)

(b) Setup for executing ISAM-related utility commands

Change the `umask` value of ISAM-related utility commands to `002`.

(2) Stopping operation by JP1/Base administrators

To stop JP1/Base administrators from using JP1/Base:

1. Back up JP1/Base setup information and the event database.
For details on how to back up the setup information and event database, see [3.5.3\(1\) Backing up JP1/Base setup information](#) and [3.5.3\(2\) Backing up an event database](#).

2. Uninstall JP1/Base.

For details on how to uninstall JP1/Base, see [3.3.3 Uninstalling JP1/Base](#). Delete any JP1/Base files remaining in the installation folder after the uninstallation process.

3. Perform a new installation of JP1/Base.

4. Restore the JP1/Base setup information.

For details on how to recover setup information, see [3.5.3\(3\) Recovering JP1/Base setup information](#).

To keep an environment in which JP1/Base administrators are unable to use JP1/Base, you need to recover the setup information in such a manner that the backed up permissions, ownership, and group settings of the definition files are not restored, and the settings of the new installation in step 3 are kept.

5. Restore the event database.

For details on how to recover the event database, see [3.5.3\(4\) Recovering an event database](#).

After recovering the event database, execute the following commands to change the owner, access permissions, and group of the database files:

```
cd /var/opt/jp1base/sys/event/servers/default# or cd shared-directory/event#  
chmod 644 ./IMEvent*.*
```

In Linux: `chown root:root ./IMEvent*.*`

In AIX: `chown root:system ./IMEvent*.*`

#: If you specified a different path for the event server directory in the event server index file (`index`), specify that path instead.

(3) Backup and recovery in environments where JP1/Base administrators can use JP1/Base

To back up and recover JP1/Base settings in an environment where JP1/Base administrators can use JP1/Base:

1. Back up JP1/Base setup information and the event database.

For details on how to back up the setup information and event database, see [3.5.3\(1\) Backing up JP1/Base setup information](#) and [3.5.3\(2\) Backing up an event database](#).

2. Recover the setup information and event database.

For details on how to recover the setup information and event database, see [3.5.3\(3\) Recovering JP1/Base setup information](#) and [3.5.3\(4\) Recovering an event database](#).

3. Enable the setting that allows JP1/Base administrators to perform operations.

Execute the `jbsssetadmingrp` command to set up an environment in which JP1/Base administrators can use JP1/Base. Use the same name and gid for the JP1 administrators group as the host on which the backup was created.

J.3 Setting up an environment for JP1/Base administrators on a logical host

On a logical host, the ability of JP1/Base administrators to use JP1/Base depends on whether this setting is enabled on the physical host. The following describes how to set up an environment in which JP1/Base administrators can use JP1/Base on a logical host. These tasks must be performed by the JP1/Base system administrator.

(1) Setting up an environment for JP1/Base administrators on an existing logical host

In a non-cluster environment:

1. Mount the shared directory.
2. Execute the following command to allow JP1/Base administrators to operate JP1/Base:

```
jbssetadmingrp -s JP1-administrators-group
```
3. From the command output in step 2, check whether the setting to allow JP1/Base administrators to operate JP1/Base is enabled on the physical and logical hosts.
Check the messages corresponding to each host in the command output.
If the command output indicates that the setting is disabled on a host, mount the host and repeat step 2.
4. Execute the following command and check whether the setting to allow JP1/Base administrators to operate JP1/Base is enabled on all logical hosts.

```
jbssetadmingrp -v
```

In a cluster environment

To allow JP1/Base administrators to operate JP1/Base in a cluster environment, the name and ID of the JP1 administrators group must be the same on the primary and secondary nodes.

1. Execute the following command on the primary node to allow JP1/Base administrators to operate JP1/Base:

```
jbssetadmingrp -s JP1-administrators-group
```
2. From the command output in step 1, check whether the setting to allow JP1/Base administrators to operate JP1/Base is enabled on the physical and logical hosts.
Check the messages corresponding to each host in the command output.
If the command output indicates that the setting is disabled on a host, mount the host and repeat step 1.
3. Execute the following command on the primary node to check whether the setting to allow JP1/Base administrators to operate JP1/Base is enabled on all logical hosts:

```
jbssetadmingrp -v
```
4. Execute the following command on the secondary node to allow JP1/Base administrators to operate JP1/Base.

```
jbssetadmingrp -s JP1-administrators-group
```
5. From the command output in step 4, check whether the name and gid of the JP1 administrators group are the same on the primary and secondary nodes.
If the values do not match, change the setting in the OS and then repeat step 4. The message KAVA1829-W is output for the logical host but can be ignored.
6. Fail over all logical hosts to the standby node.
7. Execute the following command on the secondary node and check whether the setting to allow JP1/Base administrators to operate JP1/Base is enabled on all logical hosts:

```
jbssetadmingrp -v
```


If the JP1 administrators group name and gid on the secondary node do not match those on the primary node, fail all logical hosts back to the primary node, change the setting in the OS, and then repeat step 4.

(2) Setting up an environment for JP1/Base administrators on a new logical host

When you create a new logical host, the files from the physical host to which the JP1 administrators group has access rights are copied to the new logical host. You do not need to take any additional steps to enable this feature on the logical host.

(3) Stopping JP1/Base administrators from using JP1/Base on a logical host

1. Mount the shared directory.
2. Execute the following command to disable the setting that allows JP1/Base administrators to operate JP1/Base.

```
jbssetadmingrp -s sys#  
#: system in AIX.
```

In a cluster environment, execute the command on the primary and secondary nodes.

3. Execute the following command on the physical host where you disabled the setting in step 2.

```
jbssetadmingrp -v
```

4. From the command output in step 3, make sure the setting that allows JP1/Base administrators to operate JP1/Base is disabled on the logical hosts where you disabled the setting.

K. Operating a secure system

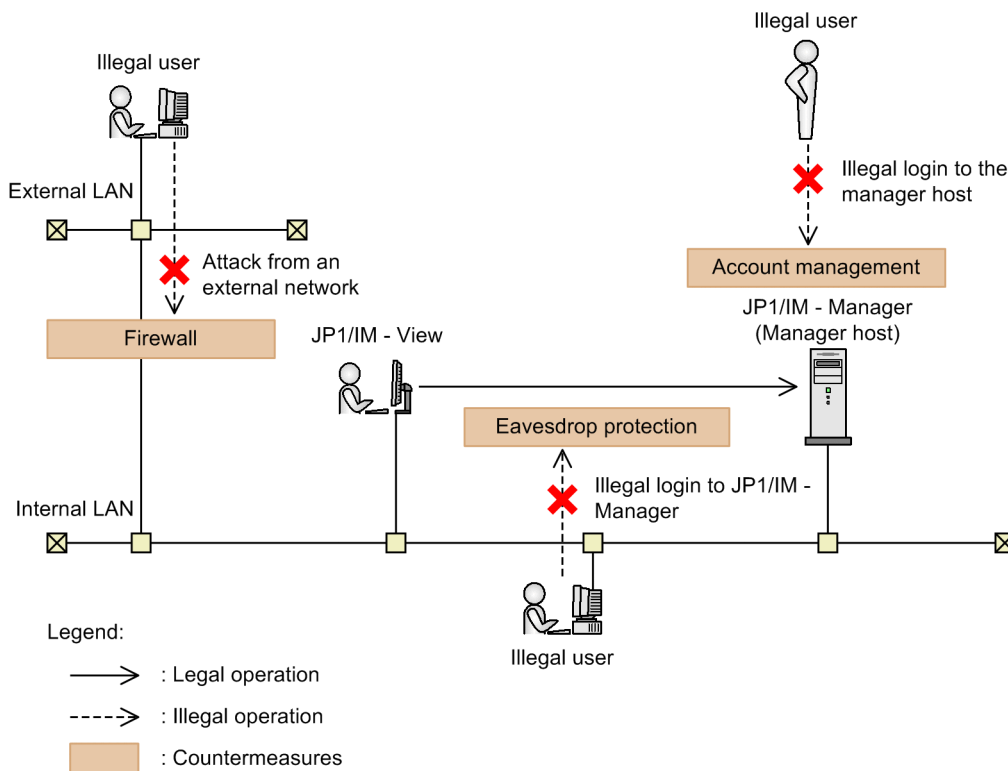
This chapter describes how to securely operate a system running JP1/Base.

To enable secure operations of a system running JP1/Base, operational measures, such as management of firewalls and OS accounts, are necessary as prerequisites. Furthermore, JP1/Base provides functionality for restricting connections from unintended hosts, which enables secure system operations.

K.1 Prerequisites for a secure system

The system administrator must take measures against illegal activities as follows, as the prerequisites for secure system operations.

Figure K-1: Illegal activities and countermeasures



Illegal activity	Countermeasure
Attack from the external network	Set up firewall.
Illegal login attempt to the manager host	Control login access to the manager host for users other than the administrators for the machine and JP1 products. Accomplish this by managing accounts on the manager host, such as the member accounts of the Administrators group, the root account, and the OS accounts that belong to the JP1/Base administrator group.
Illegal login attempt to JP1/IM - Manager	Prevent eavesdropping on the communication between JP1/IM - View and JP1/IM - Manager by setting up a VPN or by other means.

K.2 Restricting connections from unintended hosts

JP1/Base can control the hosts that are allowed to establish connections for the communication between the manager host (source host) and agent hosts (destination hosts). This can prevent unintended hosts from requesting command execution or changing configuration definitions.

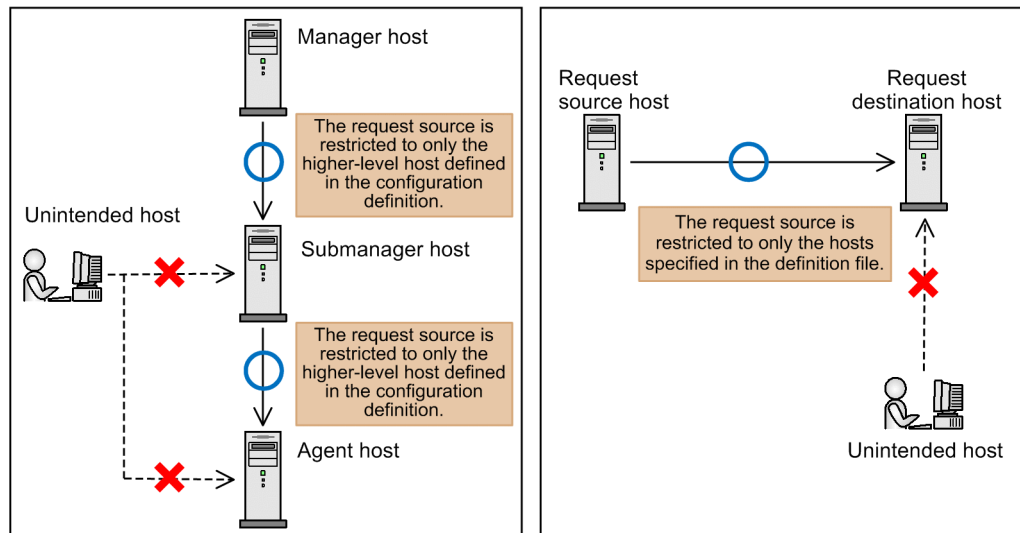
The functionality for restricting connections supports the following functions:

- **Command execution function**
You can specify the settings required to receive the requests for command execution such that only requests that were sent from the higher-level host registered in the configuration definition are accepted.
- **Configuration management function**
You can specify the settings required to receive the requests for changing configurations such that only requests that were sent from the higher-level host registered in the configuration definition are accepted.
- **Operation requests from linkage products (for communication between JP1/Base instances)**
You can specify the settings required to receive only the requests that were sent from the hosts you defined, regarding the following linkage:
 - Requests for command execution from JP1/IM - Rule Operation
 - Requests for executing operation jobs from JP1/IM - Planning Operation
 - Communication when linking between JP1/Navigation Platform and JP1/Automatic Operation
 - Communication when linking between JP1/Navigation Platform and JP1/IM - Manager

Figure K–2: Restricting connections from unintended hosts

For the command execution and configuration management functions

For operation requests from the linkage products (JP1/IM - RL, JP1/IM - PL, and JP1/IM - NP)



Legend:

- : Legal operation
- - - -> : Illegal operation
- Orange box : Countermeasures

K.3 Definition for restricting connections from unintended hosts

To restrict connections from unintended hosts, create a file that defines the hosts allowed for connection with any name you like, and execute the `jbssetcnf` command to set the definition in the common definition information.

The following table describes the contents of the definition file.

Functions to be restricted	Key name	Option name and its value	Description
<ul style="list-style-type: none"> Command execution function Configuration management function 	JP1_DEFAULT\JP1 BASE\COM_CONTROL\ROUTE	"UPPER_ONLY"=dword: { 00000000 00000001 }	This option suppresses the requests that were sent from hosts other than the higher-level host defined in the configuration definition. If no common definition information has been set, the default value is used. If the specified value is outside the range of specifiable values, the default value is used during startup, or the value before reloading is used when the definition file is reloaded. 00000000: Disable (default) 00000001: Enable
		"ALT_CLIENT_HOSTS"="{ <i>host-name</i> <i>IP-address</i> }, ..."	If the UPPER_ONLY option is enabled, the requests that were sent from the hosts specified in this option are also accepted. If the UPPER_ONLY option is disabled, the setting in this option is disabled. You can specify no more than four hosts delimited by a comma. The default value is undefined.
Operation requests from linkage products (communication between JP1/Base)	JP1_DEFAULT\JP1 BASE\COM_CONTROL\RECEIVE	"CLIENT_HOSTS"="{ <i>host-name</i> <i>IP-address</i> }, ..."	The requests that were sent from hosts other than the hosts specified with this option are suppressed. If this option is not defined, connection is not restricted. You can specify no more than eight hosts delimited by a comma. The default value is undefined.

Note:

If the system is running in a cluster environment, specify the settings by replacing JP1_DEFAULT with the logical host name on both the primary and secondary nodes.

(1) Notes on the definition file

- To disable the ALT_CLIENT_HOSTS or CLIENT_HOSTS option, define the null character ("").
- The IP address format that can be specified for the ALT_CLIENT_HOSTS and CLIENT_HOSTS options are shown below. Note that, if the specified IP address does not conform to the following IP address format, it will be treated as the host name.

The format when specifying an IPv4 address

- The format is *W.X.Y.Z*. Specify each of *W*, *X*, *Y*, and *Z* with a decimal value from 0 to 255.

The format when specifying an IPv6 or IPv4 address

- The format is *A:B:C:D:E:F:G:H*. Specify each of *A*, *B*, *C*, *D*, *E*, *F*, *G*, and *H* with a hexadecimal value from 0 to ffff.
- If the value begins with 0, you can omit that 0.
- If the value is 0000, specify it as 0.
- Consecutive 0000 patterns can be replaced with " : : " only once.

Example:

Before replacement: 0123:0000:0000:0000:4567:0000:0000:89ab

After replacement: 123::4567:0:0:89ab

- If the definition in the `ALT_CLIENT_HOSTS` or `CLIENT_HOSTS` option contains one of the following illegal specifications, the processing will continue using the default value during startup or using the definition before reloading when the definition file is reloaded:
 - A duplicate host name is specified. (Note that the value is not case sensitive.)
 - The number of specified hosts exceeds the specifiable number of hosts.
 - The specified host name exceeds 256 bytes.
 - Name resolution is not available for the specified host name.
- If you change the IP addresses corresponding to the higher-level host registered in the configuration definition and to the host name defined in the option, the new settings are applied after the `jbs_spmd_reload` command is executed.
- The IP addresses corresponding to the higher-level host registered in the configuration definition and to the host name defined in the option must be the same as the IP addresses that the source host actually uses for communication.
- If you operate in an NAT environment, define the converted source IP address in the `ALT_CLIENT_HOSTS` or `CLIENT_HOSTS` option.
- If you change the configuration definition from the submanager host for which the `UPPER_ONLY` option is enabled, define the local host name or the IP address of the local host in the `ALT_CLIENT_HOSTS` option of the manager host.
- A host for which the `UPPER_ONLY` option is enabled and no higher-level host is registered in the configuration definition behaves as follows:
 - Accepts the requests for changing configuration (definition distribution) from any hosts.
 - Suppresses the requests for command execution from the hosts other than the local host.

K.4 Procedure for restricting connections from unintended hosts

To restrict connections from unintended hosts:

1. Create a definition file with any name you like.

The following is an example setting of a definition file:

```
[JP1_DEFAULT\JP1BASE\COM_CONTROL\ROUTE]
"UPPER_ONLY"=dword:00000001
"ALT_CLIENT_HOSTS"="host1"
[JP1_DEFAULT\JP1BASE\COM_CONTROL\RECEIVE]
"CLIENT_HOSTS"="host1,host2"
```

2. Execute the `jbssetcnf` command.

Execute the `jbssetcnf` command to register the settings in the definition file into the common definition.

```
jbssetcnf definition-file-name
```

For details about the `jbssetcnf` command, see *jbssetcnf* in 15. *Commands*.

3. Restart or reload JP1/Base.

Restart or reload JP1/Base to apply the specified definitions. Execute the `jbs_spm�_reload` command to reload. For details about the `jbs_spm�_reload` command, see *jbs_spm�_reload* in 15. *Commands*.

K.5 Messages that are output when a request was denied by connection restriction

When a request from an unintended host is denied by connection restriction, a message reporting the denial is output. The following table lists messages that are output to the requesting and requested hosts for each function and each command to be restricted. These messages are output to the integrated trace log file.

Table K–1: Messages that are output when a request is denied by connection restriction

Functions to be restricted	Commands to be restricted	Hosts to be restricted	Output message
Command execution function	--	Requesting host	KAVB2630-E A request from a host without access permissions was rejected. (<i>requesting-host-name</i> or <i>IP-address-of-requesting-host</i>)
	--	Requesting host	KAVB2630-E A request from a host without access permissions was rejected. (<i>requested-host-name</i> or <i>IP-address-of-requested-host</i>)
Configuration management function	Execution of the <code>jbsrt_distrib</code> command (deletion of the configuration definition)	Requesting host	KAVB3104-W Cannot delete configurations for the host and its lower-level hosts. Try again after deleting each definition separately. <i>host-name</i>
	Execution of the <code>jbsrt_distrib</code> command (distribution of the configuration definition)		KAVB3107-E Cannot set configuration in the host. <i>host-name</i>
	Execution of the <code>jbsrt_sync</code> command (synchronization of the configuration definition)		KAVB3108-E Failed in definition distribution. Cannot set configuration information in the host. <i>host-name</i>
	--		KAVB3111-E Failed to execute the <code>jbsrt_sync</code> command. An error occurred in the host. <i>host-name</i>
	--	Requesting host	KAVB3164-E A request from a host without access permissions was rejected. (<i>requesting-host-name</i> or <i>IP-address-of-requesting-host</i>)
Operation requests from linkage products (communication between JP1/Base)	--	Requesting host	KAVA6701-E A connection to the execution host could not be established. (host= <i>host-name</i>)
	--	Requesting host	KAVA6046-E A request from a host without access permissions was rejected. (<i>requesting-host-name</i> or <i>IP-address-of-requesting-host</i>)

Legend:

--: Not applicable.

L. Using JP1/Base linked with the auto-scaling functionality

This section explains how to use JP1/Base linked with the auto-scaling functionality of a cloud platform (Amazon EC2).

The auto-scaling functionality provided by the Amazon EC2 service automatically increases the number of virtual machines (scales out) and deletes virtual machines (scales in) as needed, based on certain criteria such as thresholds for system load.

When JP1/Base is linked with the auto-scaling functionality, virtual machines that are added during scale out are automatically added to the system's monitoring targets. Specifically, settings for the following monitoring operations are automatically configured by the manager.

- Basic integrated monitoring by JP1/IM is set up, including:
 - Management of the system's hierarchical configuration based on the configuration definition (the IM configuration management functionality is not used)
 - Central management of various events that occur in the system by using JP1 events
 - Monitoring of remote hosts by using the health check function of JP1/Base
- Alarm monitoring by JP1/PFM is set up (if JP1/PFM is used for monitoring)

Note that, when a virtual machine is deleted during scale in, these settings are also cleared.

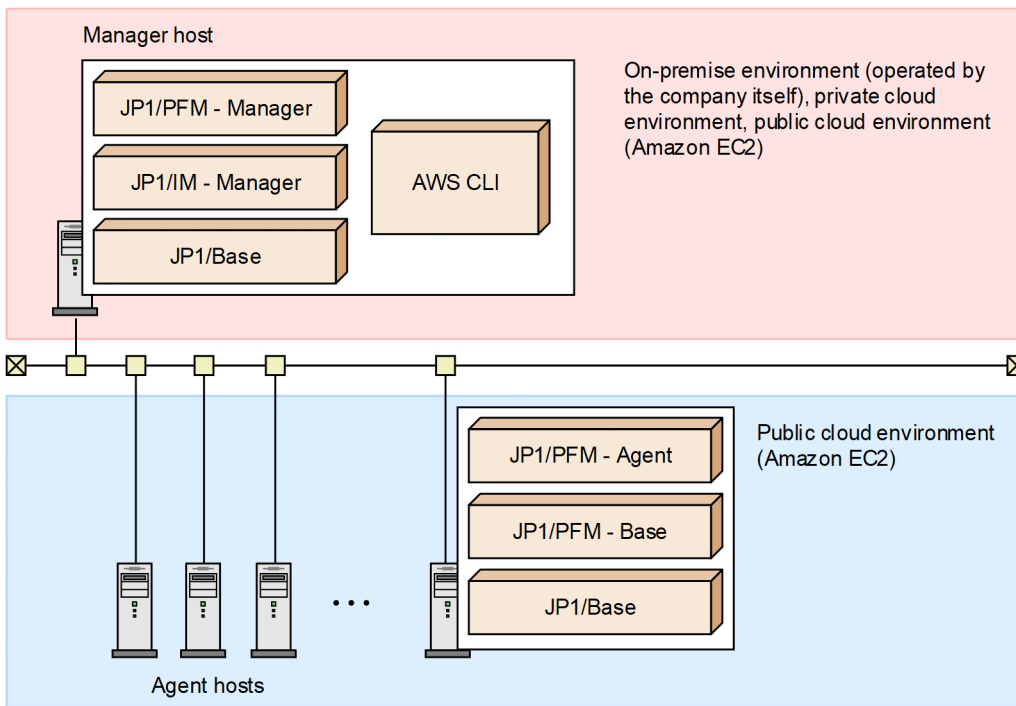
Auto-scaling linkage using Amazon EC2 API Tools is for compatibility with versions 11 and 12. For version 13 or later, use AWS CLI.

L.1 System configuration for using JP1/Base linked with the auto-scaling functionality

This subsection describes the system configuration needed to use JP1/Base linked with the auto-scaling functionality.

The system consists of hosts to be monitored (agent hosts) and a host that monitors the agents (manager host).

Figure L-1: System configuration for using JP1/Base linked with the auto-scaling functionality



(1) Prerequisite cloud services

Amazon EC2 service

(2) Supported OSs

Windows

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Linux

- Linux 7
- Linux 8
- Linux 9

(3) Prerequisite programs

The programs to be installed on the manager host and the agent hosts are as follows:

Manager host

- JP1/Base 13-00 or later[#]

- JP1/Integrated Management - Manager 13-00 or later
- AWS CLI (prerequisite program for AWS CLI)

#

The scripts bundled with JP1/Base have been tested with AWS CLI version 2.0.0 (released on 2020-02-10). You can use them within the range of versions where there is no change in the interface of the AWS CLI commands (`aws ec2 describe-instance-status`, `aws ec2 describe-instances`) used in the scripts bundled with JP1/Base.

If you want to use Amazon EC2 API Tools for compatibility, install the following program instead of the above program:

- JP1/Base 11-00 or later
- JP1/Integrated Management - Manager 11-00 or later
- Java Runtime Environment (JRE) 1.7 or later
- Amazon EC2 API Tools (prerequisite program for Amazon EC2 API Tools)

If you plan to use JP1/PFM for monitoring, install the following program:

- JP1/Performance Management - Manager 11-00 or later

Agent hosts

- JP1/Base 11-00 or later

If you plan to use JP1/PFM for monitoring, install the following programs:

- JP1/Performance Management - Agent Option for Platform 11-00 or later
- JP1/Performance Management - Base 11-00 or later

(4) Environment conditions for hosts

The environment conditions for the manager host and the agent hosts are as follows:

Manager host

There are no special restrictions. The manager host can be run in either a physical machine environment or a virtual machine environment (including on a virtual machine in a cloud environment).

Agent hosts

Agent hosts must be run in a virtual machine environment (Amazon EC2 instance) provided by the Amazon EC2 service.

L.2 Prerequisites for using JP1/Base linked with the auto-scaling functionality

The following are prerequisites for using JP1/Base linked with the auto-scaling functionality:

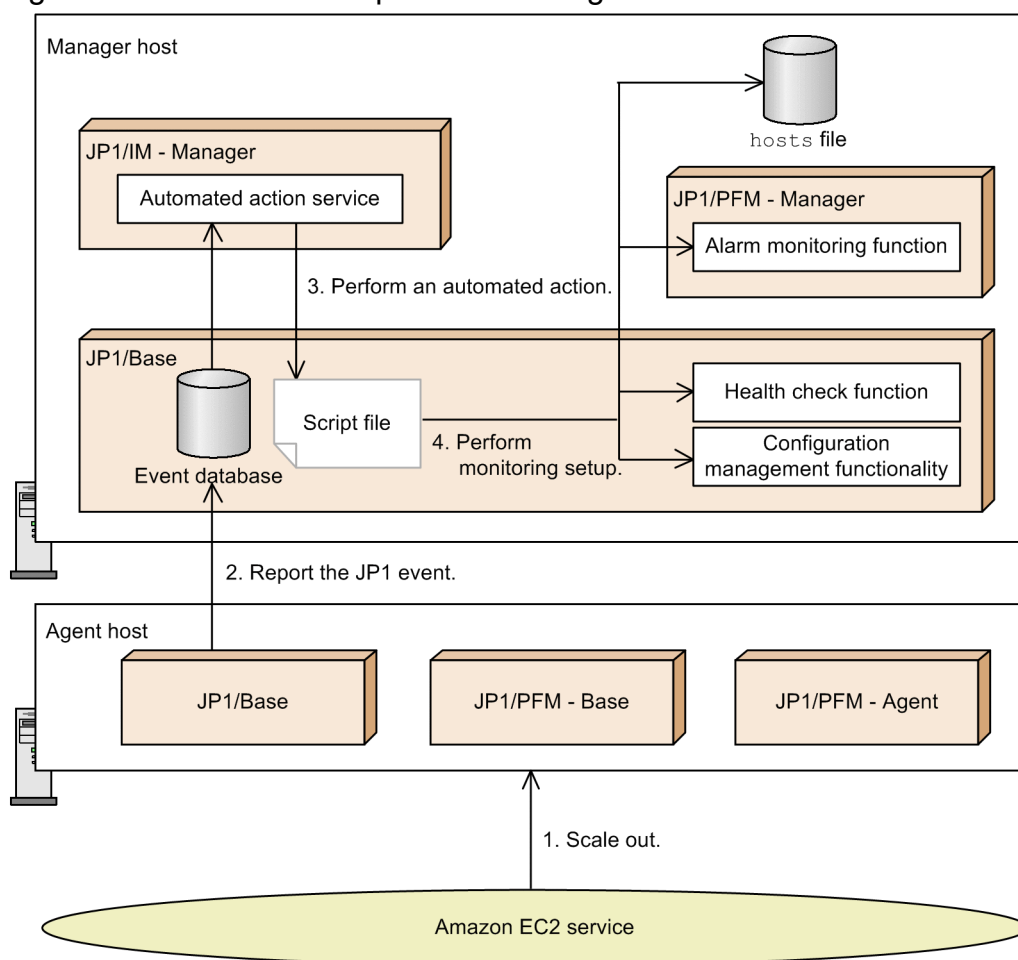
- The manager host and the agent hosts cannot be used on logical hosts in a cluster environment.
- The system configuration must be such that the number of hosts is no more than 2,500 including manager hosts.
- The number of commands to be executed concurrently by the automated action function of the manager host must be 1.
- If JP1/PFM is used for monitoring, the following conditions apply:
 - The dual monitoring function is not supported.

- Hosts cannot be added to or deleted from the Agents tree (User Agent).
If necessary, manually set hosts after a scale out or scale in.
- Hosts cannot be added to or deleted from business groups.
If necessary, manually set hosts after a scale out or scale in.
- DNS environments are supported, but FQDN names cannot be used as host names.
- Operating JP1/Base as a JP1/Base administrator is not supported.

L.3 Adding hosts to the monitoring target during scale out

If an agent host is added during scale out, a JP1 event is sent from the agent host to the manager host. The manager host then performs the automated action corresponding to this JP1 event and adds the agent host to the system's monitoring targets.

Figure L–2: Overview of operations during a scale out



(1) Reporting a scale out by using JP1 events

The first time the OS starts up after a scale out occurs, a scale-out notification event (event ID: 1011) is issued as a JP1 event to notify the manager host of the scale out. For details about this event, see [17.3.1\(1\) Details about event ID 00001011](#).

If an attempt to send the event fails, the OS will continue to attempt to send the event at intervals of 600 seconds for a maximum of six times.

The manager host to which scale-out notification events are to be sent must be specified beforehand in the script definition file. You can change the notification event's attributes (event ID and message).

For details about the script definition file, see [L.8 Auto-scaling linkage script](#).

(2) Network settings and monitoring settings

The automated action for the scale-out notification event involves the configuration of network settings and monitoring settings as follows:

- The host name and IP address of the agent host are added to the manager host's `hosts` file.
- The agent host is added to the health check definition file (`jbshc.conf`), and then JP1/Base is reloaded to apply the definition.
- The agent host is added to the configuration definition file (`jbs_route.conf`), and then the configuration information is distributed.

If JP1/PFM is used for monitoring, an alarm table is bound to the agent based on the alarm table name specified in the script definition file. You can specify the name of the alarm table to be bound to the agent in the script definition file. For details about the script definition file, see [L.8 Auto-scaling linkage script](#).

(3) Checking whether monitoring was performed successfully

You can determine whether monitoring was performed successfully by checking the termination code of the automated action for the scale-out notification event. If the automated action terminated normally, the termination code will be 0. If the action terminated abnormally, the termination code will be a nonzero value.

If the automated action terminated abnormally, remove the cause of the error, and then re-execute the automated action.

L.4 Terminating monitoring during scale in

If an agent host is deleted during scale in, the health check function detects that the agent host has stopped or that an error has occurred, and then performs the automated action for the JP1 event that is registered in the manager host. As a result, the agent host is deleted from the system's monitoring targets.

(1) Detecting a scale in by using the health check function

Scale-in events are detected by the health check function (monitoring of remote hosts).

- When the JP1/Base service stops, an agent sends the manager an event notifying the manager that the service has stopped (event ID: 4725). For details about this event, see [17.3.1\(42\) Details about event ID 00004725](#).
- If, for some reason, the event notifying the manager that the service has stopped cannot be received, an agent error is detected and an error detection event (event ID: 4749 or 474D) is issued.
 - If an error was detected during normal monitoring, an error detection event (event ID: 4749) is issued. For details about this event, see [17.3.1\(49\) Details about event ID 00004749](#).
 - If the stopping of the service cannot be distinguished from an error, an error detection event (event ID: 474D) is issued. For details about this event, see [17.3.1\(53\) Details about event ID 0000474D](#).

(2) Clearing the network settings and the monitoring settings

The network settings and monitoring settings are cleared by the automated action for the health check stop notification event (event ID: 4725) and by the automated action for the error detection event (event ID: 4749 or 474D), as follows.

- Information about the agent host that was scaled in is deleted from the manager host's `hosts` file.
- The agent host is deleted from the health check definition file (`jbshc.conf`) and then JP1/Base is reloaded to apply the definition.
- The agent host is deleted from the configuration definition file (`jbs_route.conf`).
If the value of the `JbsrtDistribByScaleIn` setting parameter is `YES` in the `jbsas_setup_manager.ini` file, the configuration definition is distributed. If the value is `NO`, the configuration definition is not distributed. It is distributed the next time a scale out occurs. The initial value is `NO`.
- If JP1/PFM is used for monitoring, the agent's monitoring information is deleted.

If a JP1 event is reported due to a temporary error, but a scale out has not occurred, these settings are not cleared even when an automated action is executed.

(3) Checking whether monitoring settings were cleared successfully

You can check whether monitoring settings were cleared successfully by checking the termination code of the automated action for the stop notification event (event ID: 4725) or for the error detection event (event ID: 4749 or 474D). If the automated action terminated normally, the termination code will be 0. If the action terminated abnormally, the termination code will be a nonzero value.

If the automated action terminated abnormally, remove the cause of the error, and then re-execute the automated action.

L.5 Setup procedure for using JP1/Base linked with the auto-scaling functionality (for the manager host)

This subsection describes how to set up manager hosts when JP1/Base is to be linked with the auto-scaling functionality.

Note that steps 7 and 9 are required if JP1/PFM is to be used for monitoring.

1. Install AWS CLI.

Download AWS CLI from the official Amazon Web Services site, and save it in a directory of your choice.

2. Specify the environment variables required for running AWS CLI.

Specify the environment variables required for running AWS CLI in the script definition file (`jbsas_setup_manager_cli.ini`). For details about the settings that are required for the execution environment of AWS CLI, see the official AWS CLI site. For details about the script definition file, see [L.8 Auto-scaling linkage script](#).

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

4. Enable the health check function of JP1/Base.

5. Set an automated action for starting the monitoring of hosts that were scaled out.

To run an auto-scaling linkage script (`jbsas_add_agent_cli`), specify the automated action definition described in the table below. For details about automated action definitions, see the chapter on executing commands by using automated actions in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table L–1: Automated action definition (for scale out)

Definition item	Definition value
Action name	Any value
Event ID	1011 (If the event ID of the scale-out notification event was changed, specify the new event ID.)
Event condition	None
User name of the user who executes the action	In Windows: User name of the JP1 user who is mapped to the OS user with <code>jpladmin</code> or Administrator permissions In Linux: User name of the JP1 user who is mapped to the OS user with <code>jpladmin</code> or superuser permissions
Target host	Manager host name
Action	In Windows: <pre>powershell -ExecutionPolicy RemoteSigned "&'installation- folder\tools\cloud\jbsas_add_agent_cli.ps1'" \$EVIPADDR \$EVHOST \$EV"OS_TYPE" \$EV"INSTALLPP_INFO" <nul</pre> If you want to use Amazon EC2 API Tools for compatibility, configure the following. <pre>powershell -ExecutionPolicy RemoteSigned "&'installation- folder\tools\cloud\jbsas_add_agent.ps1'" \$EVIPADDR \$EVHOST \$EV"OS_TYPE" \$EV"INSTALLPP_INFO" <nul</pre> In Linux: <pre>/bin/sh /opt/jplbase/tools/cloud/jbsas_add_agent_cli.sh \$EVIPADDR \$EVHOST \$EV"OS_TYPE" \$EV"INSTALLPP_INFO"</pre> If you want to use Amazon EC2 API Tools for compatibility, configure the following. <pre>/bin/sh /opt/jplbase/tools/cloud/jbsas_add_agent.sh \$EVIPADDR \$EVHOST \$EV"OS_TYPE" \$EV"INSTALLPP_INFO"</pre>

6. Set an automated action for terminating the monitoring of hosts that were scaled in.

To run an auto-scaling linkage script (`jbsas_del_agent_cli`), specify the automated action definition described in the table below. For details about automated action definitions, see the chapter on executing commands by using automated actions in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table L–2: Automated action definition (for scale in)

Definition item	Definition value
Action name	Any value
Event ID	4725, 4749, 474D
Event condition	None
User name of the user who executes the action	In Windows: User name of the JP1 user who is mapped to the OS user with <code>jpladmin</code> or Administrator permissions In Linux: User name of the JP1 user who is mapped to the OS user with <code>jpladmin</code> or superuser permissions
Target host	Manager host name
Action	In Windows: <pre>powershell -ExecutionPolicy RemoteSigned "&'installation- folder\tools\cloud\jbsas_del_agent_cli.ps1'" \$EVOBNAM <nul</pre> If you want to use Amazon EC2 API Tools for compatibility, configure the following. <pre>powershell -ExecutionPolicy RemoteSigned "&'installation- folder\tools\cloud\jbsas_del_agent.ps1'" \$EVOBNAM <nul</pre>

Definition item	Definition value
	<p>In Linux:</p> <pre>/bin/sh /opt/jplbase/tools/cloud/jbsas_del_agent_cli.sh \$EVOBNAM</pre> <p>If you want to use Amazon EC2 API Tools for compatibility, configure the following.</p> <pre>/bin/sh /opt/jplbase/tools/cloud/jbsas_del_agent.sh \$EVOBNAM</pre>

7. Install JP1/PFM - Manager.

8. Set the alarm table to be bound to agents.

In the script definition file (`jbsas_setup_manager_cli.ini`), specify the name of the alarm table that is to be bound to the agent hosts that were scaled out. For details about the script definition file, see [L.8 Auto-scaling linkage script](#).

When you perform setup for using JP1/Base linked with the auto-scaling functionality, configure other necessary settings such as the following:

- Specifying the automated action to be executed when an agent fails

In the automated action definition, if `$EVHOST` is specified as the host on which the automated action is to be executed, when an agent fails, the automated action will be executed on the agent that issued the failure event.

L.6 Setup procedure for using JP1/Base linked with the auto-scaling functionality (for agent hosts)

This subsection describes how to set up agent hosts when JP1/Base is to be linked with the auto-scaling functionality.

Perform the procedure described below on a virtual machine (EC2 instance) provided by the Amazon EC2 service.

Note that steps 3 to 7 are required if JP1/PFM is to be used for monitoring.

1. Install JP1/Base.

2. Enable the health check function of JP1/Base.

3. Install JP1/PFM - Base and JP1/PFM - Agent.

4. Configure JP1/PFM settings as necessary.

Some settings must be configured from JP1/PFM - Web Console while the JP1/PFM service is running. If you configured these settings while the JP1/PFM service is running, perform the following procedure:

1. Stop the JP1/PFM service on the agent host.

2. On the agent host, execute the `jpctool db clear` command to delete all record information.

3. On the manager host, execute the `jpctool service delete` command to delete the service information for the agent on which settings were specified. In addition, execute the `jpctool service sync` command to synchronize with JP1/PFM - Web Console.

5. (Linux only) Execute the `jpconf host hostmode - mode hostname` command to change the method for acquiring the names of monitored hosts to the `hostname` command.

6. Disable JP1/PFM's automatic startup settings.

In Windows:

For all JP1/PFM services, in the Windows **Services** dialog box, set **Startup type** to **Manual**.

In Linux:

If an automated startup script file (`jpc_start`) was deployed, delete it.

7. (JP1/PFM Base version 11 and only in Linux) Edit the automated startup script file of the service (`jpl_pc`).

Before editing:

```
#!/bin/sh
## Copyright (C) 2004, Hitachi, Ltd.
## Licensed Material of Hitachi, Ltd.
:
```

After editing:

```
#!/bin/sh
## Copyright (C) 2004, Hitachi, Ltd.
## Licensed Material of Hitachi, Ltd.
### BEGIN INIT INFO
# Provides: jpl_pc
# Required-Start: $local_fs $remote_fs $syslog $network
# Required-Stop: $local_fs $remote_fs $syslog $network
# Default-Start: 3 5
# Default-Stop: 0 6
# Description: Start PFM services.
### END INIT INFO
:
```

8. Add the manager host to the `hosts` file or DNS to enable communication.

9. Set a scale-out notification event.

In the script definition file (`jbsas_setup_agent.ini`), specify the manager host to which scale-out notification events are to be sent. You can change the event attributes (event ID and message).

For details about the script definition file, see [L.8 Auto-scaling linkage script](#).

10. (Windows only) Specify the settings for the Amazon EC2 startup service.

Specify the settings by performing the following steps.

For EC2Config:

1. Open the EC2 Services Properties dialog box.

Click the **EC2 Config Service Settings** in the Apps window.

2. Click the **General tab to expand the page.**

3. Select the **Set Computer Name check box and the **User Data** check box.**

For EC2Launch v1:

1. Open EC2LaunchSettings.

2. Select the check boxes **Set Computer Name and **Handle User Data**, and then apply the settings.**

For EC2Launch v2:

1. Open EC2LaunchSettings.

2. Click the **General tab to open the page.**

3. Select the check boxes **Set the computer name of the instance and **Reboot after setting computer name**, and then apply the settings.**

11. (Linux 7.3 or earlier only) Edit the `cloud.cfg` file.

Add the following line to the `/etc/cloud/cloud.cfg` file:

```
preserve_hostname: true
```

When you perform setup for using JP1/Base linked with the auto-scaling functionality, configure other necessary settings such as the following:

- Setting log file traps

By converting error messages that are output to the log file and other events into JP1 events and then forwarding the JP1 events to the manager host, you can perform processing such as recovery processing by the manager host.

- Changing the setting for forwarding JP1 events

During the initial configuration of the forwarding settings file (`forward`), the setting for forwarding JP1 events is set as shown below. If you plan to forward important events, change this setting.

```
to-upper
E.SEVERITY IN Warning Error Critical Alert Emergency Emergence
end-to
```

L.7 Configuring the Amazon EC2 service

This subsection describes how to configure the settings required for the Amazon EC2 service.

Perform this procedure by using the **AWS Management Console**. For details about the **AWS Management Console** and how to use it, go to the official Amazon Web Services site.

1. Create a virtual machine image of the agent host.

Create a virtual machine image (AMI) of the agent host that was set up in *L.6 Setup procedure for using JP1/Base linked with the auto-scaling functionality (for agent hosts)*. For details about how to create images, go to the official Amazon Web Services site.

2. Create an Auto Scaling launch configuration or an Auto Scaling startup template.

To start a virtual machine by Auto Scaling, you need to specify settings to execute the script (`jbsas_setup_agent`) linked with Auto Scaling.

Specify the settings by performing the following steps.

When creating a launch configuration:

1. From the **AWS Management Console**, open the **Amazon EC2** console.
2. In **Auto Scaling** in the left-hand navigation pane, click **Launch Configuration**.
3. Click **Create Launch Configuration**.
4. From the Select AMI window, select the virtual machine image (AMI) that was created in step 1.
5. In the Advanced Settings window, click **Advanced Settings - User Data**, select **Text**, and then enter the following code in the text box:

When creating a startup template:

1. From **AWS Management Console**, open the **Amazon EC2** console.
2. In **Instance** in the navigation pane on the left, click **Startup Template**.
3. Click **Create Startup Template**.
4. From the **Select AMI** window, select the virtual machine image (AMI) that you created in step 1.
5. In the **Advanced Details** window, enter the following in the textbox **User Data**.

Text to be entered in User Data.

In Windows:

```
<script>
powershell -ExecutionPolicy RemoteSigned "&'installation-folder\tools\cloud\jbsas_setup_agent.ps1'"
</script>
```

In Linux #:

```
#!/bin/sh
/bin/hostnamed set-hostname ` /bin/hostname | /bin/sed -e 's/\..*//' `
/bin/sh /opt/jplbase/tools/cloud/jbsas_setup_agent.sh
```

#: In line 2 of the command for Linux, change the domain names to short names if the host names are in FQDN format. If JP1/PFM is not used and host names in FQDN format are used, these lines are not needed.

6. Follow the displayed instructions to finish configuring the settings.

3. Create an Auto Scaling group.

Use the launch configuration or startup template that you created in step 2 to create an Auto Scaling group that controls autoscaling action.

For details about how to create Auto Scaling groups, see the official Amazon Web Services site.

When a new setup is performed by using the setup command (`jegn_setup`), the default port number that is set when the port number specification (the `-port` option) is omitted was changed.

Values related to English UTF-8 encoding were added to the values that can be specified for the environment variable `LANG` in the environment variable file (the `jegn_env.conf` file) and the `jplbs_param.conf` file of JP1/Base.

L.8 Auto-scaling linkage script

JP1/Base provides a batch-processing script (auto-scaling linkage script) that performs the setup and operations required for using JP1/Base linked with the auto-scaling functionality.

(1) File configuration

The auto-scaling linkage script consists of the following files: script files to be executed on the manager or an agent, script definition files that define the variables needed to run the scripts, and internal files that are used internally by the scripts.

Note that the script file for Windows is a PowerShell script and the script file for Linux is a shell script.

Table L-3: Script files

Script file name	Target host	Description
In Windows: <code>jbsas_setup_agent.ps1</code> <code>jbsas_setup_agent.ps1.model</code> In Linux: <code>jbsas_setup_agent.sh</code> <code>jbsas_setup_agent.sh.model</code>	Agent	Script file that is run at the agent host during scaling out, and its model file. It performs the initial setup for the agent and sends a JP1 event to the manager to notify the manager of the scale out.
In Windows: <code>jbsas_add_agent_cli.ps1</code> <code>jbsas_add_agent_cli.ps1.model</code> In Linux: <code>jbsas_add_agent_cli.sh</code>	Manager	Script file that is run at the manager host during scaling out, and its model file. It adds the new hosts to the manager's monitoring targets.

Script file name	Target host	Description
jbsas_add_agent_cli.sh.model		
In Windows: jbsas_add_agent.ps1 jbsas_add_agent.ps1.model In Linux: jbsas_add_agent.sh jbsas_add_agent.sh.model	Manager	When Amazon EC2 API Tools is used for compatibility, this is the script file that is run at the manager host during scaling out, and its model file. The script adds the new hosts to the manager's monitoring targets.
In Windows: jbsas_del_agent_cli.ps1 jbsas_del_agent_cli.ps1.model In Linux: jbsas_del_agent_cli.sh jbsas_del_agent_cli.sh.model	Manager	Script file that is run at the manager host during scaling in, and its model file. It removes deleted hosts from the manager's monitoring targets.
In Windows: jbsas_del_agent.ps1 jbsas_del_agent.ps1.model In Linux: jbsas_del_agent.sh jbsas_del_agent.sh.model	Manager	When Amazon EC2 API Tools is used for compatibility, this is the script file that is run at the manager host during scaling in, and its model file. The script removes deleted hosts from the manager's monitoring targets.

Table L–4: Script definition files

Definition file name	Target host	Description
jbsas_setup_agent.ini jbsas_setup_agent.ini.model	Agent	File that defines the shell variables used by the script file (jbsas_setup_agent) that is run by agent hosts, and its model file.
jbsas_setup_manager_cli.ini jbsas_setup_manager_cli.ini.model	Manager	File that defines the shell variables used by the script file (jbsas_add_agent_cli or jbsas_del_agent_cli) that is run by manager hosts, and its model file.
jbsas_setup_manager.ini jbsas_setup_manager.ini.model	Manager	When Amazon EC2 API Tools is used for compatibility, file that defines the shell variables used by the script file (jbsas_add_agent or jbsas_del_agent) that is run by manager hosts, and its model file.

Table L–5: Internal files

File name	Target host	Description
In Windows: jbsas_util.ps1 jbsas_util.ps1.model In Linux: jbsas_util.sh jbsas_util.sh.model	Common (manager and agent)	File containing all the functions that are used internally by the script files, and its model file.
jbsas_hosts	Manager	This file is used to manage information about monitored agent hosts.

(2) Storage directory

The files for auto-scaling linkage scripts are all stored in the following directory:

In Windows:

```
installation-folder\tools\cloud\
```

In Linux:

```
/opt/jp1base/tools/cloud/
```

(3) Script files

For details about the processing performed by the script files, see [L.3 Adding hosts to the monitoring target during scale out](#) and [L.4 Terminating monitoring during scale in](#).

You do not need to edit the script files. You can customize them, but note that our support services do not cover parts of scripts that have been added or changed.

If you performed overwrite installation from JP1/Base 11-00, the script files (such as `jbsas_add_agent.ps1`) are not overwritten. Copy the model files (such as `jbsas_add_agent.ps1.model`) and assign the correct script file names to use them.

(4) Script definition files

Format

```
variable-name-1=variable-value-1  
[variable-name-2=variable-value-2]  
:
```

Description

- Do not use any spaces or tabs before or after a variable name, a variable value, or an equal sign (=).
- In Linux, if the variable value contains a space, enclose the entire variable in double quotation marks (").

Definition application timing

The definition is loaded when the script file is executed.

Setting parameters

The following tables describe the parameters to be specified in the `jbsas_setup_agent.ini` file and the `jbsas_setup_manager.ini` file.

Table L–6: Parameters to be specified in the `jbsas_setup_agent.ini` file

Variable name	Variable value (default value)	Specification	Description
ManagerHostName	Manager	Required	Specify a manager host name. For details about the characters and the number of characters permitted for host names, see the documentation for the related products (JP1/IM or JP1/PFM).
JP1EventID	1011	Customizable	Specify the event ID of the JP1 event that is to be sent to the manager. You can specify values in the range from 0 to 1FFF and from 7FFF8000 to 7FFFFFFF.

Variable name	Variable value (default value)	Specification	Description
JP1EventMsg	<p>In Windows: Agent host (\$AgentHostName) has scale-out.</p> <p>In Linux: "Agent host (\$AgentHostName) has scale-out."</p>	Customizable	<p>Specify the message for the JP1 event that is to be sent to the manager.</p> <p>Specify a character string of no more than 1,023 bytes.</p> <p>In the default message, the agent host name is displayed for \$AgentHostName.</p>

Legend:

Required: The parameter must be specified.

Customizable: Customize the value of the parameter as needed.

Table L–7: Parameters to be specified in the jbsas_setup_manager_cli.ini file

Variable name	Variable value (default value)	Specification	Description
JbsrtDistribByScaleIn	NO	Customizable	<p>Specify whether configuration definition information is to be updated during scale in.</p> <p>If YES is specified: The target host is deleted from the configuration definition file, and then the configuration definition is distributed. The target host is immediately deleted from lower-level hosts in the configuration definition information. Do not specify YES unless it is necessary for operation, because this might result in a significant delay in monitoring due to a delay in communication. As a guideline, if you plan to specify YES, make sure that the number of hosts that are scaled in or out each hour does not exceed 20.</p> <p>If NO is specified: Specify NO to prioritize performance. The target host will not be deleted from the configuration definition file, and the configuration definition will not be distributed. The configuration definition information is updated during the next scale out.</p>
JP1PFMAgentAlarmTableList_W	"PFM Windows Template Alarms [CPU] 09.00", "PFM Windows Template Alarms [MEM] 09.00", "PFM Windows Template Alarms [DSK] 09.00"	Customizable	<p>Specify the name of the alarm table for Windows that is to be bound to agents.</p> <p>To specify multiple names, delimit the names by using commas.</p>
JP1PFMAgentAlarmTableList_L	"PFM UNIX Template Alarms [CPU] 09.00", "PFM UNIX Template Alarms [MEM] 09.00", "PFM UNIX Template Alarms [DSK] 09.00"	Customizable	<p>Specify the name of the alarm table for Linux that is to be bound to agents.</p> <p>To specify multiple names, delimit the names by using commas.</p>
EC2_HOMEPath#	Not specified	Required	Specify the path where AWS CLI is to be installed.
EC2_URL#	Not specified	Required	Specify the URL of the AWS region.

Variable name	Variable value (default value)	Specification	Description
AWS_ACCESS_KEY#	Not specified	Required	Specify the AWS access key character string.
AWS_SECRET_KEY#	Not specified	Required	Specify the AWS secret access key character string.

Legend:

Required: The parameter must be specified.

Customizable: Customize the value of the parameter as needed.

#: This environment variable is required to configure a tool execution environment for AWS CLI. For details about the values to be set, see the official Amazon Web Services site.

Table L–8: Parameters to be specified in the jbsas_setup_manager.ini file

Variable name	Variable value (default value)	Specification	Description
JbsrtDistribByScaleIn	NO	Customizable	Specify whether configuration definition information is to be updated during scale in. If YES is specified: The target host is deleted from the configuration definition file, and then the configuration definition is distributed. The target host is immediately deleted from lower-level hosts in the configuration definition information. Do not specify YES unless it is necessary for operation, because this might result in a significant delay in monitoring due to a delay in communication. As a guideline, if you plan to specify YES, make sure that the number of hosts that are scaled in or out each hour does not exceed 20. If NO is specified: Specify NO to prioritize performance. The target host will not be deleted from the configuration definition file, and the configuration definition will not be distributed. The configuration definition information is updated during the next scale out.
JP1PFMAgentAlarmTableList_W	"PFM Windows Template Alarms [CPU] 09.00", "PFM Windows Template Alarms [MEM] 09.00", "PFM Windows Template Alarms [DSK] 09.00"	Customizable	Specify the name of the alarm table for Windows that is to be bound to agents. To specify multiple names, delimit the names by using commas.
JP1PFMAgentAlarmTableList_L	"PFM UNIX Template Alarms [CPU] 09.00", "PFM UNIX Template Alarms [MEM] 09.00", "PFM UNIX Template Alarms [DSK] 09.00"	Customizable	Specify the name of the alarm table for Linux that is to be bound to agents. To specify multiple names, delimit the names by using commas.
EC2_HOMEPath#	Not specified	Required	Specify the path where Amazon EC2 API Tools is to be installed.
JAVA_HOMEPath#	Not specified	Required	Specify the path of the Java (JRE) installation target.

Variable name	Variable value (default value)	Specification	Description
EC2_URL [#]	Not specified	Required	Specify the URL of the AWS region.
AWS_ACCESS_KEY [#]	Not specified	Required	Specify the AWS access key character string.
AWS_SECRET_KEY [#]	Not specified	Required	Specify the AWS secret access key character string.

Legend:

Required: The parameter must be specified.

Customizable: Customize the value of the parameter as needed.

[#]: This environment variable is required to configure a tool execution environment for Amazon EC2 API Tools. For details about the values to be set, see the official Amazon Web Services site.

L.9 Processing time required for configuring and clearing monitoring settings

This subsection describes how to estimate the amount of time required for configuring monitoring settings after a scale out is detected by the manager host, and the amount of time required for clearing monitoring settings after a scale in is detected.

(1) Time required for configuring monitoring settings after a scale out

Use the formulas in the table below to estimate the amount of time required for configuring the monitoring settings of the manager host for agent hosts that are added during a scale out.

OS	Processing time for configuring monitoring settings
Windows	$((\text{Number of hosts managed in the configuration before scale out} + \text{number of hosts managed in the configuration after scale out})/2) \times (15 \text{ seconds}/100 \text{ hosts}) \times \text{number of hosts added during scale out}$
Linux	$((\text{Number of hosts managed in the configuration before scale out} + \text{number of hosts managed in the configuration after scale out})/2) \times (5 \text{ seconds}/100 \text{ hosts}) \times \text{number of hosts added during scale out}$

Note

In a large-scale environment where the configuration of many hosts (600 hosts or more) is managed, we recommend that you limit the number of hosts that can be scaled in or out to 20 hosts per hour.

(2) Time required for clearing monitoring settings after a scale in

Use the formulas in the table below to estimate the amount of time required for clearing the monitoring settings of the manager host for agent hosts that are deleted during scale in. Note that this processing time assumes that the default value NO is set for the setting parameter `JbsrtDistribByScaleIn`.

OS	Processing time for clearing monitoring settings	
	When JP1/PFM is used	When JP1/PFM is not used
Windows	$(\text{About } 35 \text{ seconds per host}) \times \text{number of hosts deleted during scale in}$	$(\text{About } 6 \text{ seconds per host}) \times \text{number of hosts deleted during scale in}$

OS	Processing time for clearing monitoring settings	
	When JP1/PFM is used	When JP1/PFM is not used
Linux	(About 30 seconds per host) x <i>number of hosts deleted during scale in</i>	(About 5 seconds per host) x <i>number of hosts deleted during scale in</i>

L.10 Notes about using JP1/Base linked with the auto-scaling functionality

- The monitoring settings of hosts that were monitored by the manager host before JP1/Base was linked with the auto-scaling functionality will not be cleared during scale in. Only the monitoring settings of hosts for which monitoring was started by executing a script on the manager host will be cleared during scale in.
- While JP1/Base is linked with the auto-scaling functionality, do not manually edit any of the following files on the manager host. If these files are edited, operation is not guaranteed.
 - Health check definition file (`jbshc.conf`)
 - Configuration definition file (`jbs_route.conf`)
 - Agent management information file (`jbsas_hosts`)
 - The `hosts` file of the OS

If you need to edit any of these files for maintenance or other reasons, either temporarily stop the auto-scaling functionality or suspend operation by stopping JP1 product services. Do not edit the definitions of host names that were added by the function for configuring monitoring settings that was used to link JP1/Base to the auto-scaling functionality.

- If monitoring is terminated during a scale in, depending on the status of the agent host, the monitoring process might end normally, instead of being terminated. If the number of monitored remote hosts in the health check definition file exceeds 2,500 because monitoring was not terminated, a definition error occurs and the `KAVA7052-W` message is output. If this happens, check the names of the hosts subject to auto-scaling in AWS and the health check definition file to determine whether the names of any hosts that no longer need to be monitored still remain in the definition file. If the names of hosts that no longer need to be monitored remain in the definition file because monitoring was not terminated during scale in, terminate the monitoring of those agent hosts by running the following script:

For Windows (run in PowerShell):

```
installation-folder\tools\cloud\jbsas_del_agent_cli.ps1 name-of-agent-host-for-which-monitoring-is-to-be-terminated
```

If using Amazon EC2 API Tools for compatibility:

```
installation-folder\tools\cloud\jbsas_del_agent.ps1 name-of-agent-host-for-which-monitoring-is-to-be-terminated
```

For Linux:

```
/opt/jplbase/tools/cloud/jbsas_del_agent_cli.sh name-of-agent-host-for-which-monitoring-is-to-be-terminated
```

If using Amazon EC2 API Tools for compatibility:

```
/opt/jplbase/tools/cloud/jbsas_del_agent.sh name-of-agent-host-for-which-monitoring-is-to-be-terminated
```

M. Notes on using Docker, Podman (Linux only)

M.1 Creating a Docker image

The following describes how to import this software product into a Docker image:

1. Copy the product media content to the Dockerfile storage directory in advance.

Make sure that the copied files match by performing a comparison (at the binary level).

```
# mount /dev/cdrom directory-mounted-on-the-host
# cp -a directory-mounted-on-the-host Dockerfile-storage-directory
```

In the Dockerfile example provided below, the product media is copied to *Dockerfile-storage-directory/media*.

2. If the system has a local yum repository server specified, the repository file is created in the Dockerfile storage directory.

3. Create a Dockerfile in order to create a Docker image.

A sample is shown below. For details about the Dockerfile format, see the Dockerfile reference which is posted on the Docker website, or refer to `man dockerfile`.

```
FROM rhel7.1:latest #1
MAINTAINER Name mail address #2
COPY local.repo /etc/yum.repos.d/ #3
RUN yum -y install glibc.i686 libstdc++.i686 ncompress ncursespsmisc glibc
-devel glibc-devel.i686 #4
RUN yum -y install tar iputils net-tools procps-ng hostname #5
RUN localedef -i ja_JP -f UTF-8 ja_JP.utf8 #6
RUN mkdir /var/tmp/JP1 #7
COPY media /var/tmp/JP1 #8
WORKDIR /var/tmp/JP1 #9
RUN export LANG=ja_JP.utf8 && ./LINUX/setup -f -k product-type ./ #10
...
RUN rm -rf /var/tmp/JP1 #11
```

#1

Specify the base Docker image. The script `:latest` specifies the latest image.

#2

As the image administrator, specify the name or contact email address of the person who created the image. This step can be omitted.

#3

Specify that the repository file created in advance is to be copied into the container.

#4

Specify that the prerequisite packages for this product are to be installed in advance.

#5

When using a Docker image from Linux 7 as a base image, install the commands that are not installed by default (tar, ps, hostname, netstat, and ping).

#6

Add locales. (In the example above, UTF-8 is added.)

#7

Create a work directory in the container.

#8

Specify that the following is to be copied to `/var/tmp/JP1` on the container: the contents of the product media that were previously copied to the Dockerfile storage directory.

#9

Specify that the current directory is to be set as `/var/tmp/JP1` on the container.

#10

Specify the `LANG` environment parameter according to the language requirements, and then specify that the installation is to be performed on the container by using the silent installation functionality of Hitachi Program Product Installer. (In the above example, UTF-8 is specified.)

If you do not specify the `LANG` environment parameter, the installation setup is performed assuming a `C` environment.

#11

Specify that the work directory on the container is to be deleted.

4. Use the `docker build` command to specify the Dockerfile created in step 3, and then create the Docker image.

```
# docker build -t Docker-image-name Dockerfile-storage-directory
```

To execute the above command, using the example of a Dockerfile created in step 3, the current directory must be the Dockerfile storage directory.

M.2 Notes on installing JP1/Base on a container

To install JP1/Base on a Docker container, and to connect to a Docker host or other hosts, the prerequisites below must be met, and the procedure below must be performed.

A host on which Docker is installed is referred to as a Docker host. A container provided by Docker is referred to as a container.

(1) Prerequisites

To connect a Docker container which JP1/Base is installed with outside containers, TCP/IP communication must be set in both directions to perform properly. The examples are shown below.

(a) To use port forwarding functionality

1. An IP address that can be used to communicate with a connected host is statically assigned to each container.
To connect a container that has JP1/Base installed to hosts other than containers, statically assign to the Docker host an IP address corresponding to each container.
2. Port forwarding settings are configured for Docker containers for which IP addresses are explicitly specified.
To connect a container to hosts other than containers, you must specify the port forwarding settings for the IP addresses assigned in step 1 to forward data from the port number used by JP1/Base on the Docker host side to the port number used by JP1/Base on the container side.
For details about the ports used by JP1/Base, see [Appendix C. List of Port Numbers](#).

```
# docker run -p external-IP-address:port-used-by-JP1/Base-onPthe-external
-IP-address:port-used-by-JP1/Base-on-the-container ...
```

-p: Map the port for JP1/Base in a given container to the port on the IP address over which communication can be initiated from external locations.

Example settings:

```
# docker run --privileged -p xxx.xxx.xxx.xxx:20098:20098
-p xxx.xxx.xxx.xxx:20099:20099 -p xxx.xxx.xxx.xxx:20237:20237
-p xxx.xxx.xxx.xxx:20238:20238 -p xxx.xxx.xxx.xxx:20239:20239
-p xxx.xxx.xxx.xxx:20240:20240 -p xxx.xxx.xxx.xxx:20306:20306
-p xxx.xxx.xxx.xxx:20600:20600 --name container-name --hostname host-name
-id base-image-name:tag-name
```

"xxx.xxx.xxx.xxx" indicates an IP address statically assigned to the Docker host in step 1.

For details about each option, see the Release Notes provided on the Docker website.

3. The container is started in privileged mode.

For some JP1/Base commands, you must start the container in privileged mode. Start the container that has JP1/Base installed in privileged mode (`--privileged`). See step 2 above for example settings.

4. JP1 events are forwarded from a container.

When JP1 events are forwarded from JP1/Base installed on a container to other hosts, the IP addresses specified in step 1 and step 2 are not set as the source IP addresses of the forwarded JP1 events. For this reason, avoid performing operations on the host to which the JP1 events have been forwarded that use the source IP addresses of events forwarded from a container.

(b) To use the Macvlan bridge on the Docker host

1. The container is started in privileged mode.

For some JP1/Base commands, you must start the container in privileged mode. Start the container that has JP1/Base installed in privileged mode (`--privileged`). See the following for example settings.

```
# docker run --privileged --name container-name --hostname host-name -id b
ase-image-name:tag-name
```

2. Set the macvlan on Docker host, and then create VNIC.

```
# ip link add link IF-with-IP-address-to-connect-outside-of-a-Docker-host
name VNIC-name type macvlan mode private
```

3. Assign VNIC to the container on Docker host.

```
# ID=containerID
# ip link set VNIC-name netns $(docker inspect --format "{{.State.Pid}}" $
ID)
```

4. Operate container from Docker host, and then give an IP address to the assigned VNIC.

```
# docker exec $ID yum install -y iproute libmnl libnfnetlink libnetfilter_
contrack iptables
# docker exec $ID ip addr add dev VNIC-name IP-address-to-give/net-mask
# docker exec $ID ip link set VNIC-name up
```

This operation does not required when all of the IP address setting commands have already installed.

5. JP1 event of which transferred from container

When JP1 events are transferred from JP1/Base on container to the other hosts, "Source IP address" attributes of JP1 event is not the same with the one set in step 1 and step 2 above. For this reason, you must avoid to operate using "Source IP address" attributes of JP1 events transferred from container on the destination host.

(2) Configuration procedure

1. Reconfigure the authentication server for JP1/Base within a container.

If JP1/Base is installed by using Dockerfile, the host name when JP1/Base is installed (when a Docker image is created) differs from the host name when the container is started, so the primary authentication server name specified during installation will differ from the physical host name when the container is started. For this reason, to use an authentication server within the container, you need to re-specify the host name to be used when the container is started.

To do this, you must execute the following at the command line:

```
# /opt/jp1base/bin/jbssetusrsvr `hostname`
```

2. On JP1/Base on the container, specify in JP1hosts2 the hosts to which connections are made.

The `hosts` file in a container is overwritten during start and stop operations, and the information about other hosts is deleted. For this reason, specify in `jp1hosts2` information about the hosts to which connections are made.

3. On the hosts to which connections are made, specify the settings so that the host name of the container can be resolved to the IP address corresponding to the container set in step 1 and step 2.

When a Docker container receives requests from external locations, the container waits for requests on the IP address that corresponds to the container. For this reason, on the host to which connections will be made, specify the settings so that the host name of the container can be resolved to the IP address corresponding to the container.

4. Starting a container

You cannot use the function to automatically start JP1/Base services when the Docker container starts. To start the JP1/Base services after the Docker container starts, use the command for starting JP1/Base. Alternatively, create a shell script that includes the command that must be executed to start the Docker container, and consider executing the command for starting JP1/Base by using that shell script.

For details about the commands to start JP1/Base, see [7.2 Starting and stopping JP1/Base \(in UNIX\)](#).

5. Stopping a container

Use the command for terminating JP1/Base to stop the JP1/Base services, and then stop the container.

For details about the commands for stopping JP1/Base, see [7.2 Starting and stopping JP1/Base \(in UNIX\)](#).

6. Linkage between containers

Use the container-linkage functionality (`--link`) to link between containers. For details about linking between containers, refer to the Docker Engine reference on the Docker website.

M.3 Notes on installing JP1/Base on the Docker host and container

You must specify the following settings to install JP1/Base on the Docker host and container.

Applying `physical_ipip.conf` to a JP1/Base installation on the Docker host

To install JP1/Base on both the Docker host and container, first install JP1/Base on the Docker host, and then use the `jbssetcnf` command to apply `physical_ipip.conf`.

```
# /opt/jp1base/bin/jbssetcnf /etc/opt/jp1base/conf/physical_ipip.conf
```

M.4 Creating a Podman image

Because Red Hat Enterprise Linux 8 and later does not support the Docker commands and the Docker engine, use the following procedure for importing JP1/Base into Podman provided instead of Docker.

1. Copy the product media content to the Dockerfile[#] storage directory in advance.

Make sure that the copied files match by performing a comparison (at the binary level).

```
# mount /dev/cdrom directory-mounted-on-the-host
# cp -a directory-mounted-on-the-host Dockerfile-storage-directory
```

#

Podman can also create images using the Dockerfile.

In the Dockerfile example provided below, the product media is copied to *Dockerfile-storage-directory/media*.

2. If the system has a local yum repository server specified, the repository file is created in the Dockerfile storage directory.

3. Create a Dockerfile in order to create a Podman image.

A sample is shown below. For details about the Dockerfile format, see the Dockerfile reference which is posted on the Docker website, or refer to `man dockerfile`.

```
FROM rhel8.1:latest #1
MAINTAINER Name mail address #2
COPY local.repo /etc/yum.repos.d/ #3
RUN yum -y install glibc.i686 libstdc++.i686 libnsl.i686 ncompress ncurses
psmisc glibc-devel glibc-devel.i686 #4
RUN yum -y install tar iputils net-tools procps-ng hostname #5
RUN localedef -i ja_JP -f UTF-8 ja_JP.utf8 #6
RUN mkdir /var/tmp/JP1 #7
COPY media /var/tmp/JP1 #8
WORKDIR /var/tmp/JP1 #9
RUN export LANG=ja_JP.utf8 && ./LINUX/setup -f -k product-type ./ #10
...
RUN rm -rf /var/tmp/JP1 #11
```

#1

Specify the base Podman image. The script `:latest` specifies the latest image.

#2

As the image administrator, specify the name or contact email address of the person who created the image. This step can be omitted.

#3

Specify that the repository file created in advance is to be copied into the container.

#4

Specify that the prerequisite packages for this product are to be installed in advance.

#5

When using a Podman image from Linux 7 as a base image, install the commands that are not installed by default (tar, ps, hostname, netstat, and ping).

#6

Add locales. (In the example above, UTF-8 is added.)

#7

Create a work directory in the container.

#8

Specify that the following is to be copied to `/var/tmp/JP1` on the container: the contents of the product media that were previously copied to the Dockerfile storage directory.

#9

Specify that the current directory is to be set as `/var/tmp/JP1` on the container.

#10

Specify the `LANG` environment parameter according to the language requirements, and then specify that the installation is to be performed on the container by using the silent installation functionality of Hitachi Program Product Installer. (In the above example, UTF-8 is specified.)

If you do not specify the `LANG` environment parameter, the installation setup is performed assuming a `C` environment.

#11

Specify that the work directory on the container is to be deleted.

4. Use the `docker build` command to specify the Dockerfile created in step 3, and then create the Podman image.

```
# podman build -t Podman-image-name Dockerfile-storage-directory
```

To execute the above command, using the example of a Dockerfile created in step 3, the current directory must be the Dockerfile storage directory.

M.5 Notes on installing JP1/Base on a container

To install JP1/Base on a Podman container, and to connect to a Podman host or other hosts, the prerequisites below must be met, and the procedure below must be performed.

A host on which Podman is installed is referred to as a Podman host. A container provided by Podman is referred to as a container.

(1) Prerequisites

To connect a Podman container which JP1/Base is installed with outside containers, TCP/IP communication must be set in both directions to perform properly. The examples are shown below.

(a) To use port forwarding functionality

1. An IP address that can be used to communicate with a connected host is statically assigned to each container.
To connect a container that has JP1/Base installed to hosts other than containers, statically assign to the Podman host an IP address corresponding to each container.
2. Port forwarding settings are configured for Podman containers for which IP addresses are explicitly specified.
To connect a container to hosts other than containers, you must specify the port forwarding settings for the IP addresses assigned in step 1 to forward data from the port number used by JP1/Base on the Podman host side to the port number used by JP1/Base on the container side.
For details about the ports used by JP1/Base, see [Appendix C. List of Port Numbers](#).


```
# podman run -p external-IP-address:port-used-by-JP1/Base-on-the-external-IP-address:port-used-by-JP1/Base-on-the-container ...
```

-p: Map the port for JP1/Base in a given container to the port on the IP address over which communication can be initiated from external locations.

Example settings:

```
# docker run --privileged -p xxx.xxx.xxx.xxx:20098:20098
-p xxx.xxx.xxx.xxx:20099:20099 -p xxx.xxx.xxx.xxx:20237:20237
-p xxx.xxx.xxx.xxx:20238:20238 -p xxx.xxx.xxx.xxx:20239:20239
-p xxx.xxx.xxx.xxx:20240:20240 -p xxx.xxx.xxx.xxx:20306:20306
-p xxx.xxx.xxx.xxx:20600:20600 --name container-name --hostname host-name
-id base-image-name:tag-name
```

"xxx.xxx.xxx.xxx" indicates an IP address statically assigned to the Podman host in step 1.

For details about each option, see the Release Notes provided on the Podman website.

3. The container is started in privileged mode.

For some JP1/Base commands, you must start the container in privileged mode. Start the container that has JP1/Base installed in privileged mode (`--privileged`). See step 2 above for example settings.

4. JP1 events are forwarded from a container.

When JP1 events are forwarded from JP1/Base installed on a container to other hosts, the IP addresses specified in step 1 and step 2 are not set as the source IP addresses of the forwarded JP1 events. For this reason, avoid performing operations on the host to which the JP1 events have been forwarded that use the source IP addresses of events forwarded from a container.

(b) To use the Macvlan bridge on the Podman host

1. The container is started in privileged mode.

For some JP1/Base commands, you must start the container in privileged mode. Start the container that has JP1/Base installed in privileged mode (`--privileged`). See the following for example settings.

```
# podman run --privileged --name container-name --hostname host-name -id base-image-name:tag-name
```

2. Set the macvlan on Podman host, and then create VNIC.

```
# ip link add link IF-with-IP-address-to-connect-outside-of-a-Podman-host
name VNIC-name type macvlan mode private
```

3. Assign VNIC to the container on Podman host.

```
# ID=containerID
# ip link set VNIC-name netns $(podman inspect --format "{{.State.Pid}}" $ID)
```

4. Operate container from Podman host, and then give an IP address to the assigned VNIC.

```
# podman exec $ID yum install -y iproute libmnl libnfnetlink libnetfilter_
contrack iptables
# podman exec $ID ip addr add dev VNIC-name IP-address-to-give/net-mask
# podman exec $ID ip link set VNIC-name up
```

This operation does not required when all of the IP address setting commands have already installed.

5. JP1 event of which transferred from container

When JP1 events are transferred from JP1/Base on container to the other hosts, "Source IP address" attributes of JP1 event is not the same with the one set in step 1 and step 2 above. For this reason, you must avoid to operate using "Source IP address" attributes of JP1 events transferred from container on the destination host.

(2) Configuration procedure

1. Reconfigure the authentication server for JP1/Base within a container.

If JP1/Base is installed by using Dockerfile, the host name when JP1/Base is installed (when a Podman image is created) differs from the host name when the container is started, so the primary authentication server name specified during installation will differ from the physical host name when the container is started. For this reason, to use an authentication server within the container, you need to re-specify the host name to be used when the container is started.

To do this, you must execute the following at the command line:

```
# /opt/jp1base/bin/jbssetusrsvr `hostname`
```

2. On JP1/Base on the container, specify in JP1hosts2 the hosts to which connections are made.

The `hosts` file in a container is overwritten during start and stop operations, and the information about other hosts is deleted. For this reason, specify in `jp1hosts2` information about the hosts to which connections are made.

3. On the hosts to which connections are made, specify the settings so that the host name of the container can be resolved to the IP address corresponding to the container set in step 1 and step 2.

When a Podman container receives requests from external locations, the container waits for requests on the IP address that corresponds to the container. For this reason, on the host to which connections will be made, specify the settings so that the host name of the container can be resolved to the IP address corresponding to the container.

4. Starting a container

You cannot use the function to automatically start JP1/Base services when the Podman container starts. To start the JP1/Base services after the Podman container starts, use the command for starting JP1/Base. Alternatively, create a shell script that includes the command that must be executed to start the Podman container, and consider executing the command for starting JP1/Base by using that shell script.

For details about the commands to start JP1/Base, see [7.2 Starting and stopping JP1/Base \(in UNIX\)](#).

5. Stopping a container

Use the command for terminating JP1/Base to stop the JP1/Base services, and then stop the container.

For details about the commands for stopping JP1/Base, see [7.2 Starting and stopping JP1/Base \(in UNIX\)](#).

6. Linkage between containers

Podman does not support the container link function (`--link`). If you want to link containers, edit the `/etc/hosts` file of each container so that the host name and the IP address of the container are mapped.

M.6 Notes on installing JP1/Base on the Podman host and container

You must specify the following settings to install JP1/Base on the Podman host and container.

Applying `physical_ipip.conf` to a JP1/Base installation on the Podman host

To install JP1/Base on both the Podman host and container, first install JP1/Base on the Podman host, and then use the `jbssetcnf` command to apply `physical_ipip.conf`.

```
# /opt/jp1base/bin/jbssetcnf /etc/opt/jp1base/conf/physical_ipip.conf
```

N. Version Changes

N.1 Changes in 13-00

(1) Changes in the manuals 3021-3-L09 and 3021-3-L09(E)

- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2022
 - Red Hat(R) Enterprise Linux(R) Server 9 (64-bit x86_64)
 - Oracle Linux(R) Operating System 9
- The following OSs were deleted from the supported OSs:
 - Windows(R) 10 Enterprise 32-bit
 - Windows(R) 10 Home 32-bit
 - Windows(R) 10 Pro 32-bit
 - HP-UX 11i V3 (IPF)
 - Solaris 11 (SPARC)
 - Red Hat(R) Enterprise Linux(R) Server 6 (64-bit x86_64)
 - Oracle Linux(R) Operating System 6 (x64)
 - CentOS 6 (x64)
 - CentOS 7
 - CentOS 8
- The following functions were removed:
 - JP1/SES compatibility function
 - SNMP trap conversion function

As a result, descriptions pertaining to the abovementioned functions were also deleted or changed.

- A description of the procedure used to select JP1/Base included with media provided for JP1/AJS or JP1/IM was added to the description of the JP1/Base installation procedure (for Windows).
- A precautionary note when overwriting an install of JP1/Base version 13-00 or later over a 12-50 or earlier version of JP1/Base was added.
- Explanations of the following items were added, and a description assuming the use of such in 2038 and later was provided:
 - Enabling big timestamps when running in Linux
 - Preventing the ability to start command execution services
 - JP1/Base startup process definition file
- UTF-8 was added as an English encoding available for use in Linux.

The following files were added to the JP1/Base definition files:

- Character code mapping definition file
- Language type mapping definition file

As a result, an additional procedure was added for changing the character code and language type mapping definition after installing an upgraded version of the software.

- The use of ECC-encrypted server certificates for SSL communication was enabled.
As a result, the description on how to create a private key was changed as part of the setup procedure for establishing an SSL communication environment on the server. Additional descriptions were added to provide examples of the use of the `openssl` command when using elliptic-curve cryptography, and to describe how to specify private key file names in the SSL communication definition file.
- With regard to event filter syntax, the value range of condition statement attributes `B.TIME` (Registered time) and `B.ARRIVEDTIME` (Arrived time) was changed.
As a result, descriptions of keywords for comparing condition statements, `RANGE`, `TRANGE`, and `WITHIN` were changed.
- The type of the following parameters in the event server settings file was changed from required parameters to custom parameters:
 - `include`
 - `options v5-unused`
- TLS1.3 was added as an SSL communication version that can be specified to the SSL communication definition file. An explanation on specifying an ECC-format encryption suite was added.
- AWS CLI-compatible scripts for use with auto-scaling linkage were added.

(2) Changes in the manuals 3021-3-L10 and 3021-3-L10(E)

- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2022
 - Red Hat(R) Enterprise Linux(R) Server 9 (64-bit x86_64)
 - Oracle Linux(R) Operating System 9
- The following OSs were deleted from the supported OSs:
 - Windows(R) 10 Enterprise 32-bit
 - Windows(R) 10 Home 32-bit
 - Windows(R) 10 Pro 32-bit
 - HP-UX 11i V3 (IPF)
 - Solaris 11 (SPARC)
 - Red Hat(R) Enterprise Linux(R) Server 6 (64-bit x86_64)
 - Oracle Linux(R) Operating System 6 (x64)
 - CentOS 6 (x64)
 - CentOS 7
 - CentOS 8
- The following messages were deleted:
KAJP1023-E, KAJP1068-I, KAJP1801-I (Windows), KAJP1801-I (UNIX), KAJP1802-I (Windows), KAJP1802-I (UNIX), KAJP1803-E (Windows), KAJP1803-E (UNIX), KAJP1804-E, KAJP1805-E (Windows), KAJP1805-E (UNIX), KAJP1806-E (Windows), KAJP1806-E (UNIX), KAJP1807-E, KAJP1808-W, KAJP1810-E, KAJP1811-E, KAJP1812-W, KAJP1813-E, KAJP1814-E, KAJP1815-E, KAJP1816-W, KAJP1817-E, KAJP1820-E, KAJP1826-E, KAJP1830-E, KAJP1840-E, KAJP1841-W, KAJP1852-E, KAJP1860-I, KAJP1861-I, KAJP1863-E, KAJP1864-E, KAJP1869-E, KAJP1870-E, KAJP1871-I, KAVA2000-E, KAVA2101-E, KAVA2101-E, KAVA2102-

I, KAVA2103-I, KAVA2104-I, KAVA2105-W, KAVA2106-E, KAVA2107-E, KAVA2108-E, KAVA2109-E, KAVA2110-E, KAVA2111-W

- Changes were made to the action specified for the following message:
KAJP1004-E, KAJP1503-W, KAJP1508-E, KAVA1480-W, KAVA6694-W, KAVB2639-W, KAVB3186-W, KAVB3915-E, KNAM1095-W

(3) Changes in the manuals 3021-3-L11 and 3021-3-L11(E)

- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2022
 - Red Hat(R) Enterprise Linux(R) Server 9 (64-bit x86_64)
 - Oracle Linux(R) Operating System 9
- The following OSs were deleted from the supported OSs:
 - Windows(R) 10 Enterprise 32-bit
 - Windows(R) 10 Home 32-bit
 - Windows(R) 10 Pro 32-bit
 - HP-UX 11i V3 (IPF)
 - Solaris 11 (SPARC)
 - Red Hat(R) Enterprise Linux(R) Server 6 (64-bit x86_64)
 - Oracle Linux(R) Operating System 6 (x64)
 - CentOS 6 (x64)
 - CentOS 7
 - CentOS 8
- The following functions were removed:
 - JP1/SES compatibility function
 - SNMP trap conversion function
- The following compiler was added:
 - Visual C++(R) 2019
- Explanations on use in 2038 and later were added.

As a result, descriptions of the following items were changed or added:

- The coding example provided for issuing a startup event in the SAMPLE application was changed.
- 2038-compliant libraries and link options were added.
- A description on using the `JevGetArrivedTime()` function and `JevGetRegistTime()` function as functions returning a `time_t` type return value was added.
- 2038-compliant `JevGetArrivedTimeT()` and `JevGetRegistTimeT()` functions with equivalent functionality to the conventional `JevGetArrivedTime()` and `JevGetRegistTime()` functions were added.
- The start time was removed from the events handled in the sample source file.
- The code of the sample source file `sender.c` was changed.

N.2 Changes in 12-50#

#:

Includes corrections in the version 12-50 manuals.

(1) Changes in the manuals 3021-3-D65-20 and 3021-3-D65-20(E)

- Made changes so that, when the user attempts to uninstall JP1/Base while there is a product that requires JP1/Base installed, a message is output and the uninstallation is cancelled. Also added a function for forcibly uninstalling only JP1/Base and the procedure for restoration when uninstalling and then reinstalling only JP1/Base in order to downgrade or recover JP1/Base.
- The following commands that can set the log file size, number of log files, and buffer file size of the integrated trace log have been added.
 - `hntr2utl2` (UNIX only)
 - `hntr2utl2` (Windows only)
- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows(R) 7
 - Windows(R) 8
 - Windows(R) 8.1
 - Microsoft(R) Windows Server(R) 2012
 - Microsoft(R) Windows Server(R) 2012 R2
- Added description on the use of DHCP.
- `JP1_IOTDM_Admin` was added to the description of initial settings for permissions granted to JP1 users.
- Changed the procedure description provided for deleting a logical host in UNIX.
- Added a note on applying the common definition of logical hosts for the secondary node when changes are made to the communication settings in a cluster system (for `jp1host2` information).
- Changed the description provided in the notes on the `hntr2conf` command when changing the buffer file size or the type of exclusive control.
- In the notes on the `hntr2util` command (UNIX only and Windows only) and `hntr2utl2` command (UNIX only and Windows only), the description provided in the formula used to calculate the amount of log data and the procedure for changing the buffer file size were changed.
- Added notes on the `jbsgetcnf` and `jbssetcnf` commands.
- Added a note regarding event filter syntax on the formatting of condition statements.
- Changed the description of the amount of log data output (reference values) for the event service trace log.
- Added a note on the user permission level file.
- Partially changed the description on the timing for switching the command execution log files (ISAM) `ACTISAMLOGV8.DRF` and `CMDISAMLOGV8.DRF`.
- Changed the maximum disk space occupancy for the following logs:
 - Event service message settings change log
 - The *product-number* [`_{1|2|3|4|5}`] .LOG in the trace log for communication between log processes during installation

In addition, the maximum disk space occupancy and the file switching timing were changed for the following logs:

- Remote monitoring log (log-file trap)
- Remote monitoring log (event log trap)
- Meaning description was changed for the use of . * syntax in specifying regular expressions.

(2) Changes in the manuals 3021-3-D66-20 and 3021-3-D66-20(E)

- The following messages were added:
KAJP1621-E, KAVA1870-E, KAVA1871-E, KAVB3667-E
- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows(R) 7
 - Windows(R) 8
 - Windows(R) 8.1
 - Microsoft(R) Windows Server(R) 2012
 - Microsoft(R) Windows Server(R) 2012 R2

(3) Changes in the manuals 3021-3-D67-20 and 3021-3-D67-20(E)

- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows(R) 7
 - Windows(R) 8
 - Windows(R) 8.1
 - Microsoft(R) Windows Server(R) 2012
 - Microsoft(R) Windows Server(R) 2012 R2

N.3 Changes in 12-10

(1) Changes in the manuals 3021-3-D65-10 and 3021-3-D65-10(E)

- A password policy (defined in the password policy definition file) was set for authentication of JP1 users to strengthen security.
- Communication between a manager host and agent hosts can now be SSL-encrypted. Furthermore, users can now set whether to enable SSL-encrypted communication between the manager host and agent hosts.
In addition, users can now acquire SSL communication settings as operating information.
- An example of how to back up an event database for error reporting purposes was added.

(2) Changes in the manuals 3021-3-D66-10 and 3021-3-D66-10(E)

- The following messages were added:
KAJP1503-W to KAJP1510-W, KAVA1896-Q, KAVA1951-Q, KAVA5908-E, KAVA6694-W, KAVA6695-W, KAVA8241-E, KAVA8242-W, KAVA8243-W, KAVB3186-W, KAVB3187-W, KAVB3920-W, KNAM1095-W, KNAM1096-W
- Changes were made to the output message, description, and action specified for the following message:
KAVA1586-E, KAVA5033-E, KAVA5049-E, KAVA5133-E, KAVA5233-E, KAVA5333-E, KAVA5433-E

(3) Changes in the manuals 3021-3-D67-10 and 3021-3-D67-10(E)

No change was made.

N.4 Changes in 12-00

(1) Changes in the manuals 3021-3-D65 and 3021-3-D65(E)

- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows Server(R) 2008 R2
 - AIX V6.1
 - Solaris 10 (SPARC)
- The Hitachi Network Objectplaza Trace Library (HNTRLib2) for 64-bit version was added to the Windows Installer.
- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2019
 - SUSE Linux(R) Enterprise Server 15
- The initial setting of JP1 user password save format is changed to hash level 2 mode.

(2) Changes in the manuals 3021-3-D66 and 3021-3-D66(E)

- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows Server(R) 2008 R2
- The following messages were added:
KAJP1054-E, KAJP1055-E
- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2019
 - SUSE Linux(R) Enterprise Server 15

(3) Changes in the manuals 3021-3-D67 and 3021-3-D67(E)

- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows Server(R) 2008 R2
- Visual C++(R) 2015 and Visual C++(R) 2017 was added to the supported compilers.
- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2019
 - SUSE Linux(R) Enterprise Server 15

N.5 Changes in 11-50

(1) Changes in the manuals 3021-3-A01-20 and 3021-3-A01-20(E)

- User authentication functionality was enhanced to enable management of JP1 authentication information (JP1 user authentication information and JP1 operating permission) through linking with a directory server.
- Explanation was added for reviewing the communication timeout value to be applied to the execution of configuration distribution or configuration synchronization.
- The number of agent hosts that can be monitored by a manager host through using the remote-host monitoring of the health check function was expanded to 2,500.
- A note was added for the operation to use JP1/IM - Manager remote commands or automated actions in a large-scale system (1,024 or more agents).
- Explanation was added or modified for the elapsed time spent for automatically re-organizing the command execution log file.
- The `jbslistacl` command can now display operating permissions given to DS users and DS groups.
- The `jbsrmACL` command can now delete operating permissions from DS users or DS groups.
- The `jbssetacl` command can now register operating permissions for DS users and DS groups.
- The `jbsaclreload` command can now reload DS user's JP1 authentication information from a directory server.
- A note was added for operation to use a DS user.
- The `jbslistuser` command can now display the list of DS users.
- A note was added for the case to distribute configuration definition to many hosts at a time.
- A note was added for operation under system hierarchical configuration with three or more levels.
- The initial value of the number of the `jcocmddef` command records (`-record` option) was increased to 196,600.
- A note was added for the case to execute the `jevmessageid.bat` command after initiating Event Viewer.
- A file was added to define operating permission for the JP1 resource group of a JP1 user or a DS group.
- The communication timeout value can now be specified in the common definition settings file (configuration management functionality) for the execution of configuration distribution or configuration synchronization.
- The recommended value for the total number of attribute addition setting blocks defined in an additional extended attribute settings file was extended to 2,500 or less.
- It was expressly stated that a domain name can be also specified for the `SERVER` parameter in the directory server linkage definition file and the directory server modification file.
- The `AREC_EXCLUSIVE` parameter was added to the directory server linkage definition file and the directory server modification file.
- A note on the core dump file related ABRT settings (Linux only) was added.
- The model file for Active Directory schema extension was added to the list of files and folders of JP1/Base.
- Port numbers used for directory server linkage (for the operation to use a DS user) were added to those used for JP1/Base.
- Required system configuration for the operation linked with the auto-scaling functionality was expanded to those with 2,500 or fewer hosts including manager hosts.

(2) Changes in the manuals 3021-3-A02-20 and 3021-3-A02-20(E)

- The following messages were added:
KAVA1950-E, KAVA3421-W, KAVA3422-E, KAVA6656-E, KAVA8000-I, KAVA8001-W, KAVA8002-E, KAVA8003-E, KAVA8004-I, KAVA8010-E, KAVA8011-W, KAVA8012-W, KAVA8013-W, KAVA8014-W, KAVA8015-W, KAVA8016-W, KAVA8017-W, KAVA8020-W, KAVA8100-W, KAVA8101-W, KAVA8102-W, KAVA8103-W, KAVA8104-W, KAVA8105-W, KAVA8110-E, KAVA8111-W, KAVA8112-W, KAVA8113-W, KAVA8114-W, KAVA8115-E, KAVA8120-E, KAVA8121-W, KAVA8122-W, KAVA8123-W, KAVA8125-E, KAVA8130-E, KAVA8140-E, KAVA8144-W, KAVA8210-E, KAVA8212-E, KAVA8213-E, KAVA8220-E, KAVA8221-E, KAVA8222-E, KAVA8223-E, KAVA8230-E, KAVA8240-E, KAVB3173-W, KAVB3180-W, KAVB3181-W, KAVB3185-I
- The following messages were modified:
KAVA1662-E
- Changes were made to the output message, description, and action specified for the following message:
KAVA5901-E
- Changes were made to the action specified for the following messages:
KAVA6651-E, KAVA6678-E, KAVB2605-E
- A line was added to the output message specified for the following messages, and changes were made to the action specified for them:
KAVB3118-E, KAVB3119-E

(3) Changes in the manuals 3021-3-A03-20 and 3021-3-A03-20(E)

No change was made.

N.6 Changes in 11-10

(1) Changes in the manuals 3021-3-A01-10 and 3021-3-A01-10(E)

- The IM configuration management functionality for managing definition information can now be used with commands for collecting and distributing definitions for the event service.
- Microsoft(R) Windows Server(R) 2016 was added to the list of supported operating systems.
- The configuration definition information of agents for which changes have been made can now be updated without updating the information of agents for which no changes have been made.
- A message indicating the time spent on each monitoring operation can now be output when remote hosts are monitored by using the health check function.
- `JP1_Analytics_Admin` was added to the permissions that are granted to JP1 users at initial settings for user management.
- The setup information for the configuration management functionality was added to the collection target of the `jbsparamdump` command, which performs batch collection of JP1/Base setup information.
- The user can now choose not to display a confirmation message when the commands listed below are executed. In addition, the set of values that can be returned by these commands can now be expanded.
 - `jbsrt_del`
 - `jbsrt_distrib`

- `jbsrt_sync`
- Relative paths under `installation-folder\conf\` and `/etc/opt/jplbase/conf/` can now be used to specify the log file trap definition files to be distributed or collected.
- Log files in the multi-process trace format (HTRACE) that are output in UTF-8 Unicode in a Windows environment can now be monitored. (Log file trapping is now supported.)
- The `rep-restore` flag was added to the `options` parameter in the event server settings file.
- The `SKIP` option was added to the `START_OPT` parameter of the log-file trap startup definition file.
- The following JP1 events were added:
00001011
- The following information can now be collected by the data collection tool:
 - Routing information
 - Network interface status information
 - Information about the integrated trace log settings (file name, size, count, buffer file size, and monitoring interval)
 - `-ss nap` execution results (for Red Hat(R) Enterprise Linux(R) Server 7, Oracle Linux(R) Operating System 7, CentOS 7, and SUSE Linux(R) Enterprise Server 12)
- JP1/Base can now be linked with the auto-scaling functionality of the Amazon EC2 cloud platform.
- The log size for the remote commands log was increased.

(2) Changes in the manuals 3021-3-A02-10 and 3021-3-A02-10(E)

- Microsoft(R) Windows Server(R) 2016 was added to the list of supported operating systems.
- The following messages were added:
KAJP1096-I, KAJP1097-I, KAJP1098-E, KAJP1214-E, KAJP1501-I, KAJP1502-W, KAJP1611-I, KAJP1612-I, KAJP1613-E, KAJP1614-E, KAJP1615-E, KAVA1744-E, KAVA1868-E, KAVA3035-W, KAVA7239-I
- The output destinations of the following messages were changed:
KAVA3611-E
- The following messages were changed:
KAJP1136-E, KAJP1154-E, KAVA3410-W, KAVA3510-W, KAVA3646-E

(3) Changes in the manuals 3021-3-A03-10 and 3021-3-A03-10(E)

- Microsoft(R) Windows Server(R) 2016 was added to the list of supported operating systems.

N.7 Changes in 11-00

(1) Changes from the manuals 3021-3-001-20 and 3021-3-301-20(E)

- The following OSs were added to the supported OSs:
 - Windows(R) 10
 - Red Hat(R) Enterprise Linux(R) Server 7 (64-bit x86_64)
 - SUSE Linux(R) Enterprise Server 12
 - Oracle Linux(R) Operating System 6 (x64), Oracle Linux(R) Operating System 7

- CentOS 6 (x64), CentOS 7
- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows(R) XP Professional Operating System, Microsoft(R) Windows Server(R) 2003, Microsoft(R) Windows Server(R) 2003 R2, Microsoft(R) Windows Vista(R), Microsoft(R) Windows Server(R) 2008
 - Red Hat(R) Enterprise Linux(R) 5
- For the remote host monitoring of the health check function, the monitoring threshold and communication timeout can now be specified.
- Error details are now included in the messages that are output if the remote host monitoring of the health check function fails (KAVA7223-E and KAVA7229-W).
- A list of process names and function names that are displayed in messages output by the health check function was added.
- Log file trapping can now monitor log files whose size is 2 GB or larger.
- For JP1 event conversion by event log trapping, the event ID and trap name can now be specified.
- User-created extended attributes can now be added to JP1 events.
- The communication that is related to the authentication server (user authentication) and that is related to execution of JP1/IM commands can now be encrypted by SSL communication.
- The menu name displayed by selecting **Programs** and then **JP1_Base** from the Windows **Start** menu was changed.
- The following command was added:
 - `jevextreload`
 - `openssl`
- The size and monitoring interval time of the buffer file for the integrated trace log can now be changed by using the following commands:
 - `hntr2conf`
 - `hntr2util` (UNIX only)
 - `hntr2util` (Windows only)
- The default value of the `-t` option of the `jevsendd` command was changed.
- The following definition files were added:
 - Additional extended attribute settings file
 - SSL communication definition file
- The following parameters were added:
 - `THRESHOLD`, `TIMEOUT`, and `ERROR_DETAIL` parameters in the health check definition file
- The following parameters were deleted:
 - The `log-level` parameter in the event server settings file
 - The `trap-interval` and `jp1event-send` parameters in the action definition file for event log trapping (for Windows only)
 - The `imevt_regkind` parameter in the action definition file for converting SNMP traps
- The default values of the following parameters were changed:
 - The `retry-times` parameter in the action definition file for log file trapping

- The `retry-times` parameter in the action definition file for event log trapping (for Windows only)
- The following log file was added:
 - Installation log
- The sizes of the following log files were changed:
 - Log of the health check function (local host monitoring)
 - Log of the health check function (remote host monitoring)
 - Log of the health check commands
 - Log of the health check API
- Log of the command for deleting shared memory used by the health check function
- The following messages were added:
KAJP6024-I and KAJP6025-I

(2) Changes from the manuals 3021-3-002-20 and 3021-3-302-20(E)

- The following messages were added:
KAJP1078-E, KAJP1079-E, KAJP1080-E, KAJP1090-I, KAJP1091-E, KAJP1092-W, KAJP1093-E, KAJP1094-E, KAJP1095-E, KAJP6024-I, KAJP6025-I, KAVA1480-W, KAVA1481-W, KAVA1695-W, KAVA1697-E, KAVA1895-E, KAVA3675-E, KAVA3676-E, KAVA5903-W, KAVA5905-E, KAVA7237-W, KAVA7238-W, KAVB2639-W, KAVB2640-W, KAVB3915-E, KAVB3916-I, KAVB3917-I, KAVB3918-E, KAVB3919-E
- The following messages were changed:
KAJP1756-E, KAVA1524-W, KAVA1525-I, KAVA3003-E, KAVA3009-E, KAVA7030-E, KAVA7223-E, KAVA7229-W, KAVB3647-E

(3) Changes from the manuals 3021-3-003-20 and 3021-3-303-20(E)

- Now that the supported OSs were changed, the compiler for using functions provided by JP1/Base, as well as libraries, compile options, and link options required for the OSs were changed.

N.8 Changes in 10-50

(1) Changes in the manuals 3021-3-001-20, 3021-3-002-20, and 3021-3-003-20

- The following OSs were added to the supported OSs:
 - Windows(R) 8.1
 - Microsoft(R) Windows Server(R) 2012 R2
- The following functions were added to suppress forwarding of large numbers of events:
 - Event-forwarding suppression using an event-forwarding suppression command (`jevagt fw`)
 - Event-forwarding suppression using a threshold
- `HNP_Admin` was added to the permissions that are granted to JP1 users at initial settings for user management.
- Descriptions about the language type in the `LANG` environment variable for an automated startup script were added.
- Japanese UTF-8 is now supported as a language type in JP1/Base in HP-UX, Solaris, and AIX.

- Descriptions about the JP1 events to which local action execution conditions are applied were added.
- The `jbsgetcnf` command can now be used to collect definition information by specifying a component.
- Exclusive control can now be enabled or disabled when outputting to an integrated trace log.
- The `jbshostsimport` command can now be used to forcibly register the `jp1hosts` information in an environment where `jp1hosts2` information is specified.
Descriptions about the behavior when both `jp1hosts` information and `jp1hosts2` information are specified were also added.
- Remarks about event service communication settings were added.
- Remarks to be considered when log file trapping is used to monitor a Unicode file in Windows were added.
- The JP1/Base setup information can now be collected in a single operation.
- Remarks to be considered when the `jbsmkumap` and `jbssetumap` commands are used to register user mapping information in the common definition information were added.
- Remarks to be considered when the `jbssetcnf` command is used to change the JP1/AJS common definition information were added.
- In Windows, Unicode (UTF-8)-formatted log files are now supported for monitoring by log file trapping.
- The following JP1 events were added:
00003D05, 00003D06, 00003D07, 00003D08, 00003D09, 00003D0B, 00003D0C, 00003D0D, 00003D0E
- The extended attributes that are set to a JP1 event issued by the log file trapping function now include a monitor ID and monitor name.
- The following items were added to the information that can be collected by the data collection tool:
 - Assigning user rights
 - Group policy
 - Range of dynamic ports (IPV4)
 - Range of dynamic ports (IPV6)
 - Exclusive control of the integrated trace log
 - Output destination of the integrated trace log
- The number and size of the configuration management log files were changed.
- Descriptions about the parameters defined in the communication protocol settings file were added.
- Descriptions about the differences between the communication protocols of JP1/Base version 06-51 or earlier and JP1/Base version 06-71 or later were added.
- Descriptions about the communication protocols specified during cluster setup were added.
- Descriptions about the messages that are output when a request is denied by connection restriction were added.
- The following messages were added:
KAJP1083-W, KAJP1084-I, KAJP1085-I, KAJP1086-W, KAJP1087-W, KAJP1350-I, KAJP1351-I, KAJP1352-E, KAJP1401-I, KAJP1402-E, KAJP1403-E, KAJP1404-I, KAJP1405-I, KAJP1406-E, KAJP1407-E, KAJP1408-I, KAJP1410-I, KAJP1411-E, KAJP1413-I, KAJP1414-I, KAJP1415-E, KAJP1416-I, KAJP1417-I, KAJP1418-I, KAJP1419-I, KAJP1420-I, KAJP1421-I, KAJP1422-I, KAJP1423-E, KAJP1424-I, KAJP1425-E, KAJP1426-I, KAJP1427-I, KAJP1428-I, KAJP1429-I, KAJP1430-I, KAJP1431-I, KAJP1432-E, KAJP1433-I, KAJP1434-E, KAJP1435-E, KNAM9001-I, KNAM9002-I, KNAM9003-E, KNAM9004-E, KNAM9005-E, KNAM9006-E, KNAM9007-E, KNAM9008-E, KNAM9009-E, KNAM9010-E, KNAM9011-W, KNAM9012-I, KNAM9013-E, KNAM9014-E, KNAM9015-W, KNAM9016-W, KNAM9020-I, KNAM9021-E, KNAM9022-I, KNAM9023-E, KNAM9024-I, KNAM9025-E, KNAM9026-I, KNAM9027-E, KNAM9028-W

- The following messages were changed:
KAJP1033-E, KAVA0443-E, KAVA0590-E, KAVA0592-E, KAVA0678-E, KAVA0901-E, KAVA0906-E, KAVA3650-I, KAVA6726-E, KAVB2027-E, KAVB3098-E, KAVB3107-E, KNAM3130-E, KNAM3170-E
- Visual C++(R) 2012 was added to the supported compilers.

(2) Changes in the manuals 3021-3-301-20(E), 3021-3-302-20(E), and 3021-3-303-20(E)

- The following OSs were added to the supported OSs:
 - Windows(R) 8.1
 - Microsoft(R) Windows Server(R) 2012 R2
- The following functions were added to suppress forwarding of large numbers of events:
 - Event-forwarding suppression using an event-forwarding suppression command (`jevagtfw`)
 - Event-forwarding suppression using a threshold
- `HNP_Admin` was added to the permissions that are granted to JP1 users at initial settings for user management.
- Descriptions about the language type in the `LANG` environment variable for an automated startup script were added.
- Japanese UTF-8 is now supported as a language type in JP1/Base in HP-UX, Solaris, and AIX.
- Descriptions about the JP1 events to which local action execution conditions are applied were added.
- The `jbsgetcnf` command can now be used to collect definition information by specifying a component.
- Exclusive control can now be enabled or disabled when outputting to an integrated trace log.
- The `jbshostsimport` command can now be used to forcibly register the `jplhosts` information in an environment where `jplhosts2` information is specified.
Descriptions about the behavior when both `jplhosts` information and `jplhosts2` information are specified were also added.
- Remarks about event service communication settings were added.
- Remarks to be considered when log file trapping is used to monitor a Unicode file in Windows were added.
- The JP1/Base setup information can now be collected in a single operation.
- Remarks to be considered when the `jbsmkumap` and `jbssetumap` commands are used to register user mapping information in the common definition information were added.
- Remarks to be considered when the `jbssetcnf` command is used to change the JP1/AJS common definition information were added.
- In Windows, Unicode (UTF-8)-formatted log files are now supported for monitoring by log file trapping.
- The following JP1 events were added:
00003D05, 00003D06, 00003D07, 00003D08, 00003D09, 00003D0B, 00003D0C, 00003D0D, 00003D0E
- The extended attributes that are set to a JP1 event issued by the log file trapping function now include a monitor ID and monitor name.
- The following items were added to the information that can be collected by the data collection tool:
 - Assigning user rights
 - Group policy
 - Range of dynamic ports (IPV4)
 - Range of dynamic ports (IPV6)

- Exclusive control of the integrated trace log
- Output destination of the integrated trace log
- The number and size of the configuration management log files were changed.
- Descriptions about the parameters defined in the communication protocol settings file were added.
- Descriptions about the differences between the communication protocols of JP1/Base version 06-51 or earlier and JP1/Base version 06-71 or later were added.
- Descriptions about the communication protocols specified during cluster setup were added.
- Descriptions about the messages that are output when a request is denied by connection restriction were added.
- The following messages were added:
KAJP1083-W, KAJP1084-I, KAJP1085-I, KAJP1086-W, KAJP1087-W, KAJP1350-I, KAJP1351-I, KAJP1352-E, KAJP1401-I, KAJP1402-E, KAJP1403-E, KAJP1404-I, KAJP1405-I, KAJP1406-E, KAJP1407-E, KAJP1408-I, KAJP1410-I, KAJP1411-E, KAJP1413-I, KAJP1414-I, KAJP1415-E, KAJP1416-I, KAJP1417-I, KAJP1418-I, KAJP1419-I, KAJP1420-I, KAJP1421-I, KAJP1422-I, KAJP1423-E, KAJP1424-I, KAJP1425-E, KAJP1426-I, KAJP1427-I, KAJP1428-I, KAJP1429-I, KAJP1430-I, KAJP1431-I, KAJP1432-E, KAJP1433-I, KAJP1434-E, KAJP1435-E, KNAM9001-I, KNAM9002-I, KNAM9003-E, KNAM9004-E, KNAM9005-E, KNAM9006-E, KNAM9007-E, KNAM9008-E, KNAM9009-E, KNAM9010-E, KNAM9011-W, KNAM9012-I, KNAM9013-E, KNAM9014-E, KNAM9015-W, KNAM9016-W, KNAM9020-I, KNAM9021-E, KNAM9022-I, KNAM9023-E, KNAM9024-I, KNAM9025-E, KNAM9026-I, KNAM9027-E, KNAM9028-W
- The following messages were changed:
KAJP1033-E, KAVA0443-E, KAVA0590-E, KAVA0592-E, KAVA0678-E, KAVA0901-E, KAVA0906-E, KAVA3650-I, KAVA6726-E, KAVB2027-E, KAVB3098-E, KAVB3107-E, KNAM3130-E, KNAM3170-E
- Visual C++(R) 2012 was added to the supported compilers.

N.9 Changes in 10-10

(1) Changes in the manuals 3021-3-001-10, 3021-3-002-10, and 3021-3-003-10

- The following OSs were added to the supported OSs:
 - Windows(R) 8, Microsoft(R) Windows Server(R) 2012
 - Red Hat(R) Enterprise Linux(R) 5 (AMD/Intel 64), Red Hat(R) Enterprise Linux(R) 5 (x86)
 - Solaris 11 (SPARC)
- Descriptions about log file formats that cannot be monitored by log file trapping were added.
- Descriptions about the settings for duplicate communication protocols using IM configuration management were added.
- The following functions for login authentication linking with the directory server were extended:
 - All OUs (organization units) under the specified OU can now be linked to the directory server.
 - Attribute names other than CN can now be specified as the attribute name used for a JP1 user name.
- Descriptions about how to check the log file format specified by log file trapping were added.
- Commands (`jbschkds`, `jbsmkpass`, `jbspassmgr`, `jbsrmumappass`, and `jbsumappass`) and a definition file (password definition file) regarding the setting method and display format of the information-search user (which is necessary for the expanded directory server linkage function) were changed.

- Notes on the following command and definition file were added:
 - `jbsrt_distrib`
 - Action definition file for event log trapping (Windows only)
- A matching method based on Unicode search can now be specified, in order to prevent mismatching of regular expressions or garbled characters when event logs in Unicode format are monitored. Also, the code set used to register JP1 events has now changed to UTF-8.
- In Windows, logs output in Unicode (UTF-16) format can now be monitored by log file trapping.
- Connections from unintended hosts can now be restricted in order to securely operate a system running JP1/Base.
- Messages were added or modified.
- Now that Red Hat(R) Enterprise Linux(R) 5 was added to the supported OSs, gcc version 4.1.2 was added to the supported compilers.
- The `CODECONV` parameter was added to the common definition settings file for the local action function.

(2) Changes in the manuals 3021-3-301-10(E), 3021-3-302-10(E), and 3021-3-303-10(E)

- The following OSs were added to the supported OSs:
 - Windows(R) 8, Microsoft(R) Windows Server(R) 2012
 - Red Hat(R) Enterprise Linux(R) 5 (AMD/Intel 64), Red Hat(R) Enterprise Linux(R) 5 (x86)
 - Solaris 11 (SPARC)
- Descriptions about log file formats that cannot be monitored by log file trapping were added.
- Chinese was added to the language settings.
- Descriptions about the settings for duplicate communication protocols using IM configuration management were added.
- The following functions for login authentication linking with the directory server were extended:
 - All OUs (organization units) under the specified OU can now be linked to the directory server.
 - Attribute names other than CN can now be specified as the attribute name used for a JP1 user name.
- Descriptions about how to check the log file format specified by log file trapping were added.
- Commands (`jbschkds`, `jbsmkpass`, `jbspassmgr`, `jbsrmumappass`, and `jbsumappass`) and a definition file (password definition file) regarding the setting method and display format of the information-search user (which is necessary for the expanded directory server linkage function) were changed.
- Notes on the following command and definition file were added:
 - `jbsrt_distrib`
 - Action definition file for event log trapping (Windows only)
- A matching method based on Unicode search can now be specified, in order to prevent mismatching of regular expressions or garbled characters when event logs in Unicode format are monitored. Also, the code set used to register JP1 events has now changed to UTF-8.
- In Windows, logs output in Unicode (UTF-16) format can now be monitored by log file trapping.
- Connections from unintended hosts can now be restricted in order to securely operate a system running JP1/Base.
- Messages were added or modified.

- Now that Red Hat(R) Enterprise Linux(R) 5 was added to the supported OSs, gcc version 4.1.2 was added to the supported compilers.
- The CODECONV parameter was added to the common definition settings file for the local action function.

N.10 Changes in 10-00

(1) Changes in the manuals 3021-3-001-10, 3021-3-002-10, and 3021-3-003-10

- Support for the following OSs was added:
 - Microsoft(R) Windows(R) 7 Enterprise
 - Microsoft(R) Windows(R) 7 Professional
 - Microsoft(R) Windows(R) 7 Ultimate
 - Microsoft(R) Windows Server(R) 2003, Datacenter Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
 - Microsoft(R) Windows Server(R) 2008 Datacenter
 - Microsoft(R) Windows Server(R) 2008 R2 Datacenter
 - Microsoft(R) Windows Server(R) 2008 R2 Enterprise
 - Microsoft(R) Windows Server(R) 2008 R2 Standard
 - AIX V7.1
 - Red Hat(R) Enterprise Linux(R) 6 (AMD/Intel 64)
 - Red Hat(R) Enterprise Linux(R) 6 (x86)
- The following OSs are no longer supported:
 - AIX 5L V5.3
 - HP-UX 11i V2 (IPF)
 - Solaris 9 (SPARC)
- A description of language type settings was added.
- `jp1hosts2` information can now be used as JP1-specific hosts information
- JP1/Base can now use IPv6 addresses to communicate.
- Users with JP1/Base administrator privileges can now use JP1/Base.
- The event log trapping function now supports event types added in Windows Vista and Windows Server 2008.
- Log file traps can now monitor log files in SEQ3 and UPD format.
- Log file traps can now be started using a log-file trap startup definition file.

- The description of log files that cannot be monitored by a log file trap now includes files in which log information is always recorded at the beginning.
- Log file traps in HP-UX, Solaris, and AIX can now monitor log information output in UTF-8 encoding.
- The definitions in the log-file trap startup definition file can now be collected and distributed by the event service.
- Users can now select whether to monitor the starting and stopping of monitored hosts when using the health check function to monitor a remote host. Accordingly, the following changes were made:
- The `STOP_CHECK` parameter was added to the health check definition file.
- The `auto-forward-off` flag was added to the options parameter of the event server settings file. The occurrence conditions for JP1 event 0000474A were also added.
- Descriptions of the IP address used in an environment with multiple LAN connections were added and changed.
- A cautionary note was added regarding setting the installation folder when installing JP1/Base in an x64 environment.
- A description of the default location and permission settings of the JP1/Base installation folder was added.
- `JP1_ITSLM_Admin` and `Cosminexus_vMNG_Admin` were added as default permissions for JP1 users in the description of the user management function.
- To enhance password security, a way to change the password save method was added.
- A description of how to update the common definition information was added.
- A cautionary note about registering JP1/Base services with cluster software was added.
- Descriptions of situations where communication settings need to be changed, and the definition files to use to make those changes have been added and changed.
- Changes were made to the communication protocol settings file specified when executing the `jbssetcnf` command.
- A cautionary note about stopping the event service was added.
- A procedure for temporarily changing the linked directory server was added.
- The tasks required when changing the IP of a computer running JP1/Base were changed.
- A command for checking the status of the log-file trap management service (daemon) was added.
- A procedure for suppressing the messages output when you execute the `jbs_start.cluster` command was added.
- The return values of the following commands were amended:
`jbsadduser`, `jbschgpasswd`, `jbslistuser`, `jevexport`, `jevlogreload`
- The `-s` option was added to the `jevdef_distrib` command, allowing for distribution of the definition information in the log-file trap startup definition file.
- The `-s` option was added to the `jevdef_get` command, allowing definition information to be collected from the log-file trap startup definition file. The `-r` option was also added to allow definition information to be collected for specific hosts.
- The `-x` option was added to the `jevlogstart` command, allowing the output source host name for log data to be set in the `JP1_SOURCEHOST` extended attribute when converting log entries to JP1 events. Also, the specification of the `-s` option was made case sensitive.
- Errors in the format of the `jbs_setup_cluster` (Windows only) command were corrected.
- Cautionary notes were added for the following commands:
`jbsrt_distrib` command, `jevexport` command
- The description of the `-r` option of the `jevlogstart` command was changed.

- A cautionary note about specifying batch file names that contain spaces in parameters of the start sequence definition file was added.
- The instruction not to insert a space or any other characters in front of a parameter name at the start of a line now mentions hash marks (#) (code 0x23).
- A cautionary note was added regarding the client-bind parameter of the event server settings file, about situations where multiple addresses are specified.
- A cautionary note has been added about log types in Windows Vista and Windows Server 2008.
- The log-file trap startup definition file has been added as a distribution definition file.
- The description of the *@action-definition-file-name* parameter in the section about distribution definition files was changed.
- The format of the directory server linkage definition file (Windows only) was amended.
- The following JP1 events were added:
00003A25, 00003A26, 00003A27, 00003A28, 00003A29, 00003A2A, 00003A30, 00003A31, 00003A32,
00004724, 00004725, 0000474C, 0000474D
- The PP name of JP1 event 00003A71 is now different depending on whether a remote monitoring event log trap or a JP1/Base event log trap generated the event.
- The PP name of JP1 events whose ID is the value specified in the ACTDEF parameter of the action definition file is now different depending on whether a remote monitoring log file trap or a JP1/Base log file trap generated the event.
- The format of the ACTDEF parameter in the action definition file for log file trapping was amended.
- There is now more information to be collected when troubleshooting errors.
- The *jbs_setup_cluster* (Windows only) can now not be executed while JP1/Base is running.
- Data is now output to additional log files during installation.
- Remote monitoring logs were added to log file traps and event log traps.
- The file name of the trace log for the *jbs_killall.cluster* command was changed.
- The number of *jbscomd_api.exe* processes was amended.
- *jelallog* was added to the list of UNIX processes.
- The direction in which *jp1bscom* data passes through the firewall was added.
- A note about V5 compatibility in Windows Server 2008 was added to the cautionary notes regarding JP1/SES events.
- The procedure for outputting data to operations logs was changed.
- Messages were added, changed, and deleted.
- Compatible compilers were added, changed, and deleted.

(2) Changes in the manuals 3021-3-301(E), 3021-3-302(E), and 3021-3-303(E)

- Support for the following OSs was added:
 - Microsoft(R) Windows(R) 7 Enterprise
 - Microsoft(R) Windows(R) 7 Professional
 - Microsoft(R) Windows(R) 7 Ultimate
 - Microsoft(R) Windows Server(R) 2003, Datacenter Edition
 - Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition

- Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
- Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
- Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition
- Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
- Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
- Microsoft(R) Windows Server(R) 2008 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise
- Microsoft(R) Windows Server(R) 2008 R2 Standard
- AIX V7.1
- Red Hat(R) Enterprise Linux(R) 6 (AMD/Intel 64)
- Red Hat(R) Enterprise Linux(R) 6 (x86)
- The following OSs are no longer supported:
 - AIX 5L V5.3
 - HP-UX 11i V2 (IPF)
 - Solaris 9 (SPARC)
- A description of language type settings was added.
- `jp1hosts2` information can now be used as JP1-specific hosts information
- JP1/Base can now use IPv6 addresses to communicate.
- Users with JP1/Base administrator privileges can now use JP1/Base.
- The event log trapping function now supports event types added in Windows Vista and Windows Server 2008.
- Log file traps can now monitor log files in SEQ3 and UPD format.
- Log file traps can now be started using a log-file trap startup definition file.
- The description of log files that cannot be monitored by a log file trap now includes files in which log information is always recorded at the beginning.
- Log file traps in HP-UX, Solaris, and AIX can now monitor log information output in UTF-8 encoding.
- The definitions in the log-file trap startup definition file can now be collected and distributed by the event service.
- Users can now select whether to monitor the starting and stopping of monitored hosts when using the health check function to monitor a remote host. Accordingly, the following changes were made:
 - The `STOP_CHECK` parameter was added to the health check definition file.
 - The `auto-forward-off` flag was added to the options parameter of the event server settings file.
- The occurrence conditions for JP1 event 0000474A were also added.
- Descriptions of the IP address used in an environment with multiple LAN connections were added and changed.
- A cautionary note was added regarding setting the installation folder when installing JP1/Base in an x64 environment.
- A description of the default location and permission settings of the JP1/Base installation folder was added.
- `JP1_ITSLM_Admin` and `Cosminexus_vMNG_Admin` were added as default permissions for JP1 users in the description of the user management function.
- To enhance password security, a way to change the password save method was added.

- A description of how to update the common definition information was added.
- A cautionary note about registering JP1/Base services with cluster software was added.
- Descriptions of situations where communication settings need to be changed, and the definition files to use to make those changes have been added and changed.
- Changes were made to the communication protocol settings file specified when executing the `jbssetcnf` command.
- A cautionary note about stopping the event service was added.
- A procedure for temporarily changing the linked directory server was added.
- The tasks required when changing the IP of a computer running JP1/Base were changed.
- A command for checking the status of the log-file trap management service (daemon) was added.
- A procedure for suppressing the messages output when you execute the `jbs_start.cluster` command was added.
- The return values of the following commands were amended:
`jbsadduser, jbschgpasswd, jbslistuser, jevexport, jevlogreload`
- The `-s` option was added to the `jevdef_distrib` command, allowing for distribution of the definition information in the log-file trap startup definition file.
- The `-s` option was added to the `jevdef_get` command, allowing definition information to be collected from the log-file trap startup definition file. The `-r` option was also added to allow definition information to be collected for specific hosts.
- The `-x` option was added to the `jevlogstart` command, allowing the output source host name for log data to be set in the `JP1_SOURCEHOST` extended attribute when converting log entries to JP1 events. Also, the specification of the `-s` option was made case sensitive.
- Errors in the format of the `jbs_setup_cluster` (Windows only) command were corrected.
- Cautionary notes were added for the following commands:
`jbsrt_distrib` command, `jevexport` command
- The description of the `-r` option of the `jevlogstart` command was changed.
- A cautionary note about specifying batch file names that contain spaces in parameters of the start sequence definition file was added.
- The instruction not to insert a space or any other characters in front of a parameter name at the start of a line now mentions hash marks (`#`) (code `0x23`).
- A cautionary note was added regarding the `client-bind` parameter of the event server settings file, about situations where multiple addresses are specified.
- A cautionary note has been added about log types in Windows Vista and Windows Server 2008.
- The log-file trap startup definition file has been added as a distribution definition file.
- The description of the `@action-definition-file-name` parameter in the section about distribution definition files was changed.
- The format of the directory server linkage definition file (Windows only) was amended.
- The following JP1 events were added:
`00003A25, 00003A26, 00003A27, 00003A28, 00003A29, 00003A2A, 00003A30, 00003A31, 00003A32, 00004724, 00004725, 0000474C, 0000474D`
- The PP name of JP1 event `00003A71` is now different depending on whether a remote monitoring event log trap or a JP1/Base event log trap generated the event.

- The PP name of JP1 events whose ID is the value specified in the ACTDEF parameter of the action definition file is now different depending on whether a remote monitoring log file trap or a JP1/Base log file trap generated the event.
- The format of the ACTDEF parameter in the action definition file for log file trapping was amended.
- There is now more information to be collected when troubleshooting errors.
- The `jbs_setup_cluster` (Windows only) can now not be executed while JP1/Base is running.
- Data is now output to additional log files during installation.
- Remote monitoring logs were added to log file traps and event log traps.
- The file name of the trace log for the `jbs_killall_cluster` command was changed.
- The number of `jbscomd_api.exe` processes was amended.
- `jelallog` was added to the list of UNIX processes.
- The direction in which `jp1bscom` data passes through the firewall was added.
- A note about V5 compatibility in Windows Server 2008 was added to the cautionary notes regarding JP1/SES events.
- The procedure for outputting data to operations logs was changed.
- Messages were added, changed, and deleted.
- Compatible compilers were added, changed, and deleted.

N.11 Changes in 09-00

(1) Changes in the manuals 3021-3-R71(E), 3021-3-R72(E), and 3021-3-R73(E)

- 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 `jisininfo` 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`, `Jismlocktr`, `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.

O. Reference Material for this Manual

This appendix provides reference material for readers of this manual.

O.1 Related publications

The related manuals of this manual are listed below. Refer to these manuals when necessary.

JP1/Base manuals

- JP1 Version 13 JP1/Base User's Guide (3021-3-L09(E))
- JP1 Version 13 JP1/Base Messages (3021-3-L10(E))
- JP1 Version 13 JP1/Base Function Reference (3021-3-L11(E))

JP1/IM manuals

- JP1 Version 13 Integrated Management: Getting Started (3021-3-L01(E))
- JP1 Version 13 JP1/Integrated Management 3 - Manager Overview and System Design Guide (3021-3-L02(E))
- JP1 Version 13 JP1/Integrated Management 3 - Manager Configuration Guide (3021-3-L03(E))
- JP1 Version 13 JP1/Integrated Management 3 - Manager Administration Guide (3021-3-L04(E))
- JP1 Version 13 JP1/Integrated Management 3 - Manager GUI Reference (3021-3-L05(E))
- JP1 Version 13 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference (3021-3-L06(E))
- JP1 Version 13 JP1/Integrated Management 3 - Manager Messages (3021-3-L07(E))
- Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide (3020-3-K10(E))
- Job Management Partner 1/Integrated Management - Rule Operation GUI Reference (3020-3-K11(E))

JP1/AJS manuals

- JP1 Version 13 Job Management: Getting Started (Job Scheduler) (3021-3-L41(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Overview (3021-3-L42(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 System Design (Configuration) Guide (3021-3-L43(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide (3021-3-L44(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Configuration Guide (3021-3-L45(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Administration Guide (3021-3-L46(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Troubleshooting (3021-3-L47(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Operator's Guide (3021-3-L48(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Command Reference (3021-3-L49(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Linkage Guide (3021-3-L50(E))
- JP1 Version 13 JP1/Automatic Job Management System 3 Messages (3021-3-L51(E))

Other manuals

- JP1 Version 12 JP1/SNMP System Observer Description, Operator's Guide and Reference (3021-3-E04(E))

- Job Management Partner 1/Software Distribution Description and Planning Guide (For Windows Systems) (3020-3-S79(E))
- Job Management Partner 1/Software Distribution Setup Guide (For Windows Systems) (3020-3-S80(E))
- Job Management Partner 1/Software Distribution Administrator's Guide Volume 1 (For Windows Systems) (3020-3-S81(E))
- Job Management Partner 1/Software Distribution Administrator's Guide Volume 2 (For Windows Systems) (3020-3-S82(E))
- Job Management Partner 1/Software Distribution Client Description and User's Guide (For UNIX Systems) (3020-3-S85(E))
- Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide (For UNIX Systems) (3020-3-L42(E))
- Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide (3000-3-841(E))

O.2 Abbreviations

This manual uses the following abbreviations for product names:

Abbreviation		Full name	
AIX		AIX V7.2	
		AIX V7.3	
HNTRLib2		Hitachi Network Objectplaza Trace Library 2	
JP1/AJS	JP1/AJS	Job Management Partner 1/Automatic Job Scheduler	
	JP1/AJS - Agent	JP1/AJS3 - Agent	JP1/Automatic Job Management System 3 - Agent
		JP1/AJS3 - Agent Minimal Edition	JP1/Automatic Job Management System 3 - Agent Minimal Edition
	JP1/AJS - Manager	JP1/AJS3 - Manager	JP1/Automatic Job Management System 3 - Manager
	JP1/AJS - View	JP1/AJS3 - View	JP1/Automatic Job Management System 3 - View
	JP1/AJS3 - WOA		JP1/Automatic Job Management System 3 - Web Operation Assistant
JP1/AOM		JP1/Automatic Operation Monitor	
JP1/Audit		JP1/Audit Management - Manager [#]	
JP1/IM	JP1/IM - EG	JP1/Integrated Management - Event Gateway for Network Node Manager i (version 9 or later) [#]	
		JP1/Integrated Management 2 - Event Gateway for Network Node Manager i	
		JP1/Integrated Management 3 - Event Gateway for Network Node Manager i	
	JP1/IM2 - EG	JP1/Integrated Management 2 - Event Gateway for Network Node Manager i	
		JP1/Integrated Management 3 - Event Gateway for Network Node Manager i	
		JP1/Integrated Management 3 - Event Gateway for Network Node Manager i	

Abbreviation		Full name
	JP1/IM - Manager	JP1/Integrated Management - Manager
		JP1/Integrated Management 2 - Manager
		JP1/Integrated Management 3 - Manager
	JP1/IM2 - Manager	JP1/Integrated Management 2 - Manager
		JP1/Integrated Management 3 - Manager
	JP1/IM - Rule Operation	Job Management Partner 1/Integrated Management - Rule Operation
	JP1/IM - View	JP1/Integrated Management - View
		JP1/Integrated Management 2 - View
		JP1/Integrated Management 3 - View
	JP1/IM2 - View	JP1/Integrated Management 2 - View
		JP1/Integrated Management 3 - View
	JP1/IM - Planning Operation	
JP1/Navigation Platform		JP1/Navigation Platform [#]
JP1/NETM/DM	JP1/NETM/DM Client	JP1/NETM/DM Client
		JP1/NETM/DM Client - Base
	JP1/NETM/DM Manager	JP1/NETM/DM Manager
JP1/Power Monitor		JP1/Power Monitor
Linux	Oracle Linux 7	Oracle Linux(R) Operating System 7
	Oracle Linux 8	Oracle Linux(R) Operating System 8
	Oracle Linux 9	Oracle Linux(R) Operating System 9
	Linux 7	Red Hat Enterprise Linux(R) Server 7 (64-bit x86_64)
	Linux 8	Red Hat Enterprise Linux(R) Server 8 (64-bit x86_64)
	Linux 9	Red Hat Enterprise Linux(R) Server 9 (64-bit x86_64)
	SUSE Linux 12	SUSE Linux(R) Enterprise Server 12
	SUSE Linux 15	SUSE Linux(R) Enterprise Server 15

[#]: This product operates in a Japanese environment only.

AIX and Linux are sometimes referred to collectively as *UNIX*.

Names appear in abbreviated form in messages and other information output by program products.

O.3 Acronyms

This manual uses the following acronyms:

Acronym	Meaning
AMD	Advanced Micro Devices

Acronym	Meaning
API	Application Programming Interface
CA	Certificate Authority
CN	Common Name
CSR	Certificate Signing Request
CSV	Comma Separated Value
DB	Database
DN	Distinguished Name
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
TLS	Transport Layer Security
UTC	Universal Time Coordinated
UTF	UCS Transformation Format
WWW	World Wide Web

Acronym	Meaning
VPN	Virtual Private Network

O.4 Conventions for KB (kilobytes) and other units

1 KB (kilobyte), 1 MB (megabyte), 1 GB (gigabyte), and 1 TB (terabyte) are equivalent to $1,024$ bytes, $1,024^2$ bytes, $1,024^3$ bytes, and $1,024^4$ bytes respectively.

P. Glossary

A

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.

B

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.

C

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.

D

directory server

A server that provides services required to centrally manage various resources on the network and their respective attributes.

DS group

A security group of the Active Directory to which JP1 operating permission is assigned. JP1 operating permission can be easily assigned because assigning JP1 operating permission to a security group also gives JP1 operating permission to accounts to belong to the security group.

DS user

A JP1 user on which user authentication is performed through linking with a directory server. JP1 authentication information (JP1 user authentication information and JP1 operating permission) is managed on the directory server.

E

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.

F

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*.

I

information-search user

A user who can search for the users linked to a directory server on the directory server. An information-search user is a directory server user who has view permission for the search-origin container object and the underlying container objects.

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.)

J

JP1/AJS

A program for running jobs automatically. You can execute a sequence of processes according to a predefined schedule, or initiate processing when a specific event occurs.

JP1 administrators group

A user group that allows users other than the system administrator (users with superuser permission) to operate JP1/Base. Permission to operate JP1/Base is granted to OS users whose primary group is the JP1 administrators group.

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/Base administrator

A user who has been given permission to operate JP1/Base. In a UNIX environment, a JP1/Base administrator is an OS user whose primary group is the JP1 administrators group. Enable this feature when you want OS users other than those with JP1/Base system administrator permission to be able to use JP1/Base.

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 information

JP1-specific hosts information. 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.

jp1hosts2 information

JP1-specific hosts information. `jp1hosts2` information allows JP1/Base to resolve multiple IP addresses from one host name, even in environments where the operating system can only resolve one IP address from a given host name. `jp1hosts2` information takes effect when registered on a host.

JP1/IM - Manager

JP1/IM - Manager (JP1/Integrated Management 3 - 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: *central console* and *central 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 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.

JP1 users can be classified into the following JP1 user types according to their method of user authentication:

- Standard user
- DS user

- Linked user

K

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.

L

large numbers of events

Many unexpected JP1 events that occur over a short period.

linked user

A JP1 user on which user authentication is performed through linking with a directory server. Only JP1 user authentication information of JP1 authentication information (JP1 user authentication information and JP1 operating permission) is 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.

M

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

N

NNM

A generic name for the integrated network management programs designed for network configuration, performance, and trouble management.

node switching system

See *cluster system*.

O

operating information

Definition information loaded by JP1/Base services. This information can be used to check the currently valid definition for JP1/Base.

P

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.

R

regular expression

A list of characters and special characters corresponding to one or more specific text strings.

S

secondary authentication server

One of two authentication servers installed in a single user authentication block. The secondary authentication server is used as a backup.

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. JP1 authentication information (JP1 user authentication information and JP1 operating permission) is managed by the authentication server.

U

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.

V

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

A

- action definition file (log file trapping)
 - distributing definitions 379
- action definition file (ntevent.conf)
 - collecting definitions 377
 - distributing definitions 379
- action definition file for event log trapping 371, 721
- action definition file for log file trapping 703
 - collecting definitions 377
- adding hosts to the monitoring target during scale out 961
- additional extended attribute settings files 697
- "Administrator permissions" as used in this manual 9
- agent
 - glossary 1010
- ANY binding method 104
 - glossary 1010
- api (API settings file) 693
- API settings file 693
- authentication server
 - after setting 296
 - blocked status 39
 - example measures for enhancing reliability of 37
 - glossary 1010
 - setting by command (Windows) 295
 - setting up by using GUI (in Windows) 294
 - specifying (UNIX) 328
 - specifying (Windows) 294
- authentication server 33
- authentication servers
 - example measures for enhancing reliability of 37
- automatic setup (UNIX) 125
- automatic setup (Windows) 114
- automatic startup
 - event log trapping function 372
 - log file trap 367
 - setting (UNIX only) 288
- automatic stop (UNIX only) 288
- auto-scaling linkage script 968

B

- backup
 - common definition information (UNIX) 155
 - common definition information (Windows) 148

- definition files (UNIX) 153
- definition files (Windows) 146
- event database (UNIX) 156
- event database (Windows) 149
- jp1hosts2 information (UNIX) 156
- jp1hosts2 information (Windows) 149
- target JP1/Base files (UNIX) 153
- target JP1/Base files (Windows) 146
- basic attribute 800
 - glossary 1010
- blocked status
 - checking (command) 336
 - checking (GUI) 335
 - glossary 1010
 - of authentication server 39
 - releasing (command) 336
 - releasing (GUI) 335
 - setting (command) 336
 - setting (GUI) 335

C

- changing
 - host name 391
 - language (UNIX only) 216
 - system time 393
- character code compatibility mode 137
- client
 - glossary 1010
- cluster ID 717
- cluster system 103
 - glossary 1010
 - overview 176
 - primary server 176
 - secondary server 176
- cluster system use
 - changing language (UNIX only) 216
 - JP1/Base functions 182
 - notes 214
 - overview 177
 - prerequisites 178
 - registering daemon (UNIX) 204
 - registering service (Windows) 196
 - restarting JP1 206
 - setting environment (UNIX) 199

- setting environment (Windows) 188
- setup (UNIX) 201
- setup (Windows) 189
- tasks after changing settings 207
- collecting
 - definitions 28
 - definitions of JP1 programs 87
 - JP1/Base setup information in single operation 401
- collecting data
 - in UNIX 863
 - in Windows 859
- collection information file 788
- command execution log
 - directory (UNIX) 898
 - directory (Windows) 886
- command execution triggered by JP1 event 100
- commands 395
 - checking network setup 396
 - collecting JP1/Base setup information in single operation 401
 - common definition information 401
 - communication encryption 402
 - configuration definition 401
 - event service 399
 - ISAM file operation and maintenance 400
 - jbsrt_del 504
 - jbsrt_distrib 506
 - jbsrt_get 510
 - jbsrt_sync 512
 - jcocmdddef 532
 - jcocmddel 539
 - jcocmdlog 541
 - jcocmdshow 544
 - JP1-specific hosts information 401
 - list 396
 - local actions, automated actions, and command execution 402
 - starting, stopping, and setting up 396
 - startup control 396
 - troubleshooting 401
 - upgrading 397
 - user management 397
- common definition information
 - backup (UNIX) 155
 - backup (Windows) 148
 - command 401
 - glossary 1011
- recovery (UNIX) 157
- recovery (Windows) 150
- common definition settings file (configuration management functionality) 790
- common definition settings file (health check function) 758
- common definition settings file (local action function) 786
- common message log 845
- communication encryption function of JP1/Base
 - setting up 281
- communication encryption in JP1/Base 276
- communication protocol
 - setting 228
- communication protocols 104
 - ANY binding method 104
 - IP binding method 105
- communication settings 223
 - changing 928
 - necessity of 273
 - resetting JP1/Base to single network 266
- compatibility 110
- conf (event server settings file) 347, 673
- configuration definition
 - glossary 1011
- Configuration definition file 792
- configuring Amazon EC2 service 967
- confirming startup (UNIX) 291
- confirming startup (Windows) 286
- connection
 - restricting unintended hosts 954
- connection status 912
- controlling startup of services 28
- conventions
 - "Administrator permissions" as used in this manual 9
 - directory names 9
 - fonts and symbols 9
 - JP1/Base installation folder 11
 - syntax 10
 - version numbers 11
- converting
 - application program log files 53
 - event log data into JP1 events 53
 - events 28
 - log messages into JP1 events 53
 - cpysvprm (Windows only) 404

D

- data collection tool 849
- definition files
 - action definition file for event log trapping (Windows only) 721
 - action definition file for log file trapping 703
 - additional extended attribute settings files 697
 - API settings file 693
 - collection information file 788
 - common definition settings file (health check function) 758
 - common definition settings file (local action function) 786
 - Configuration definition file 792
 - directory server linkage definition file (Windows only) 744
 - directory server modification file (Windows only) 742
 - distribution definition file 731
 - environment variable file 795
 - event server index file 669
 - event server settings file 672
 - extended startup process definition file 762
 - forwarding settings file 687
 - health check definition file 754
 - host access control definition file 771
 - host group definition file 797
 - JP1/Base parameter definition file 760
 - jp1hosts 766
 - jp1hosts2 definition file 768
 - list 645
 - local action environment variable file 780
 - local action execution definition file 781
 - log-file trap startup definition file 714
 - log information definition file 719
 - Non-SSL communication host configuration file 777
 - password definition file (Windows only) 736
 - password policy definition file 751
 - service startup delay time / timer monitoring period definition file (Windows only) 667
 - SSL communication definition file 773
 - start sequence definition file (Windows) 661
 - user mapping definition file 749
 - User permission definition file 740
 - user permission level files 738
- definition files required for each operational case 648
- definitions
 - collecting 28

- distributing 28
 - of JP1 programs, collecting 87
- details of JP1/Base Functions 32
- detecting process hangup and abnormal termination 89
- directories list 879
- directory name conventions 9
- directory server 30
 - glossary 1011
 - specifying 316
- directory server linkage 40
 - notes 315
 - setting up 313
- directory server linkage definition file 744
- directory server modification file 742
- disk space requirements
 - shared disk 918
 - UNIX 918
 - Windows 918
- distribution definition file 731
- DS user 41
 - glossary 1011
- duplicate communication 232

E

- environment variable file 795
- environment variables
 - JP1_HOSTNAME 179
 - LANG 135
- event database 48
 - backup (UNIX) 156
 - backup (Windows) 149
 - capacity 677
 - CSV output 356
 - initializing 354
 - recovery (UNIX) 158
 - recovery (Windows) 151
- event filter
 - setting example 658
- event ID
 - 00001011 details 807
 - 00003A10 details 812
 - 00003A20 details 813
 - 00003A21 details 814
 - 00003A22 details 815
 - 00003A25 details 816
 - 00003A26 details 816
 - 00003A27 details 817

00003A28 details 818
 00003A29 details 819
 00003A2A details 820
 00003A30 details 821
 00003A31 details 822
 00003A32 details 823
 00003A71 details 824
 00003D00 details 807
 00003D04 details 807
 00003D05 details 808
 00003D06 details 808
 00003D07 details 809
 00003D08 details 809
 00003D09 details 810
 00003D0B details 810
 00003D0C details 811
 00003D0D details 811
 00003D0E details 812
 00003FA0 details 827
 00003FA1 details 827
 00003FA2 details 828
 00003FA3 details 828
 00003FA5 details 829
 00003FA6 details 829
 00003FA7 details 830
 00004700 details 830
 00004701 details 831
 00004702 details 831
 00004720 details 831
 00004721 details 832
 00004722 details 832
 00004724 details 832
 00004725 details 833
 00004740 details 833
 00004741 details 834
 00004742 details 834
 00004743 details 835
 00004747 details 835
 00004748 details 835
 00004749 details 836
 0000474A details 836
 0000474B details 837
 0000474C details 837
 0000474D details 837
 0000474E details 838
 0000474F details 838
 00004750 details 839
 00004780 details 839
 00004781 details 840
 00004782 details 841
 00004783 details 842
 event ID specified in filter of action definition file for event log trapping, details about 824
 event IDs specified in ACTDEF parameter in action definition file for log file trapping, details about 826
 glossary 1011
 event log trapping 28
 glossary 1012
 event log trapping function 1012
 cluster system use 185
 monitoring end timing 68
 monitoring interval 68
 monitoring start timing 68
 reattempting to connect to event service 68
 starting 371
 stopping 372
 events
 handling 28
 JP1 events acquired by JP1/Base 51
 large numbers of 69
 event server
 glossary 1012
 event server index file 669
 event server index file (index) 346
 event server settings file 672
 event server settings file (conf) 347
 event server setup for DNS services 351
 event service 48
 changing communication settings 244, 249
 collecting definitions 377
 command 399
 distributing definitions 379
 event server setup for DNS services 351
 glossary 1012
 initializing an event database while active 354
 initializing an event database while stopped 354
 notes 361
 setup tasks 345
 event service definitions
 collecting 377
 distributing 379
 event service functionality 48
 extended attribute 801
 glossary 1012

extended regular expressions 920
extended startup process definition file 762

F

failover 176
 glossary 1012
files list 879
firewall
 collecting and distributing definitions 87
 traffic direction 911
font conventions 9
forced termination 341
forward (forwarding settings file) 687
 collecting definitions 377
 distributing definitions 379
forwarding settings file 687
forwarding settings file (forward)
 collecting definitions 377
 distributing definitions 379
functionality
 event log trapping 1012
 event service 48
 HNTRLib2 29

G

glossary 1010
 DS group 1011

H

handling events 28
health check definition file 754
health check function
 cluster operation 186
 detect process errors 164
 monitored processes 90
 problems that can be detected by 89
 process monitoring 90
 remote host monitoring 92
 troubleshooting problems 89
Hitachi Network Objectplaza Trace Library (HNTRLib2)
 29
 setting 171
Hitachi Network Objectplaza Trace Monitor 2 (service)
 284
Hitachi Network Objectplaza Trace Monitor 2 for 64bit
(service) 284
Hitachi Program Product Installer

notes 126
sample initial window 127
using 126
hnr2conf 405
hnr2getconf 408
hnr2getname (Windows only) 411
hnr2kill (UNIX only) 412
hnr2mon (UNIX only) 413
hnr2util (UNIX only) 414
hnr2util (Windows only) 416
hnr2utl2 (UNIX only) 419
hnr2utl2 (Windows only) 421
HNTRLib2 (Hitachi Network Objectplaza Trace Library)
 29
 setting 171
host access control definition file 771
host group definition file 797
host name
 changing 391

I

index (event server index file) 346, 669
information-search user
 glossary 1012
installation
 notes (UNIX) 128
 notes (Windows) 116
 procedure (UNIX) 125
 procedure (Windows) 114
integrated trace log 845
IP address
 checking 107
 effects and tasks for changing 393
IP binding method 105
 glossary 1012
IPv6 environment 268
ISAM files
 utility commands for operation and maintenance 400

J

jbs_killall.cluster (UNIX only) 424
jbs_log.bat (Windows only) 425
jbs_log.sh (UNIX only) 428
jbs_setup_cluster (Windows only) 432
jbs_spmd_reload 435
jbs_spmd_status 437

[jbs_spmd_stop](#) 439
[jbs_spmd \(UNIX only\)](#) 434
[jbs_start.cluster \(UNIX only\)](#) 442
[jbs_start \(UNIX only\)](#) 440
[jbs_stop.cluster \(UNIX only\)](#) 445
[jbs_stop \(UNIX only\)](#) 444
[jbsacllint](#) 446
[jbsaclreload](#) 447
[jbsadduser](#) 449
[jbsadmin \(Windows only\)](#) 451
[jbsblockadesrv](#) 452
[jbscancellcact](#) 454
[jbschgds \(Windows only\)](#) 455
[jbschgpasswd](#) 456
[jbschkds \(Windows only\)](#) 458
[jbsdfts_srv.conf \(host access control definition file\)](#) 771
[jbsgetcnf](#) 461
[jbsgetopinfo](#) 463
[jbsgetumap](#) 466
[jbshc.conf \(health check definition file\)](#) 754
[jbshosts2export](#) 468
[jbshosts2import](#) 472
[jbshostsexport](#) 467
[jbshostsimport](#) 469
[jbslcact.conf \(local action execution definition file\)](#) 781
[jbslistacl](#) 475
[jbslistlcact](#) 478
[jbslistsrv](#) 479
[jbslistuser](#) 481
[jbsmkpass \(Windows only\)](#) 484
[jbsmkumap](#) 485
[jbsparamdump](#) 487
[jbspassmgr \(Windows only\)](#) 496
[jbsrmacl](#) 497
[jbsrmumap](#) 499
[jbsrmumappass \(Windows only\)](#) 501
[jbsrmuser](#) 502
[jbsrt_del](#) 504
[jbsrt_distrib](#) 506
[jbsrt_get](#) 510
[jbsrt_sync](#) 512
[jbssetacl](#) 514
[jbssetadmingrp \(UNIX only\)](#) 516
[jbssetcnf](#) 518
[jbssetumap](#) 519
[jbssetupsrv \(Windows only\)](#) 522
[jbssetusrsrv \(UNIX only\)](#) 524
[jbsumappass \(Windows only\)](#) 525
[jbsunblockadesrv](#) 527
[jbsunsetcnf](#) 528
[jcocmdconv](#) 530
[jcocmddef](#) 532
[jcocmddel](#) 539
[jcocmdlog](#) 541
[jcocmdshow](#) 544
[jev_forward.conf \(distribution definition file\)](#) 731
[jev_logstart.conf \(distribution definition file\)](#) 731
[jev_logtrap.conf \(distribution definition file\)](#) 731
[jev_ntevent.conf \(distribution definition file\)](#) 731
[jevagtfw](#) 547
[jevdbinit](#) 551
[jevdbmkrep](#) 553
[jevdbswitch](#) 555
[jevdef_distrib](#) 557
[jevdef_get](#) 561
[jevltreload \(Windows only\)](#) 563
[jevexport](#) 564
[jevextreload](#) 568
[jevfwstat](#) 571
[jevlogd.conf \(log information definition file\)](#) 719
[jevlogdstart \(UNIX only\)](#) 570
[jevlogdstat](#) 573
[jevlogdstop \(UNIX only\)](#) 574
[jevlogreload](#) 575
[jevlogstart](#) 577
[jevlogstart \(cluster environment\)](#) 584
[jevlogstat](#) 585
[jevlogstop](#) 586
[jevlogstop \(cluster environment\)](#) 588
[jevmessageid.bat \(Windows only\)](#) 589
[jevregsvc \(Windows only\)](#) 590
[jevreload](#) 591
[jevsend](#) 593
[jevsend \(overview\)](#) 51
[jevsendd](#) 596
[jevsendd \(overview\)](#) 51
[jevstart \(UNIX only\)](#) 599
[jevstat](#) 600
[jevstop \(UNIX only\)](#) 603
[Jischk](#) 604
[Jiscond](#) 606
[Jisconv](#) 608
[Jiscpy](#) 611
[Jisext](#) 612

- Jisinfo 614
- Jiskeymnt 616
- Jisktod 620
- Jislckclear (Windows only) 625
- Jislckext 626
- Jislckfree (Windows only) 628
- Jislckreg (UNIX only) 629
- Jismcktr (Windows only) 630
- Jisprt 631
- Jirsdel (UNIX only) 633
- JP1_HOSTNAME environment variable 179
- JP1_UserLevel (user permission level file) 738
- JP1/AJS
 - glossary 1013
 - note on using log file monitoring job 369
 - Windows event-log monitoring job 373
- JP1/Base
 - communication settings 223
 - compatibility 110
 - confirming startup (UNIX) 291
 - confirming startup (Windows) 286
 - functionality 28
 - functionality (UNIX) 31
 - functionality (Windows) 30
 - glossary 1013
 - installation folder 11
 - limits 916
 - modifying settings during operation 387
 - notes on usage 875
 - overview 27
 - port numbers 911
 - setup 135
 - starting (UNIX) 287
 - starting (Windows) 284
 - stopping (UNIX) 287
 - stopping (Windows) 284
- JP1/Base (service) 284
- JP1/Base administrator 109
 - glossary 1013
- JP1/Base administrator (UNIX only) 946
- JP1/Base Control Service (service) 284
- JP1/Base Event (service) 284
- JP1/Base EventlogTrap (service) 284
- JP1/Base LogTrap (service) 284
- JP1/Base parameter definition file 760
- JP1/IM - Manager
 - glossary 1014
- JP1/IM - View
 - glossary 1014
- JP1/Power Monitor
 - glossary 1014
- JP1 administrators group 109
 - glossary 1013
- jp1base_setup_cluster (UNIX only) 635
- jp1base_setup (UNIX only) 634
- jp1bs_ds_setup.conf (directory server linkage definition file) 744
- jp1bs_param_V7.conf (JP1 Base parameter definition file) 760
- jp1bs_service_0700.conf (extended startup process definition) 762
- jp1bshasetup (Windows only) 638
- jp1BsUmap.conf (user mapping definition file) 749
- JP1 events
 - attributes 800
 - basic attributes 800
 - details 807
 - duplication check 689
 - expiry time 677
 - extended attributes 801
 - forwarding 51
 - glossary 1013
 - list 803
 - number acquired per day 681
 - retrying transfer 676
 - sending and receiving 48
 - types acquired by JP1/Base 51
- jp1hosts (definition file) 766
- jp1hosts2 (definition file) 768
- jp1hosts2 information
 - backup (UNIX) 156
 - backup (Windows) 149
 - defining 248
 - glossary 1014
 - recovery (UNIX) 158
 - recovery (Windows) 151
- jp1hosts information
 - defining 243
 - glossary 1014
- JP1 permission level 33
 - glossary 1014
- jp1ping 639
- JP1 resource group 33

- glossary 1014
- JP1 Resource Group Details dialog box 299
- JP1-specific hosts information
 - command 401
- Jp1svprm_wait.dat (service startup delay time - timer monitoring period definition file) 667
- JP1SVPRM.DAT (start sequence definition file) 339, 662
- JP1 user
 - glossary 1014
 - setting (UNIX) 330
 - setting operating permissions (UNIX) 331
 - setting operating permissions (Windows) 299
 - using commands to set (Windows) 298
 - using GUI to set up (Windows) 297
- JP1 User dialog box (add user) 318
- JP1 User dialog box (user mapping) 306

K

- key definition file
 - glossary 1015
- key file
 - glossary 1015

L

- LANG environment variable 135
- language setting
 - changing (UNIX only) 216
- large numbers of events
 - conditions for suppression of event-forwarding 77
 - glossary 1015
 - precautions 69
 - suppressing forwarding 69
- limits 916
- linkage user
 - setting 318
- Linkage user 41
- linked user
 - glossary 1015
 - setting by command 319
 - setting by using GUI 318
- local action 100
 - glossary 1015
- local action environment variable file 780
- local execution definition file 781
- log files list 848
- log file trap 28

- checking operating status 366
 - starting 366
 - stopping 367
- log file trapping function
 - cluster system use 182
 - end of monitoring 54
 - glossary 1015
 - number of log files (that can be monitored) 64
 - prerequisites 54
 - reattempting to connect to event service 67
 - reattempting to monitor log file when trap fails 65
 - start of monitoring 54
 - types of log files (that can be monitored) 55
 - types of log files (that cannot be monitored) 62
- log-file trap startup definition file 714
- logical host 176
 - deleting (UNIX) 212
 - deleting (Windows) 212
 - glossary 1015
 - prerequisites 178
 - service start control 215
 - setup (UNIX) 201
 - setup (Windows) 189
 - setup in non-cluster environment 218
 - using in non-cluster environment 103
- Logical Host Settings for Primary Node System dialog box 191
- Logical Host Settings for Secondary Node System dialog box 194
- login authentication
 - by linking with directory server 40
- log information
 - types 845
- log information definition file 719
- log on as service 302
- logon check is not done to Windows, when OS user is set 305
- log on locally 302

M

- manager
 - glossary 1015
- managing process 29
- managing system's hierarchical configuration by using commands 83
- managing users 28, 33
- mapping users 45

- memory requirements 918
- monitoring end timing
 - event log trapping function 68
- monitoring interval
 - event log trapping function 68
- monitoring start timing
 - event log trapping function 68
- multi-LAN connectivity
 - glossary 1016
- multiple LAN connections 228

N

- network
 - configuration settings 223
 - multiple network configuration 225
 - network setup check command 396
 - single network configuration 224
- networks
 - use in environments with distinct networks (using jp1hosts2 information) 246
 - use in environments with distinct networks (using jp1hosts information) 241
- NNM 1016
- node switching system
 - glossary 1016
- Non-SSL communication definition file 777
- note on using log-file monitoring job 369
- notes about using JP1/Base linked with the auto-scaling functionality 974
- nvent.conf (action definition file)
 - collecting definitions 377
 - distributing definitions 379
- nvent.conf (action definition file for event log trapping) 721

O

- openssl 642
- operating
 - secure system 953
- operating information
 - glossary 1016
- operating permissions 33
 - batch registration (UNIX) 331
 - batch registration (Windows) 300
 - deleting (UNIX) 332
 - deleting (Windows) 300
 - registering individually (UNIX) 331

- registering individually (Windows) 300
 - setting by GUI (Windows) 299
- operation log 848
 - definition file (jp1bs_baselog_setup.conf) details 943
 - messages 944
 - operation log definition file definition example 944
 - output 935
 - output format 936
 - storage format 935
 - trigger conditions 940
 - types of events recorded 935
- operation log definition file
 - definition example 944
 - details 943
- operation logs
 - settings for outputting 941
- OS user
 - deleting individually (command) 310
 - registering individually (command) 309
 - setting password management information (GUI) 304
 - setting password management information in one operation (command) 309
- OS User Mapping Details dialog box 306
- output setup
 - dump output 172

P

- parameters
 - types of 653
- password 297
 - password for linked user 320
 - Password Manager dialog box 305
- password definition file 736
- password policy definition file 751
- passwords
 - setting save format 142
- physical host
 - glossary 1016
 - prerequisites 179
- physical merge mechanism 236
- port numbers 911
- prerequisites
 - for secure system 953
- prerequisites for using JP1/Base linked with the auto-scaling functionality 960
- primary authentication server 38

- copying settings (UNIX) 332
- copying settings (Windows) 300
- glossary 1016
- primary server 176
- processes
 - glossary 1016
 - list (UNIX) 908
 - list (Windows) 906
- processing time required for configuring and clearing monitoring settings 973
- process log information 848

R

- recovery
 - common definition information (UNIX) 157
 - common definition information (Windows) 150
 - definition files (UNIX) 157
 - definition files (Windows) 150
 - event database (UNIX) 158
 - event database (Windows) 151
 - jp1hosts2 information (UNIX) 158
 - jp1hosts2 information (Windows) 151
- regular expressions 919
 - comparison among 921
 - default syntax 919
 - extended 920
 - extending 140
 - glossary 1016
 - tips on using 922
 - usage examples 923
- remote installation
 - UNIX 126
 - Windows 115
- restricting
 - connection from unintended hosts 954
- routing 226

S

- secondary authentication server 38
 - glossary 1017
- secondary server 176
- secure system
 - operating 953
 - prerequisites 953
- services
 - confirming startup 286

- Hitachi Network Objectplaza Trace Monitor 2 (Hitachi Network Objectplaza Trace Library) 284
- Hitachi Network Objectplaza Trace Monitor 2 (Hitachi Network Objectplaza Trace Library for 64bit) 284
- JP1/Base (process management including user management) 284
- JP1/Base Control Service (startup control) 284
- JP1/Base Event (event services) 284
- JP1/Base EventlogTrap (event log trapping service) 284
- JP1/Base LogTrap (log-file trap management service) 284
- list 284
- setting start timing 342
- starting 284
- start sequence 339
- start sequence control (overview) 47
- start sequence setup 338
- stopping 286
- stop sequence control (overview) 47
- stop sequence setup 338
- services (UNIX) 287
- service startup delay time/timer monitoring period definition file (Windows) 667
- setting
 - authentication server (UNIX) 328
 - authentication server (Windows) 294
 - clustering environment (UNIX) 199
 - clustering environment (Windows) 188
 - communication protocol 228
 - directory server 316
 - event log trapping function 371
 - extending regular expressions 140
 - JP1 user (UNIX) 330
 - JP1 user (Windows) 296
 - linkage user 318
 - log file trap 365
 - new IP address 393
 - operating permissions (UNIX) 331
 - operating permissions (Windows) 299
 - outputting operation logs 941
 - standard user 296
 - user mapping (UNIX) 333
 - user mapping (Windows) (command) 308
 - user mapping (Windows) (GUI) 303
- settings file
 - api 347

- forwarding (forward) 347
- Settings for Base Cluster System dialog box 191
- settings to configure both physical and logical host environments on the same host 196
- setting system's hierarchical configuration 376
- setting up
 - directory server linkage 313
- setup
 - command 396
 - logical host (UNIX) 201
 - logical host (Windows) 189
- setup procedure for using JP1/Base linked with the auto-scaling functionality (for agent hosts) 965
- setup procedure for using JP1/Base linked with the auto-scaling functionality (for the manager host) 963
- shared directory and files 199
- sparse character 618
 - glossary 1017
- specifying shared folder (Windows) 188
- specifying the method for distributing configuration definition information 376
- SSL communication
 - files required 278
- SSL communication definition file 773
- SSL communication environment
 - setting up on client side 281
 - setting up on server side 280
- standard user
 - glossary 1017
 - setting (Windows) 296
 - setting operating permissions (UNIX) 331
 - setting operating permissions (Windows) 299
 - using commands to set (Window) 298
 - using GUI to set up (Window) 297
- Standard user 41
- starting
 - command 396
 - event log trapping function 371
 - JP1/Base (UNIX) 287
 - JP1/Base (Windows) 284
 - log file trap 366
- start sequence definition file 661
- start sequence definition file (JP1SVPRM.DAT) 339
- startup control
 - command 396
 - disable 338
 - notes 343
- stopping

- command 396
- event log trapping function 372
- JP1/Base (UNIX) 287
- JP1/Base (Windows) 284
- log file trap 367
- symbol conventions 9
- syntax conventions 10
- system configuration for using JP1/Base linked with the auto-scaling functionality 958
- system time
 - changing 393

T

- terminating monitoring during scale in 962
- troubleshooting 843
 - action (any OS) 867
 - action (UNIX) 872
 - action (Windows) 869
 - command 401
 - errors detected by health check function 873
 - procedure 844
 - required data 849

U

- uninstallation
 - notes (UNIX) 128
 - notes (Windows) 116
 - procedure (UNIX) 128
 - procedure (Windows) 115
- unintended hosts
 - restricting connection 954
- user authentication 28, 33
 - Settings for the operation to use a DS user 322
 - Settings for the operation to use a linkage user 316
- user authentication block 36
 - glossary 1017
- user management
 - command 397
 - notes (UNIX) 334
 - notes (Windows) 311
 - setting (UNIX) 328
 - setting (Windows) 293
 - setting up (directory server linkage) 313
 - setup procedure (directory server linkage) 314
 - setup procedure (UNIX) 328
 - setup procedure (Windows) 293

- user management function
 - initial settings (UNIX) [125](#)
 - initial settings (Windows) [114](#)
- user mapping [28](#)
 - assigning OS user permissions [301](#)
 - batch setting (UNIX) [333](#)
 - batch setting (Windows) [310](#)
 - changing (Windows) [307](#)
 - checking (Windows) [307](#)
 - deleting individually (UNIX) [334](#)
 - deleting individually (Windows) [311](#)
 - glossary [1017](#)
 - registering individually (UNIX) [333](#)
 - registering individually (Windows) [310](#)
 - setting (UNIX) [333](#)
 - setting (Windows) (command) [308](#)
 - setting (Windows) (GUI) [303](#)
- user mapping definition file [749](#)
- user permission level file [738](#)
- using JP1/Base [946](#)
- using JP1/Base linked with the auto-scaling functionality [958](#)
- using JP1/Base on multiple networks [225](#)
- using JP1/Base on single network [224](#)

V

- version changes
 - changes in 09-00 [1003](#)
 - changes in 10-00 [998](#)
 - changes in 10-10 [996](#)
 - changes in 10-50 [993](#)
 - changes in 11-00 [991](#)
 - changes in 11-10 [990](#)
 - changes in 11-50 [989](#)
- version number conventions [11](#)
- versions
 - compatibility [110](#)
- viewer
 - glossary [1017](#)

W

- Windows event-log monitoring job [373](#)

 **Hitachi, Ltd.**

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