

JP1 Version 13

**JP1/Integrated Management 3 - Event Gateway for
Network Node Manager i**

3021-3-L08(E)

Notices

■ Relevant program products

For details about the supported OS versions, and about the OS service packs and patches required by JP1/Integrated Management 3 - Event Gateway for Network Node Manager i, see the release notes for the relevant product.

JP1/Integrated Management 3 - Event Gateway for Network Node Manager i (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-2A2C-8GDL JP1/Integrated Management 3 - Event Gateway for Network Node Manager i 13-00

JP1/Integrated Management 3 - Event Gateway for Network Node Manager i (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12)

P-842C-8GDL JP1/Integrated Management 3 - Event Gateway for Network Node Manager i 13-00

■ Trademarks

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

Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. 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, 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.

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.

JP1/Integrated Management 3 - Event Gateway for Network Node Manager i includes Dell BSAFE(TM) Cryptographic software of Dell Inc.

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

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

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

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

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

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

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

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

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

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

Java is a registered trademark of Oracle and/or its affiliates.



■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

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

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

■ Restrictions

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

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

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

■ Issued

Aug. 2023: 3021-3-L08(E)



■ Copyright

Copyright (C) 2023, Hitachi, Ltd.

Copyright (C) 2023, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-L08(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) 2019 • Microsoft(R) Windows Server(R) 2022 • Red Hat(R) Enterprise Linux(R) Server 8 (64-bit x86_64) • Red Hat(R) Enterprise Linux(R) Server 9 (64-bit x86_64) • Oracle Linux(R) Operating System 8 • Oracle Linux(R) Operating System 9 • SUSE Linux(R) Enterprise Server 15 	--
<p>The following OSs were deleted from the supported OSs:</p> <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2012 • Red Hat(R) Enterprise Linux(R) Server 6 (64-bit x86_64) • CentOS 6 (x64) • CentOS 7 • Oracle Linux(R) Operating System 6 (x64) 	--
A description of the JP1/IM - EG for NNMi service was added.	1.5
The default port number, which is set when a port number (<code>-port</code> option) is not specified during a new setup using the setup command (<code>jegn_setup</code>), was changed.	2.4.1, <i>jegn_setup</i>
English UTF-8 encoding values were added for the environment variables file (<code>jegn_env.conf</code> file) and environment variable <code>LANG</code> in the JP1/Base <code>jplbs_param.conf</code> file.	2.3.1, 2.4.2(1), 2.4.2(2)
A description was added to the procedure for configuring automatic startup and termination settings in UNIX when SELinux is enabled.	2.4.4(2)
A description regarding data collection preparations for troubleshooting (Windows only) was added.	2.4.5(2)
<p>The following descriptions were added to backup and restoration procedures:</p> <ul style="list-style-type: none"> • Configuration information management • Backup and restoration of common definition information 	6.1.1, 6.1.2(2), 6.1.3(2)
Boot process information was removed from OS log information retrievable using data collection tools in UNIX. Additional changes were made to the description of distribution information.	10.3.2(1)

Legend:

--: Not applicable

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

Preface

This manual describes the functions of JP1/Integrated Management 3 - Event Gateway for Network Node Manager i and how to configure and operate it. In this manual, JP1/Integrated Management 3 - Event Gateway for Network Node Manager i is abbreviated as *JP1/IM - EG for NNMi*. Replace the term JP1/Integrated Management - Event Gateway for Network Node Manager I with the term *JP1/IM - EG for NNMi* while reading this manual.

■ Intended readers

This manual is intended for users who convert NNMi incidents issued by JP1/Network Node Manager i, or JP1/Network Node Manager i Advanced into JP1 events and who use JP1/Integrated Management to manage and monitor such JP1 events. The manual assumes that the user is familiar with JP1/Base, JP1/Integrated Management, JP1/Network Node Manager i, and JP1/Network Node Manager i Advanced.

■ Organization of this manual

This manual consists of the following parts.

PART 1: Overview

Part 1 provides an overview of JP1/IM - EG for NNMi and describes the system configuration and procedure for converting NNMi incidents.

PART 2: Configuration and Operation

Part 2 explains how to install and set up JP1/IM - EG for NNMi and the tasks required during operation.

PART 3: Reference

Part 3 describes the commands supported by JP1/IM - EG for NNMi and the JP1 events and messages that are issued by JP1/IM - EG for NNMi.

PART 4: Troubleshooting

Part 4 describes troubleshooting when problems occur in JP1/IM - EG for NNMi.

■ Conventions: Diagrams

This manual uses the following conventions in diagrams:

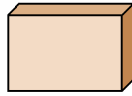
- Computer (terminal)



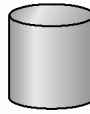
- Computer



- Program



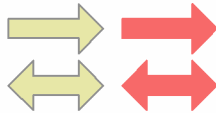
- File



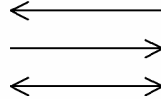
- Flow of procedure or task



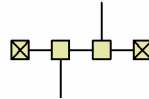
- Flow of data



- Flow of control



- Network



- Failure



■ Conventions: Fonts and symbols

Font and symbol conventions are classified as:

- General font conventions
- Conventions in syntax explanations

These conventions are described below.

General font conventions

The following table lists the general font conventions:

Font	Convention
Bold	<p>Bold type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio button options, and explanatory labels. For example, bold type 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 actual text provided by the user or the 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>. • Use the <code>send</code> command to send mail. • The following message is displayed: <code>The password is incorrect.</code>

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

```
MakeDatabase
```

```
...
```

```
StoreDatabase temp DB32
```

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

Conventions in syntax explanations

Syntax definitions appear as follows:

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

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
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.
<u>perm</u>	Underlined characters indicate the default value.
[]	Square brackets enclose an item or set of items whose specification is optional. Example: [A] means either nothing or A can be specified.
	Only one of the options separated by a vertical bar can be specified at the same time. Example: A B C means A, or B, or C.
...	An ellipsis (...) indicates that the item or items enclosed in () or [] immediately preceding the ellipsis may be specified as many times as necessary. Example: A, B, ... means that as many Bs as necessary are to be specified immediately after A.
{ }	One of the items or sets of items enclosed in curly brackets must be selected. Inside the curly brackets, each item or set of items is separated by a vertical bar (). Example: {A B C} means that A, or B, or C must be specified.
()	Parentheses indicate the range of items to which the vertical bar () or ellipsis (...) is applicable.

■ Conventions: Installation folders for the Windows versions of JP1/IM - EG for NNMi, JP1/Base, and JP1/IM

In this manual, the installation folders for the Windows versions of JP1/IM - EG for NNMi, JP1/Base, and JP1/IM are as follows:

Product name	Installation folder	Default installation folder [#]
JP1/IM - EG for NNMI	<i>EG-for-NNMI-path</i>	<i>system-drive:\Program Files(x86)\HITACHI\JP1EG4NNMI</i>
JP1/Base	<i>Base-path</i>	<i>system-drive:\Program Files\HITACHI\JP1Base</i>
JP1/IM - Manager	<i>Console-path</i>	<i>system-drive:\Program Files\HITACHI\JP1Cons</i>

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

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

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

Contents

Notices	2
Summary of amendments	5
Preface	6

Part 1: Overview

1	Overview of JP1/IM - EG for NNMi	15
1.1	About JP1/IM - EG for NNMi	16
1.2	Overview of operation using JP1/IM - EG for NNMi	17
1.3	System configuration of JP1/IM - EG for NNMi	18
1.3.1	Applicable OSs	18
1.3.2	Prerequisite programs	19
1.4	NNMi incident conversion procedure	20
1.5	JP1/IM - EG for NNMi service	21

Part 2: Configuration and Operation

2	Installation and Setup	22
2.1	Installation and setup procedures	23
2.2	Installing (in Windows)	24
2.2.1	Installation procedure	24
2.2.2	Uninstallation procedure	25
2.2.3	Notes about installation	25
2.3	Installing (in UNIX)	26
2.3.1	Installation procedure	26
2.3.2	Uninstallation procedure	27
2.3.3	How to use Hitachi Program Product Installer	27
2.3.4	Notes about installation	29
2.4	Setting up	30
2.4.1	Executing the setup command	30
2.4.2	Environment variable settings (UNIX only)	31
2.4.3	Setting the definition files	33
2.4.4	Setting automatic startup and automatic termination	33
2.4.5	Settings for handling errors	35
3	Operation and Environment Configuration in a Cluster System	39
3.1	Environment setup procedure	40

3.2	Installing and setting up the logical host	42
3.2.1	Installing and setting up the active server	42
3.2.2	Installing and setting up the standby server	43
3.2.3	Procedure for changing settings	44
3.3	Registering into the cluster software	45
3.3.1	Registering into the cluster software (in Windows)	45
3.3.2	Registering into the cluster software (in UNIX)	46
3.4	Deleting the logical host	49
3.5	Notes about cluster operation	50
4	Converting NNMi Incidents into JP1 Events	51
4.1	Creating an NNMi incident forwarding filter definition file	52
4.1.1	Format of the NNMi incident forwarding filter definition file	52
4.1.2	Defining a filter condition block	54
4.1.3	Defining a mapping block	61
4.1.4	Definition example (sample file)	64
4.2	Creating a mapping definition file	66
4.2.1	Name and storage location of the mapping definition file	66
4.2.2	Format of the mapping definition file	66
4.3	Creating a custom attribute mapping definition file	68
4.3.1	Name and storage location of the custom attribute mapping definition file	68
4.3.2	Format of the custom attribute mapping definition file	69
4.4	Editing the JP1/IM - Manager definition files	71
4.4.1	Definition file for extended event attributes	71
4.4.2	Definition file for opening monitor windows	75
5	Startup and Termination	77
5.1	Starting JP1/IM - EG for NNMi	78
5.1.1	In Windows	78
5.1.2	In UNIX	78
5.2	Terminating JP1/IM - EG for NNMi	79
5.2.1	In Windows	79
5.2.2	In UNIX	79
6	JP1/IM - EG for NNMi Operations	80
6.1	Backup and restoration	81
6.1.1	Managing the configuration information	81
6.1.2	Backing up the settings	81
6.1.3	Restoring the settings	83
6.2	Changing settings	84
6.2.1	Editing the definition files	84

- 6.2.2 Changing the settings of the host name, IP address, and port number on which JP1/IM - EG for NNMi is running 84
- 6.2.3 Changing the date and time of the system on which JP1/IM - EG for NNMi is running 85
- 6.3 Notes regarding operation 88

Part 3: Reference

7 Commands 89

- Format of command explanations 90
- Lists of commands 91
- jegn_killall.cluster (UNIX only) 92
- jegn_log.bat (Windows only) 93
- jegn_log.sh (UNIX only) 95
- jegn_setup 98
- jegn_setup_cluster 103
- jegn_spm�_reload 104
- jegn_spm�_status 106
- jegn_start (UNIX only) 108
- jegn_start.cluster (UNIX only) 109
- jegn_stop (UNIX only) 110
- jegn_stop.cluster (UNIX only) 111

8 JP1 Events 112

- 8.1 Attributes of JP1 events 113
- 8.2 JP1 events obtained by converting NNMi incidents 114
- 8.3 JP1 events issued by JP1/IM - EG for NNMi 119
- 8.4 Details of JP1 events issued by JP1/IM - EG for NNMi 120
- 8.4.1 List of JP1 events issued by JP1/IM - EG for NNMi 120
- 8.4.2 Details of JP1 events 120

9 Messages 122

- 9.1 Message output destinations 123
- 9.1.1 Output destinations of messages related to installation (KNAG0001 to KNAG0999) 123
- 9.1.2 Output destinations of messages related to execution of commands (KNAG1000 to KNAG1999) 123
- 9.1.3 Output destinations of messages related to services (KNAG2000 to KNAG2999) 124
- 9.1.4 Output destinations of messages related to process management (KAVB3501 to KAVB3999) 125
- 9.2 Message format 129
- 9.2.1 Output format of messages 129
- 9.2.2 Format of message explanations 129
- 9.2.3 For system administrators 130
- 9.3 Messages 131
- 9.3.1 Messages related to installation (KNAG0001 to KNAG0999) 131
- 9.3.2 Messages related to execution of commands (KNAG1000 to KNAG1999) 134
- 9.3.3 Messages related to services (KNAG2000 to KNAG2999) 149

Part 4: Troubleshooting

10 Troubleshooting 192

- 10.1 Troubleshooting procedure 193
- 10.2 Types of log information 194
 - 10.2.1 Integrated trace log 194
 - 10.2.2 Trace log for issued JP1 events 195
 - 10.2.3 Trace logs for each process 198
- 10.3 Data to be collected in the event of an error 199
 - 10.3.1 Data to be collected (in Windows) 199
 - 10.3.2 Data to be collected (in UNIX) 206

Appendixes 216

- A Lists of Files and Directories 217
 - A.1 Files and folders (in Windows) 217
 - A.2 Files and directories (in UNIX) 218
- B Lists of Processes 221
 - B.1 List of processes (in Windows) 221
 - B.2 List of processes (in UNIX) 221
- C List of Limit Values 222
- D Performance and Estimation 223
- E Regular Expressions 224
 - E.1 Syntax for regular expressions 224
 - E.2 How to specify regular expressions 225
 - E.3 Hints on using regular expressions 226
 - E.4 Examples of regular expressions 226
- F Definition Files 228
 - F.1 Extended startup process definition file (jegn_service_0700.conf) 229
 - F.2 JP1/IM - EG for NNMI parameter definition file (jegn_param_V7.conf) 230
- G Version Changes 232
 - G.1 Changes in version 13-00 232
 - G.2 Changes in version 12-00 232
 - G.3 Changes in version 11-50 233
- H Reference Material for this Manual 234
 - H.1 Related publications 234
 - H.2 Conventions: Abbreviations 235
 - H.3 Acronyms 235
 - H.4 Conventions: KB, MB, GB and TB 236
- I Glossary 237

1

Overview of JP1/IM - EG for NNMi

This chapter provides an overview of JP1/IM - EG for NNMi and describes the system configuration and the procedure for converting NNMi incidents.

1.1 About JP1/IM - EG for NNMi

When an event such as a failure occurs on a network device that is managed by JP1/NNMi, an *NNMi incident* is issued. JP1/IM - EG for NNMi is a product that converts such NNMi incidents into *JP1 events* so that they are in a format that can be managed by JP1/Base.

The converted JP1 events are forwarded to a JP1/IM integrated management system product, which manages and monitors the converted JP1 events in the same way that it manages and monitors JP1 events that are issued by other JP1-series programs.

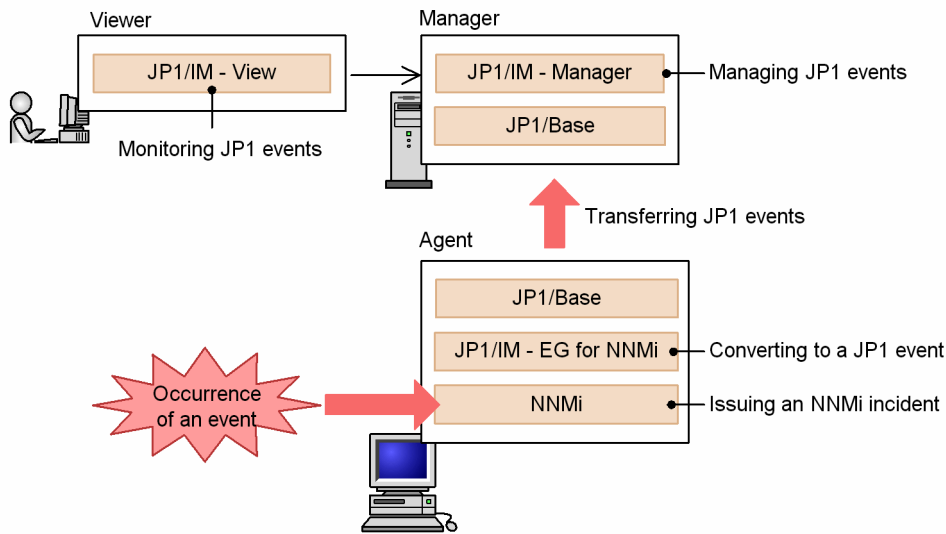
JP1/IM achieves integrated management of systems by linking with middleware products (JP1 series products), such as for job management and storage management, as well as with JP1/IM - EG for NNMi, thus enabling it to manage the configuration and operations of the entire system.

In this manual, JP1/NNMi are abbreviated as *NNMi*.

1.2 Overview of operation using JP1/IM - EG for NNMi

The following figure provides an overview of using JP1/IM - EG for NNMi to convert NNMi incidents into JP1 events and then using JP1/IM to manage and monitor the converted JP1 events.

Figure 1–1: Managing and monitoring JP1 events converted by JP1/IM - EG for NNMi



NNMi issues an NNMi incident whenever an event such as a failure occurs in a network device. Periodically, JP1/IM - EG for NNMi acquires the NNMi incidents issued by NNMi and converts them into JP1 events. If you define filter conditions, you can convert only specific NNMi incidents into JP1 events.

The JP1 events converted by JP1/IM - EG for NNMi are registered into JP1/Base's event database and then forwarded to the manager host. They are then registered into the JP1/Base event database at the manager host, from where they can be managed centrally by JP1/IM - Manager.

The converted JP1 events can be viewed in the Event Console window of JP1/IM - View. When necessary, you can open the NNMi window from the Event Console window to check why events occurred.

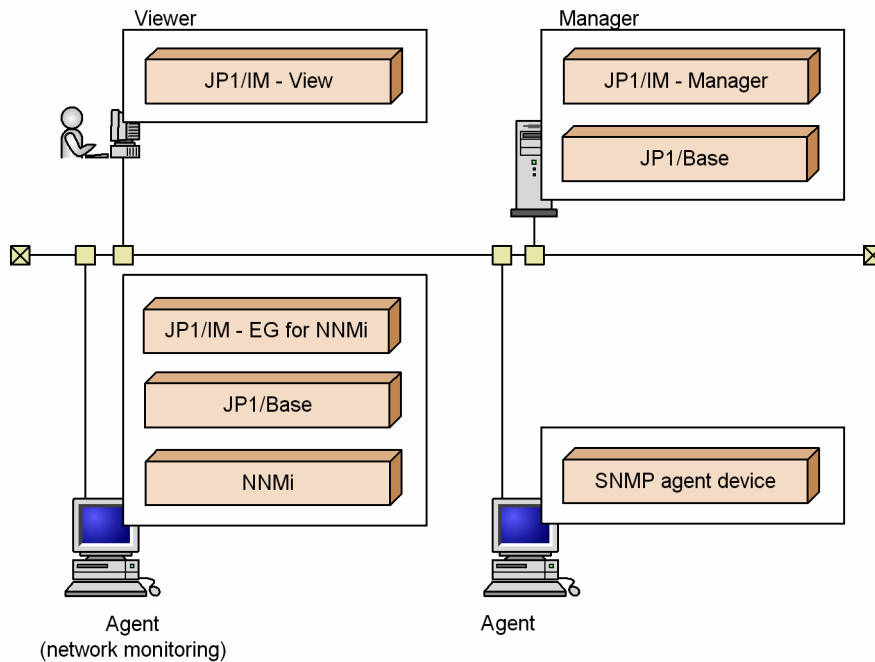
1.3 System configuration of JP1/IM - EG for NNMi

You use JP1/IM - EG for NNMi by linking it with the JP1/IM system.

The JP1/IM system consists of a *manager* that performs integrated management of systems, *agents* that run on the monitored servers, and a *viewer* from which monitoring and operations are performed.

JP1/IM - EG for NNMi is installed together with JP1/Base and NNMi on an agent. The following figure shows an example of a system configuration for JP1/IM - EG for NNMi.

Figure 1–2: Example of a system configuration for JP1/IM - EG for NNMi



Cluster system support

JP1/IM - EG for NNMi supports operations in a cluster system. By applying JP1/IM - EG for NNMi to a cluster, you can inherit processing from the primary node to the secondary node in the event of a server failure.

1.3.1 Applicable OSs

The OSs under which JP1/IM - EG for NNMi can be used are listed below. For details about the versions and types of supported OSs (such as Enterprise Edition), see the applicable Release Notes.

In Windows:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

In UNIX:

- Linux

1.3.2 Prerequisite programs

This subsection describes the prerequisite programs for JP1/IM - EG for NNMi and the JP1/IM system. For details, see the *Release Notes* for the applicable products.

Important

In order for JP1/IM - EG for NNMi to run normally, the corresponding DLL and OS-standard DLLs are required. If another product injects a DLL into a JP1/IM - EG for NNMi process, it will affect the behavior of JP1/IM - EG for NNMi. This might lead to unstable operation or prevent JP1/IM - EG for NNMi from starting.

If this problem occurs, to identify the cause, you can ask the customer to confirm whether the same problem occurs when no other products are installed.

If the customer cannot verify that a DLL being injected by another product is not the cause of the problem, Hitachi might not be able to provide normal support service.

(1) Prerequisite programs for JP1/IM - EG for NNMi

The following table lists the prerequisite programs for JP1/IM - EG for NNMi.

- JP1/Base
- NNMi

(2) Prerequisite programs for JP1/IM system

(a) Prerequisite programs for the manager host

The prerequisite programs for the manager host are listed below.

- JP1/IM - Manager
- JP1/Base

(b) Prerequisite program for the viewer host

The prerequisite program for viewer host is listed below.

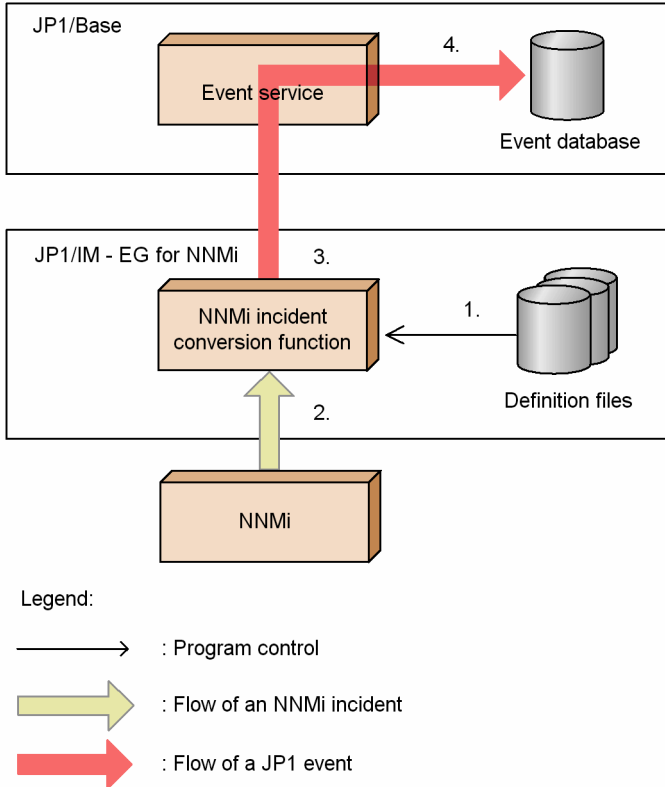
- JP1/IM - View

A Web browser is required in order to open the NNMi windows from a monitor. For details about the supported Web browsers, see the documentation for the NNMi product.

1.4 NNMi incident conversion procedure

JP1 events obtained by converting NNMi incidents are registered into the event database that is provided by the event service of JP1/Base, where they are managed in the same manner as with JP1 events issued by JP1-series programs. The figure below shows the procedure for converting NNMi incidents into JP1 events and then registering them into the JP1/Base event database. The numbers in the figure indicate the sequence of the steps in the procedure.

Figure 1–3: NNMi incident conversion procedure



The following describes each step shown in the figure.

To convert NNMi incidents:

1. Load definition files.

When JP1/IM - EG for NNMi starts, the definition files listed below are loaded:

- NNMi incident forwarding filter definition file
- Mapping definition file

2. Acquire NNMi incidents from NNMi periodically.

Periodically, JP1/IM - EG for NNMi issues NNMi incident acquisition requests to NNMi. If any applicable NNMi incidents have occurred, JP1/IM - EG for NNMi acquires them.

3. Convert the NNMi incidents into JP1 events.

JP1/IM - EG for NNMi converts into JP1 events only those acquired NNMi incidents that match the filter conditions specified in the NNMi incident forwarding filter definition file.

4. Register the JP1 events into the event database of JP1/Base.

JP1/IM - EG for NNMi uses the event service of JP1/Base to register the JP1 events into the event database.

1.5 JP1/IM - EG for NNMi service

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

In the following table, italic character strings indicate variables.

Table 1–1: JP1/IM - EG for NNMi services

Displayed name	Service name	Startup type	Description
JP1/IM3 - EG for NNMi	JP1_IM-EG_for_NNMI	Manual	JP1/IM - EG for NNMi service on a physical host
JP1/IM3 - EG for NNMi <i>logical-host-name</i> [#]	JP1_IM-EG_for_NNMI_ <i>logical-host-name</i>	Manual	JP1/IM - EG for NNMi service on a logical host (<i>logical-host-name</i>)

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

Important

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

2

Installation and Setup

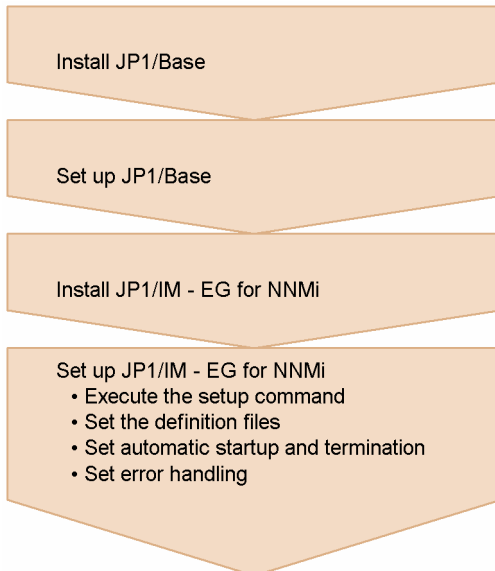
This chapter describes how to install, set up, and uninstall JP1/IM - EG for NNMi.

2.1 Installation and setup procedures

This section describes the installation and setup procedures.

You must have Administrator permissions in Windows and superuser permissions in UNIX to perform the installation and setup procedures.

Figure 2–1: Installation and setup procedures



Installing JP1/Base

For details about how to install and set up JP1/Base, see the *JP1/Base User's Guide*.

Installing NNMi

For details about how to install NNMi, see the documentation for the applicable NNMi product.

You can install NNMi at any time; however, at the time you set up JP1/IM - EG for NNMi, you will need the NNMi settings listed in the table below. Check these settings before you begin the setup of JP1/IM - EG for NNMi.

Table 2–1: NNMi settings required during setup

Item	Description
NNMi user name	User name of the Web service client [#] of NNMi
NNMi password	Password of the Web service client [#] of NNMi
NNMi port number	Port number of the NNMi that is to be connected
NNMi language	Language of the NNMi that is to be connected
Availability of TLS	Whether TLS is to be used when NNMi is connected

#

For details about how to create a Web service client of NNMi, see the documentation for the applicable NNMi product.

2.2 Installing (in Windows)

This section describes how to install and uninstall JP1/IM - EG for NNMi in a Windows environment.

2.2.1 Installation procedure

JP1/IM - EG for NNMi requires JP1/Base as a prerequisite product. You must install JP1/Base before you can install JP1/IM - EG for NNMi.

The following table lists the language type for JP1/IM - EG for NNMi that is specified based on OS system locale.

Table 2–2: Language type for JP1/IM - EG for NNMi (in Windows)

OS system locale	Language type
Japanese	Japanese
English	English

Important

Once you have installed JP1/IM - EG for NNMi, you cannot change the language environment. To change the language environment, uninstall JP1/IM - EG for NNMi, change the system locale for the OS, and then install JP1/IM - EG for NNMi again.

To install JP1/IM - EG for NNMi:

1. Terminate the programs.

Stop the JP1/Base services.

Stop the NNMi services.

2. Insert the distribution medium into the corresponding drive.

Follow the instructions of the installer, which starts automatically. In the case of a new installation, specify the following information:

- User information
- Installation folder

The default installation folder is as follows:

```
system-drive:\Program Files(x86)\HITACHI\JP1EG4NNMI
```

In the case of an overwrite installation or upgrade installation, the existing information specified during the previous installation is inherited. To change the installation folder, uninstall the product and then re-install it.

About remote installation using JP1/Software Distribution

Remote installation (software distribution) by JP1/Software Distribution is supported for JP1/IM - EG for NNMi. For details about how to use JP1/Software Distribution to perform remote installation, see the *Job Management Partner I/Software Distribution Administrator's Guide Volume 1*.

About overwrite installation and upgrade installation

Before you perform an overwrite installation or upgrade installation of JP1/IM - EG for NNMi, stop the services of JP1/IM - EG for NNMi.

2.2.2 Uninstallation procedure

To uninstall JP1/IM - EG for NNMi:

1. Terminate the programs.

Stop the JP1/Base services.

Stop the NNMi services.

Stop the JP1/IM - EG for NNMi services.

2. Delete JP1/IM - EG for NNMi.

In Windows, choose **Control Panel**, then **Add or Remove Programs**, and then remove **JP1/Integrated Management 3 - Event Gateway for Network Node Manager i**.

3. Delete user files.

Definition files and log files that were created after installation and files that may be edited by the user are not deleted. To delete these files, use Explorer to delete the folder in which JP1/IM - EG for NNMi had been installed.

Important

When JP1/Base is uninstalled, the definition information for JP1/IM - EG for NNMi is also deleted. JP1/IM - EG for NNMi will no longer run, even when JP1/Base is reinstalled. In this case, an overwrite installation of JP1/IM - EG for NNMi needs to be performed.

2.2.3 Notes about installation

JP1/IM - EG for NNMi does not support the disk-copy installation function of ServerConductor/DeploymentManager, JP1/ServerConductor/Deployment Manager, and products from other companies.

Furthermore, JP1/IM - EG for NNMi does not support the function for copying disks by creating image files.

(This function is provided by virtualization platforms.) Before performing a disk-copy installation or a copy operation using a virtualization platform, uninstall JP1/IM - EG for NNMi.

Perform the disk-copy installation or copy operation using the virtualization platform, and then re-install JP1/IM - EG for NNMi.

For details on how to perform disk-copy installations, see the manuals for ServerConductor/DeploymentManager and JP1/ServerConductor/Deployment Manager.

For details on the copy functions of virtualization platforms, see the relevant manual for the applicable virtualization software.

2.3 Installing (in UNIX)

This section describes how to install and uninstall JP1/IM - EG for NNMi in a UNIX environment.

2.3.1 Installation procedure

JP1/IM - EG for NNMi requires JP1/Base as a prerequisite product. You must install JP1/Base before you can install JP1/IM - EG for NNMi.

First check that the temporary directory (/tmp) meets the following requirements before starting the installation:

- 5 MB of free space
- The `noexec` option is not specified

The following table lists the language type for JP1/IM - EG for NNMi that is specified based on the environment variables file configured during the setup after installation of JP1/IM - EG for NNMi.

Table 2–3: Language type for JP1/IM - EG for NNMi (in UNIX)

Value of environment variable LANG in the environment variables file (jegn_env.conf)	Language type
ja_JP.UTF-8, ja_JP.utf8, ja_JP.SJIS, or ja_JP.sjis	Japanese
en_US.UTF-8, or en_US.utf8	English
C	
Other than above	

To install JP1/IM - EG for NNMi:

1. Terminate the programs.
 - Stop the JP1/Base services.
 - Stop the NNMi services.
 - Stop the JP1/IM - EG for NNMi services.
2. Run Hitachi Program Product Installer.
 - Follow the instructions of Hitachi Program Product Installer. For details about how to use Hitachi Program Product Installer, see [2.3.3 How to use Hitachi Program Product Installer](#).

About remote installation using JP1/Software Distribution

Remote installation (software distribution) by JP1/Software Distribution is supported for JP1/IM - EG for NNMi. For details about how to use JP1/Software Distribution to perform remote installation, see *Job Management Partner I/Software Distribution Administrator's Guide Volume 1*.

About overwrite installation and upgrade installation

Before you perform an overwrite installation or upgrade installation of JP1/IM - EG for NNMi, stop the services of JP1/IM - EG for NNMi.

2.3.2 Uninstallation procedure

To uninstall JP1/IM - EG for NNMi:

1. Terminate the programs.
Stop the JP1/Base services.
Stop the NNMi services.
2. Back up the user files.
Directories containing files, such as definition files and log files, will also be deleted. If necessary, back them up before proceeding to the next step.
3. Run Hitachi Program Product Installer.
Follow the instructions of Hitachi Program Product Installer to perform uninstallation. For details about how to use Hitachi Program Product Installer, see [2.3.3 How to use Hitachi Program Product Installer](#).

Important

- When JP1/Base is uninstalled, the definition information for JP1/IM - EG for NNMi is also deleted. JP1/IM - EG for NNMi will no longer run, even when JP1/Base is reinstalled. In this case, an overwrite installation of JP1/IM - EG for NNMi needs to be performed.
- After uninstalling JP1/IM - Manager, check if the following directories remain. If any remain, delete them.
 - /etc/opt/jp1eg4nnmi
 - /opt/jp1eg4nnmi
 - /var/opt/jp1eg4nnmi

2.3.3 How to use Hitachi Program Product Installer

Hitachi Program Product Installer is stored on the distribution medium of JP1/IM - EG for NNMi. This subsection describes the following procedures:

- How to start Hitachi Program Product Installer
- How to use Hitachi Program Product Installer to install JP1/IM - EG for NNMi
- How to use Hitachi Program Product Installer to uninstall JP1/IM - EG for NNMi
- How to use Hitachi Program Product Installer to check the version of currently installed Hitachi products

User permissions for execution of Hitachi Program Product Installer

You must have superuser permissions in order to use Hitachi Program Product Installer. Either log in as a superuser or use the `su` command to change to a superuser.

(1) Starting Hitachi Program Product Installer

To start Hitachi Program Product Installer:

1. Insert the JP1/IM - EG for NNMi distribution medium in the drive.
2. Mount the distribution medium.

The mounting method depends on the OS, hardware, and environment. For details about the mounting method, see the documentation for the OS.

- In Linux

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

Note that the underlined distribution medium file system mount directory name depends on the environment.

3. Start Hitachi Program Product Installer.

The directory and file names on the distribution medium may not be as shown here depending on the machine environment. Use the `ls` command to check the directory and file names, and make sure to use the displayed names.

- In Linux

```
/mnt/cdrom/linux/setup /mnt/cdrom
```

Replace the underlined part with the actual distribution medium mount directory name.

4. Unmount the distribution medium.

When installation is completed, unmount the distribution medium. For details about how to unmount a distribution medium, see the documentation for the OS.

- In Linux

```
/bin/umount /mnt/cdrom
```

Replace the underlined part with the actual distribution medium mount directory name.

(2) Installing JP1/IM - EG for NNMi

This subsection describes how to use Hitachi Program Product Installer to install JP1/IM - EG for NNMi. When you start Hitachi Program Product Installer, the initial window appears.

Figure 2–2: Example of Hitachi Program Product Installer's 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 the initial window to display a list of software programs that can be installed. Move the cursor to the software program that you wish to install and press the space bar to select it. Enter `I` again to install the selected software (JP1/IM - EG for NNMi). When installation is completed, enter `Q` to return to the initial window.

(3) Uninstalling JP1/IM - EG for NNMi

Enter the following command to start Hitachi Program Product Installer:

```
/etc/hitachi_setup
```

Hitachi Program Product Installer's initial window is displayed.

Enter **D** in the initial window to display a list of software programs that can be uninstalled. Move the cursor to the software program that you wish to uninstall and press the space bar to select it. Enter **D** again to uninstall the selected software (JP1/IM - EG for NNMi). When uninstallation is completed, enter **Q** to return to the initial window.

(4) Displaying version information

Execute the following command to start Hitachi Program Product Installer:

```
/etc/hitachi_setup
```

Hitachi Program Product Installer's initial window is displayed.

Enter **L** in the initial window to display a list of Hitachi products that have been installed.

2.3.4 Notes about installation

JP1/IM - EG for NNMi does not support the disk-copy installation function of ServerConductor/DeploymentManager, JP1/ServerConductor/Deployment Manager, and products from other companies.

Furthermore, JP1/IM - EG for NNMi does not support the function for copying disks by creating image files.

(This function is provided by virtualization platforms.) Before performing a disk-copy installation or a copy operation using a virtualization platform, uninstall JP1/IM - EG for NNMi.

Perform the disk-copy installation or copy operation using the virtualization platform, and then re-install JP1/IM - EG for NNMi.

For details on how to perform disk-copy installations, see the manuals for ServerConductor/DeploymentManager and JP1/ServerConductor/Deployment Manager.

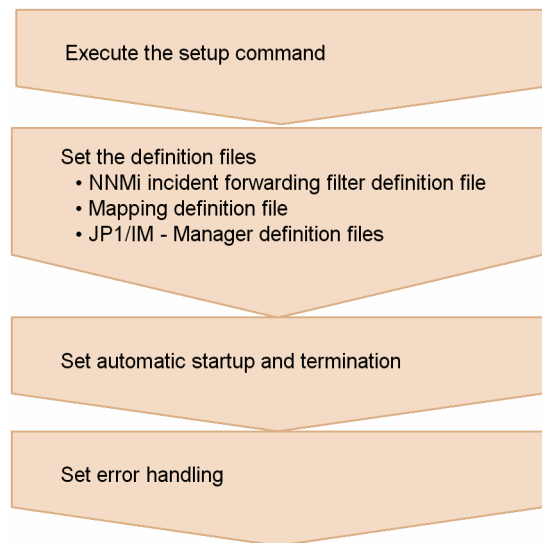
For details on the copy functions of virtualization platforms, see the relevant manual for the applicable virtualization software.

2.4 Setting up

This section describes how to set up JP1/IM - EG for NNMi.

The following figure shows the setup procedure.

Figure 2–3: Setup procedure



2.4.1 Executing the setup command

After you have installed JP1/IM - EG for NNMi, you execute the setup command (`jegn_setup`) to set up an operating environment for JP1/IM - EG for NNMi.

For details about the `jegn_setup` command, see *jegn_setup* in 7. *Commands*.

The following table lists and describes the information that is set by the `jegn_setup` command.

Table 2–4: Information set by the `jegn_setup` command

Item	Description	Setting
NNMi user name	Sets the user name of the Web service client ^{#1} of NNMi.	Y
NNMi password	Sets the password of the Web service client ^{#1} of NNMi.	Y
NNMi port number	Sets the port number of the NNMi that is to be connected.	_{#2}
NNMi language	Sets the language of the NNMi that is to be connected.	--
NNMi incident re-acquisition interval	Sets the interval at which another attempt is to be made to acquire NNMi incidents when there are no NNMi incidents to be acquired or in the event of an exception such as a communication error.	--
NNMi incident acquisition method	Sets the first NNMi incident to be acquired in cases where NNMi incidents issued while the JP1/IM - EG for NNMi services are stopped are to be acquired the next time the services start (except during the initial start).	--
Availability of TLS	Sets whether TLS is to be used when NNMi is connected.	--

Legend:

Y: Setting is required

--: Setting is optional

#1
For details about how to create a Web service client of NNMi, see the documentation for the NNMi product.

#2
The port number set by default when performing a new installation of JP1/IM - EG for NNMi version 13 is the port number used by default when performing a new installation of NNMi version 13. The http/https port in use by JP1/NNMi must be set to the NNMi port number using the `jegn_setup` command under one of the following conditions:

- When installing JP1/IM - EG for NNMi version 13 on an operating environment running JP1/NNMi version 12 or an earlier version
- When performing a new installation of JP1/IM - EG for NNMi version 13 on an operating environment that has upgraded from JP1/NNMi version 12 or an earlier version to version 13
- When changing the default JP1/NNMi http/https port values

About overwrite setup

You can use the `-update` option of the `jegn_setup` command to change the operating environment of JP1/IM - EG for NNMi.

TLS protocol versions can be used

The following TLS protocol versions can be used in JP1/IM - EG for NNMi:

- TLSv1.2 protocol
- TLSv1.1 protocol
- TLSv1 protocol

For this reason, specify settings in the connection-destination JP1/NNMi so that one or more of the preceding protocol versions can be used. For information on how to specify settings in JP1/NNMi, see the JP1/NNMi documentation.

2.4.2 Environment variable settings (UNIX only)

UNIX users must set the language code used by JP1/IM - EG for NNMi. Configure the language code setting for both the environment variables file and common definitions.

Note the following points about the environment variables settings.

- When `LC_ALL` is not specified, the settings of `LC_MESSAGES`, `LANG`, and `LC_CTYPE`[#] must be the same.
- When `LC_ALL` and `LC_MESSAGES` are not specified, the settings of `LANG` and `LC_CTYPE`[#] must be the same.

#

The settings of `LC_CTYPE` are optional.

Each setting must maintain uniformity within the local host. For details about the procedure to use to configure settings, see below.

(1) Setting the language encoding in the environment variable file

Using a text editor such as `vi`, open the `/etc/opt/jpleg4nnmi/conf/jegn_env.conf` file and, following `LANG=` on the first line, set the appropriate value for the `LANG` environment variable based on the following table.

Table 2–5: Values that can be specified for LANG in the `jegn_env.conf` file

OS			Language type in use	Value of LANG environment variable
Type	Language type	Encoding		
Linux	Japanese	UTF-8 ^{#1}	Japanese	<code>ja_JP.UTF-8</code> or <code>ja_JP.utf8</code>
		SJIS ^{#2}		<code>ja_JP.SJIS</code> or <code>ja_JP.sjis</code>
	English	UTF-8 ^{#1}	English	<code>en_US.UTF-8</code> or <code>en_US.utf8</code>
		C		C

#1

In UTF-8 encoding, two character codes are used to represent each of the following symbols:

Yen sign (\): 0x5C or 0xC2A5

Tilde (~): 0x7E or 0xE280BE

JP1/IM - EG for NNMi uses character codes 0x5C and 0x7E for these symbols.

#2

Applicable to SUSE Linux only.

Environment variables file settings will be applied the next time you start up JP1/IM - EG for NNMi.

(2) Setting the language encoding in the common definitions

1. Edit the `jp1bs_param.conf` file of JP1/Base.

Use a text editor to open the `/etc/opt/jp1base/conf/jp1bs_param.conf` file. After `LANG=`, set a value for the LANG environment variable based on the table below.

Table 2–6: Values that can be specified for LANG in the `jp1bs_param.conf` file

OS			Language type in use	Value of LANG
Type	Language	Encoding		
Linux	Japanese	UTF-8	Japanese	UTF-8
		SJIS [#]		SJIS
	English	UTF-8	English	UTF-8
		C		C

#: Applicable to SUSE Linux only.

2. Stop JP1/IM - EG for NNMi.
3. Stop JP1/Base.
4. Execute the following command:
`/opt/jp1base/bin/jbssetcnf /etc/opt/jp1base/conf/jp1bs_param.conf`
5. Start JP1/Base.
6. Start JP1/IM - EG for NNMi.

2.4.3 Setting the definition files

To convert NNMi incidents into JP1 events and then use JP1/IM to manage and monitor them, you must set the definition files listed in the following table.

Table 2–7: Definition files to be set

Definition file name	Description
NNMi incident forwarding filter definition file	This file defines conditions for converting NNMi incidents acquired from NNMi into JP1 events.
Mapping definition file	This file defines mapping for displaying category and family labels (which are attributes of NNMi incidents) on the Event Details window of JP1/IM - View.
JP1/IM - Manager definition files	The following two definition files are used by JP1/IM - Manager: Definition file for extended event attributes This definition file is used to display the extended attributes specific to JP1/IM - EG for NNMi in the Event Details window of JP1/IM - View. Definition file for opening monitor windows This definition file is used to open NNMi windows from the Event Console window of JP1/IM - View.

Create the NNMi incident forwarding filter definition file and the mapping definition file by copying the sample files provided by JP1/IM - EG for NNMi.

The JP1/IM - Manager definition files are included in JP1/IM - Manager. Normally, there is no need to edit the included definition files. Edit these definition files only when it is necessary to add attributes to be displayed in the Event Details window of JP1/IM - View or change the Web browser to open NNMi windows.

For details about the settings in each definition file, see [4. Converting NNMi Incidents into JP1 Events](#).

2.4.4 Setting automatic startup and automatic termination

You must start the services of NNMi and JP1/Base before you can start the services of JP1/IM - EG for NNMi. The services of JP1/IM - EG for NNMi must be stopped before you stop the services of NNMi and JP1/Base.

If you set automatic startup and termination of JP1/IM - EG for NNMi, you can specify in advance the service start and termination sequences. Set automatic startup and termination when necessary.

The settings for automatic startup and termination depend on the OS.

(1) In Windows

In Windows, use JP1/Base's startup control to set automatic startup and termination of JP1/IM - EG for NNMi. Startup control starts and stops services according to a predefined sequence.

Setting automatic startup

You set automatic startup by specifying the definition of JP1/IM - EG for NNMi in JP1/Base's start sequence definition file (JP1SVPRM.DAT). The following shows the definition of JP1/IM - EG for NNMi:

```
[Jp1IMEGforNNMi]
Name=JP1/IM - EG for NNMi
ServiceName=JP1_IM-EG_for_NNMi
StopCommand=<JP1/IM - EG for NNMi Path>\bin\jegn_spmd_stop.exe
```

At the time of a new installation, these lines are commented out by inclusion of a hash mark (#) at the beginning of each line. Delete these hash marks.

The services are started in the order specified. If you edit the start sequence definition file, make sure that you enter the definition of JP1/IM - EG for NNMi after the definition of JP1/Base.

Setting automatic termination

In order to use JP1/Base's startup control to set automatic termination of JP1/IM - EG for NNMi, JP1/Power Monitor must be installed on the same computer. For details about JP1/Power Monitor, see the manual *Job Management Partner 1/Power Monitor Description, User's Guide and Reference*.

When JP1/Power Monitor is used to turn off the power, the services for which the termination command (StopCommand=) is specified are stopped in the reverse order of their startup among all the services specified in JP1/Base's start sequence definition file.

Express the termination command as an absolute path. It is specified as follows during the new installation:

```
StopCommand=JP1/IM-EG-for-NNMi-path\bin\jegn_spm�_stop.exe
```

Replace *JP1/IM-EG-for-NNMi-path* with the actual JP1/IM - EG for NNMi installation path. If the installation path contains a space, enclose character strings following StopCommand= in double-quotation marks (").

(2) In UNIX

In UNIX, use an automated startup script and an automated stop script to set automatic startup and termination of JP1/IM - EG for NNMi.

Setting automatic startup

Execute the following command to copy the automated startup script (jegn_start):

```
# cd /etc/opt/jpleg4nnmi
# cp -p jegn_start.model jegn_start
```

Further, when SELinux is enabled, you need to execute the following command to set the automated startup script (jegn_start) context type to bin_t:

```
# semanage fcontext -a -t bin_t '/etc/opt/jpleg4nnmi/jegn_start'
# restorecon -F /etc/opt/jpleg4nnmi/jegn_start
```

When you execute the above command, the automated startup script is called when the system starts and JP1/IM - EG for NNMi is started automatically. For details about the automated startup script, see *jegn_start (UNIX only)* in *7. Commands*.

Setting automatic termination

Execute the following command to copy the automated stop script (jegn_stop):

```
# cd /etc/opt/jpleg4nnmi
# cp -p jegn_stop.model jegn_stop
```

Further, when SELinux is enabled, you need to execute the following command to set the automated stop script (jegn_stop) context type to bin_t:

```
# semanage fcontext -a -t bin_t '/etc/opt/jpleg4nnmi/jegn_stop'
# restorecon -F /etc/opt/jpleg4nnmi/jegn_stop
```

When you execute the above command, the automated stop script is called when the system is terminated and JP1/IM - EG for NNMi is terminated automatically. For details about the automated stop script, see *jegn_stop (UNIX only)* in *7. Commands*.

In addition, C is set for the environment variable LANG by default in the automated startup script and automated stop script. To change the language of output messages when executing a script, edit the environment variable LANG line in the script.

When SELinux is enabled on Linux 8 or later, set the context type to bin_t for jegn_start and jegn_stop.

Setting example

```
# semanage fcontext -a -t bin_t '/etc/opt/jpleg4nnmi/jegn_start'  
# semanage fcontext -a -t bin_t '/etc/opt/jpleg4nnmi/jegn_stop'  
# restorecon -F /etc/opt/jpleg4nnmi/jegn_start  
# restorecon -F /etc/opt/jpleg4nnmi/jegn_stop
```

2.4.5 Settings for handling errors

JP1/IM - EG for NNMi provides various measures for handling errors in JP1/IM - EG for NNMi, such as a tool for collecting data needed for investigation of errors and a function for automatically restarting the process in the event of an abnormal process termination.

This subsection describes the settings for handling JP1/IM - EG for NNMi errors.

(1) Preparations for collecting data in the event of an error (Windows only)

If a JP1/IM - EG for NNMi process stops due to an application error, while the error dialog box is displayed, use the following procedure to collect a user dump:

1. Start Task Manager.

You can use either of the following procedures to start Task Manager:

- Right-click a blank area on the task bar and choose Task Manager.
- Press Ctrl + Shift + Esc keys to start Task Manager.

2. Click the Process tab.

3. Right-click the name of the JP1/IM - EG for NNMi process that was stopped by an application error, and then choose Create Dump File.

4. When a dialog box showing the user dump output destination path opens, collect a dump from there.

Important

If the error dialog box is closed, a normal dump cannot be collected, and consequently you will not be able to collect a user dump. If you closed the error dialog box by mistake (by clicking OK, for example) before collecting a user dump, reproduce the error and then collect a user dump.

(2) Preparations for collecting data in the event of an error (UNIX only)

JP1/IM - EG for NNMi provides a shell script (jegn_log.sh) as a tool for collecting data in the event of a problem. This tool enables you to collect data needed for resolving problems in batch mode.

The data collection tool of JP1/IM - EG for NNMi can collect troubleshooting data for JP1/IM - EG for NNMi and JP1/Base. For details about the data that can be collected, see [10.3 Data to be collected in the event of an error](#).

About the data collection tool

For details about the `jegn_log.sh` command, see *jegn_log.sh (UNIX only)* in Chapter 7.

In the event of a problem, you might need to obtain a core dump to facilitate investigation of the cause. Output of a core dump depends on the user environment settings. Check the settings described below.

(a) Setting the kernel parameters regarding core dump (Linux only)

In kernel parameter of Linux (`kernel.core_pattern`), when the output destination of core dump file is set to directory other than collection-target log file directory, or when the name of the core dump file is changed from the default setting, the data collection tool would not be able to acquire the core dump file when the tool is executed.

The data collection tool collects files whose file names start with `core` in the following default collection-target log file directories.

For physical hosts:

```
/var/opt/jp1eg4nnmi/log
```

For logical hosts:

```
shared-directory/jp1eg4nnmi/log
```

Depending on the setting of `kernel.core_pattern`, it might be necessary to check and address the following points before executing the data collection tool.

- When the output directory of a core dump file is changed
Make a copy of the core dump file in the default output directory.
- When the file name of a core dump file is changed
Change the file name of the core dump file to a name beginning with `core`.

(b) Setting ABRT for core dump files (Linux only)

In a Linux with Automatic Bug Reporting Tool (ABRT) installed, ABRT can be configured to allow limited processes, OS user accounts, or user groups to generate core dump files. In such a case, you cannot investigate problems because a core dump file might not be generated in case of core dump output events such as a segmentation failure in a JP1/IM - EG for NNMi process, a bus failure.

Depending on your operation, you should change the ABRT settings to ensure that processes or OS user accounts or user groups that run JP1/IM - EG for NNMi are allowed to generate core dump files. For details, see the documentation for your Linux.

(c) The systemd settings related to core dump files (Linux only)

These settings apply to Linux environments where the settings file for core dump file names (`/proc/sys/kernel/core_pattern`) begins with the character string `"|/usr/lib/systemd/systemd-coredump"`.

If the operation settings file for core dump files (`/etc/systemd/coredump.conf`) includes a setting that specifies that no core dump files are to be created, no core dump file will be output and users will not be able to investigate the failure in situations such as when a segmentation fault or a bus failure occurs in a JP1/IM - EG for NNMi process.

Based on operations to be performed, revise the settings in the operation settings file for core dump files (`/etc/systemd/coredump.conf`) so that core dump files are created. For details, see the documentation for your Linux.

(3) Settings for restarting after an abnormal process termination

A process is generated when JP1/IM - EG for NNMI starts. JP1/IM - EG for NNMI enables you to make settings so that the process will restart automatically after it has terminated abnormally for some reason.

To specify the settings for process restart after abnormal termination of the process:

1. Specify process restart.

Edit the extended startup process definition file (`jegn_service_0700.conf`). This file is stored at the following locations:

In Windows:

- Physical host: *EG-for-NNMi-path*\conf
- Logical host: *shared-folder*\JP1EG4NNMI\conf

In UNIX:

- Physical host: `/etc/opt/jpleg4nnmi/conf`
- Logical host: *shared-directory*/jpleg4nnmi/conf

The relevant parameter is the fourth value of the values separated by the vertical bar (`|`). Set either 0 (do not restart (default)) or 1 (restart). Do not change any other parameter values.

For details about the extended startup process definition file, see [F.1 Extended startup process definition file \(`jegn_service_0700.conf`\)](#).

2. Apply the settings.

Either restart JP1/IM - EG for NNMI or execute the `jegn_spmc_reload` command to apply the settings. For details about the `jegn_spmc_reload` command, see [jegn_spmc_reload](#) in [7. Commands](#).

3. Suppress error reporting to Microsoft (Windows only).

In the case of Windows, you must specify settings so that the Microsoft error reporting dialog box, which is displayed in the event of error detection, will not be displayed. This is because a process cannot restart if this dialog box is displayed.

1. In the **Run** text box, enter `gpedit.msc`, and then click **OK**.
2. In the Local Group Policy Editor, click **Computer Configuration, Administrative Templates, Windows Components**, and then **Windows Error Reporting**.
3. Right-click **Disable Windows Error Reporting** in the right pane of the window, and then select **Edit**.
4. In the settings window, select the **Enabled** radio button.
5. Click **OK**.

(4) Setting JP1 event issuance in the event of an abnormal process termination

JP1/IM - EG for NNMI enables you to issue JP1 events in the event of automatic recovery from a process error or abnormal termination. By issuing JP1 events, you can manage the error logs of JP1/IM - EG for NNMI itself.

To specify settings for JP1 event issuance:

1. Set JP1 event issuance.

Edit the JP1/IM - EG for NNMI parameter definition file (`jegn_param_v7.conf`). This file is stored at the following locations:

In Windows:

- Physical host: *EG-for-NNMi-path*\conf
- Logical host: *shared-folder*\JP1EG4NNMI\conf

In UNIX:

- Physical host: /etc/opt/jp1eg4nnmi/conf
- Logical host: *shared-directory*/jp1eg4nnmi/conf

In this file, `SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT` and `SEND_PROCESS_RESTART_EVENT` are the JP1 event issuance setting parameters. To issue JP1 events, change the values of these parameters to `dword:1`.

For details about the JP1/IM - EG for NNMI parameter definition file, see [F.2 JP1/IM - EG for NNMI parameter definition file \(jegn_param_V7.conf\)](#).

2. Execute the `jbssetcnf` command to apply the definition information.

For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

3. Restart JP1/IM - EG for NNMI.

The specified settings take effect after the restart.

3

Operation and Environment Configuration in a Cluster System

This chapter describes use of JP1/IM - EG for NNMi in a cluster system and the setup procedure. For an overview of cluster systems, see the *JP1/Base User's Guide*.

3.1 Environment setup procedure

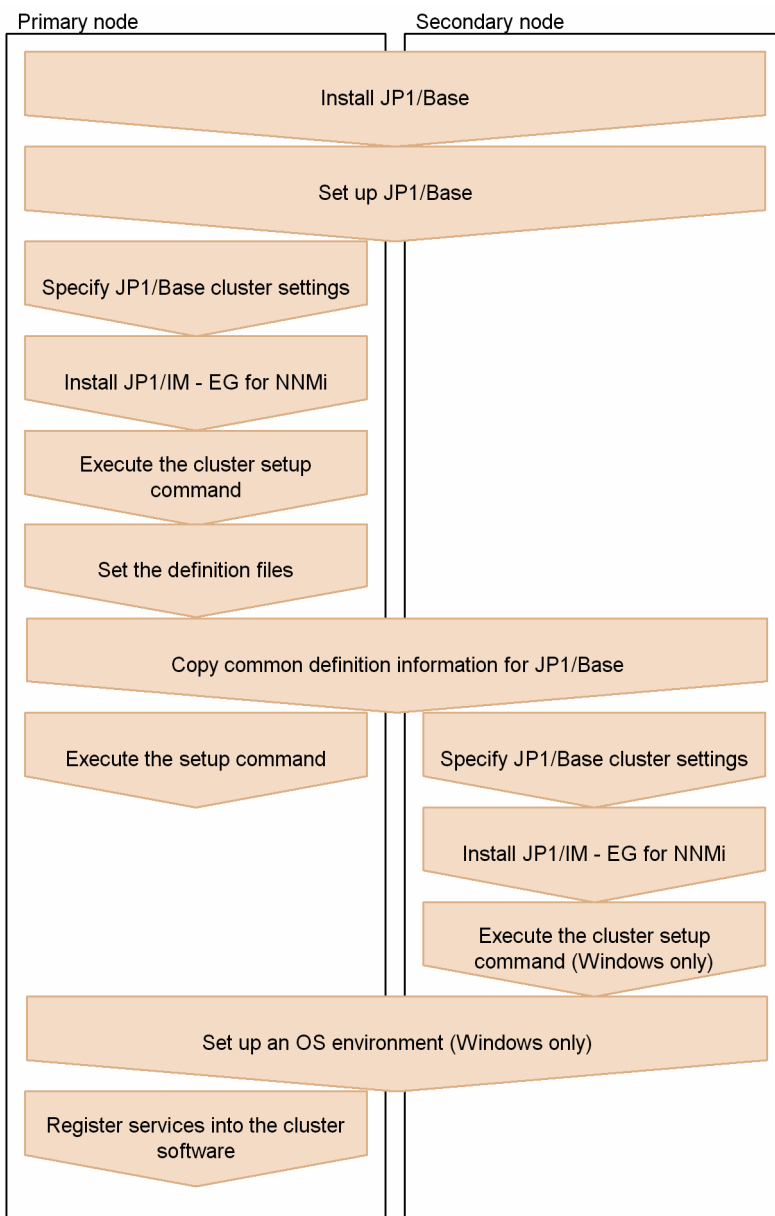
Use of JP1/IM - EG for NNMi in a cluster system is supported. When you use JP1/IM - EG for NNMi in a cluster system, processing can be inherited from the primary node to the secondary node in the event of a server failure.

If you intend to run JP1/IM - EG for NNMi in a cluster system, make sure in advance that operation of JP1/IM - EG for NNMi is supported by your cluster software.

This section describes the environment setup procedure for running JP1/IM - EG for NNMi in a cluster system.

You must have Administrator permissions in Windows and superuser permissions in UNIX in order to perform the installation and setup procedures.

Figure 3–1: Environment setup procedure (cluster operation)



Installing JP1/Base

For details about how to install and set up JP1/Base and how to specify cluster settings, see the *JP1/Base User's Guide*.

Installing NNMi

You can install NNMi at any time. However, if you intend to run JP1/IM - EG for NNMi in a cluster system, you must first install and set up NNMi. For details about how to set up NNMi, see the manuals and Release Notes for NNMi. At the time you set up JP1/IM - EG for NNMi, you will need the NNMi settings. For details about the NNMi settings that will be required during setup, see *Table 2-1 NNMi settings required during setup* in *2.1 Installation and setup procedures*.

3.2 Installing and setting up the logical host

This section describes installation and setup of the logical host for JP1/IM - EG for NNMi.

JP1/IM - EG for NNMi must run on the same logical host where NNMi and JP1/Base run.

Before you start the procedure, check the cluster system information shown in the table below.

Table 3–1: Items to be checked before you install and set up the logical host

Item to be checked	Description
Logical host name	Name of the logical host that executes the services of JP1/Base and NNMi
Logical IP address	IP address that corresponds to the logical host name
Shared folder (or shared directory)	Folder (or directory) on the shared disk that stores the file set for the JP1 execution environment on the logical host

For details about the prerequisites and the supported scope of cluster operation, see the *JP1/Base User's Guide*.

After you have finished checking these items, you can start installation and setup.

Important

- In Windows, install both the active server and the standby server on the same drive and in the same folders. Do not install the logical host on the shared disk.
- Before you set up JP1/IM - EG for NNMi in a cluster system, make sure that JP1/IM - EG for NNMi on the physical host has terminated. If you set up the cluster system while JP1/IM - EG for NNMi is running on the physical host, the logical host services will no longer function correctly. In such a case, you must restart the server to recover the system.

3.2.1 Installing and setting up the active server

To install and set up the active server:

1. Install and set up JP1/Base.

For details about how to install and set up JP1/Base, see the *JP1/Base User's Guide*.

2. Specify the cluster settings for JP1/Base.

Set the logical host for the primary node. For details about the procedure, see the *JP1/Base User's Guide*.

Note that you can specify a maximum of 32 bytes for the logical host name in the process forced termination command (`jegn_killall.cluster`) (applicable to UNIX only). A process cannot be terminated forcibly on a logical host whose name consists of more than 32 bytes.

3. Install JP1/IM - EG for NNMi.

For details about how to install JP1/IM - EG for NNMi, see [2.2 Installing \(in Windows\)](#) or [2.3 Installing \(in UNIX\)](#).

4. Set up an OS environment (Windows only).

In Windows, if either the Dr. Watson dialog box or the Microsoft error reporting dialog box is set to be displayed when an error occurs, failover of JP1/IM - EG for NNMi might fail. For this reason, you must suppress display of

these dialog boxes. For details about the suppression method, see [2.4.5\(3\) Settings for restarting after an abnormal process termination](#).

In the event of an error, you might need a memory dump and a crash dump in order to determine the cause of the error. To be prepared for such errors, we recommend that you set your system to output these dump files. For details about how to specify the settings, see [2.4.5\(1\) Preparations for collecting data in the event of an error \(Windows only\)](#) and [2.4.5\(2\) Preparations for collecting data in the event of an error \(UNIX only\)](#).

5. Execute the cluster setup command.

Execute the cluster setup command (`jegn_setup_cluster`) to set up an operating environment for JP1/IM - EG for NNMi during cluster operation.

```
jegn_setup_cluster -h logical-host-name -d shared-folder
```

Whenever you execute the `jegn_setup_cluster` command, the shared disk must be mounted.

For details about the `jegn_setup_cluster` command, see [jegn_setup_cluster](#) in [7. Commands](#).

Note:

Use the same time zone in a cluster system.

6. Set the definition files.

Set the following definition files:

- NNMi incident forwarding filter definition file
- Mapping definition file
- JP1/IM - Manager definition files

For details about the settings for the definition files, see [4. Converting NNMi Incidents into JPI Events](#).

7. Copy the common definition information for JP1/Base.

Copy the common definition information for JP1/Base from the active server to the standby server.

Execute the `jbsgetcnf` command of JP1/Base to back up the common definition information located on the active server.

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

For details about the `jbsgetcnf` command, see the [JPI/Base User's Guide](#).

8. Execute the setup command.

Execute the setup command (`jegn_setup`) to set up an operating environment for JP1/IM - EG for NNMi on the logical host.

For details about execution of the setup command, see [2.4.1 Executing the setup command](#). For details about the `jegn_setup` command, see [jegn_setup](#) in [7. Commands](#).

9. Register the services into the cluster software.

Register JP1/IM - EG for NNMi and JP1/Base on the logical host into the cluster software and then set them to be started and terminated by the cluster software. For details, see [3.3 Registering into the cluster software](#).

3.2.2 Installing and setting up the standby server

To install and set up the standby server:

1. Install and set up JP1/Base.

For details about how to install and set up JP1/Base, see the [JPI/Base User's Guide](#).

2. Copy the common definition information for JP1/Base.

Copy the common definition information for JP1/Base from the active server to the standby server.

Copy the common definition information that was backed up on the active server to the standby server using a method such as FTP. Use the `jbssetcnf` command of JP1/Base to set the common definition information in the backup file that was copied from the active server.

```
jbssetcnf backup-file-name
```

For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

3. Specify the cluster settings for JP1/Base.

Set the logical host at the secondary node. For details about the procedure, see the *JP1/Base User's Guide*.

4. Install JP1/IM - EG for NNMi.

For details about how to install JP1/IM - EG for NNMi, see [2.2 Installing \(in Windows\)](#) or [2.3 Installing \(in UNIX\)](#).

5. Set up an OS environment (Windows only).

In Windows, if either the Dr. Watson dialog box or the Microsoft error reporting dialog box is set to be displayed when an error occurs, failover of JP1/IM - EG for NNMi might fail. For this reason, you must suppress display of these dialog boxes. For details about the suppression method, see [2.4.5\(3\) Settings for restarting after an abnormal process termination](#).

In the event of an error, you might need a memory dump and a crash dump in order to determine the cause of the error. To be prepared for such errors, we recommend that you set your system to output these dump files. For details about how to specify the settings, see [2.4.5\(1\) Preparations for collecting data in the event of an error \(Windows only\)](#) and [2.4.5\(2\) Preparations for collecting data in the event of an error \(UNIX only\)](#).

6. Execute the cluster setup command (Windows only).

In Windows, execute the cluster setup command (`jegn_setup_cluster`) to set up an operating environment for JP1/IM - EG for NNMi during cluster operation.

```
jegn_setup_cluster -h logical-host-name
```

For details about the `jegn_setup_cluster` command, see [jegn_setup_cluster](#) in [7. Commands](#).

Note:

Use the same time zone in a cluster system.

3.2.3 Procedure for changing settings

In JP1/IM - EG for NNMi, if you change settings on the active server after operations have started in a cluster system, there is no need to change the settings on the standby server.

3.3 Registering into the cluster software

To use JP1/IM - EG for NNMi in a cluster operation, you must register JP1/IM - EG for NNMi and JP1/Base on the logical host into the cluster software and then set them to be started and terminated by the cluster software.

This section describes how to register JP1/IM - EG for NNMi and JP1/Base into the cluster software.

For details about how to register NNMi into the cluster software, see the manuals and Release Notes for NNMi. As for the start and stop sequence or dependencies between JP1/IM - EG for NNMi and NNMi, specify settings so that NNMi starts before JP1/IM - EG for NNMi starts and NNMi stops after JP1/IM - EG for NNMi stops.

The method for registering into the cluster software depends on the OS.

3.3.1 Registering into the cluster software (in Windows)

This subsection describes how to register JP1/IM - EG for NNMi and JP1/Base on the logical host into the cluster software in a Windows environment.

The following table shows the information to be registered into the cluster software.

Table 3–2: Information to be registered into the cluster software

No.	Name	Service name	Dependency
1	JP1/Base Event <i>logical-host-name</i>	JP1_Base_Event <i>logical-host-name</i>	IP address resource Physical disk resource
2	JP1/Base <i>logical-host-name</i>	JP1_Base_ <i>logical-host-name</i>	Cluster resource of No. 1
3	JP1/IM - EG for NNMi <i>logical-host-name</i>	JP1_IM-EG_for_NNMi_ <i>logical-host-name</i>	Cluster resources of NNMi and Nos. 1 and 2

For details about cluster resources of NNMi, see the NNMi manuals.

(1) Registering into the cluster software

Notes

- About restart of JP1
In the case of cluster operation, do not restart JP1 by JP1 process management. Restart JP1 by the cluster software.

(a) In MSCS

Register the services of JP1/IM - EG for NNMi and JP1/Base as MSCS resources. Set each resource as described below. Bold typeface indicates the MSCS setting items.

- For **Resource Types**, register as **Generic Service**.
- Set **Name**, **Dependencies**, and **Service name** as shown in *Table 3-2 Information to be registered into the cluster software*. **Name** is used to display the service, and **Service name** is used to specify the service that is controlled from MSCS.
- Do not set **Start parameters** and **Registry Replication**.
- Set the **Advanced properties** page for properties according to whether failover is to occur in the event of a JP1/IM - EG for NNMi failure.

For example, to set failover to occur in the event of a JP1/IM - EG for NNMi failure, select the **Restart** and **Affect the group** check boxes and specify **Threshold** for the restart retry count, using a value of 3 (times) as a guideline.

(b) When registering the service start and stop commands

Register into the cluster software the services of JP1/IM - EG for NNMi and JP1/Base to be started and stopped. For example, specify the settings so that the services shown in the *Name* column in *Table 3-2 Information to be registered into the cluster software* are to be started and stopped by the `net` command.

You can use the following commands to check the operation of JP1/IM - EG for NNMi and JP1/Base:

- `jegn_spmd_status`
Checks the operation of JP1/IM - EG for NNMi.
- `jbs_spmd_status`
Checks the operation of JP1/Base.
- `jevstat`
Checks the operation of the JP1/Base event service.

For details about the `jegn_spmd_status` command, see *jegn_spmd_status* in *7. Commands*. For details about the `jbs_spmd_status` and `jevstat` commands, see the *JP1/Base User's Guide*.

(2) Setting the resource start and stop sequence

To execute JP1/IM - EG for NNMi and JP1/Base on the logical host, the shared disk and logical IP address must be available for use.

Set the start and stop sequence or dependencies in such a manner that they are controlled by the cluster software as described below.

- When the logical host starts
 1. Allocate the shared disk and logical IP address and make them available for use.
 2. Start JP1/Base, NNMi and JP1/IM - EG for NNMi, in this order.
- When the logical host terminates
 1. Terminate JP1/IM - EG for NNMi, NNMi and JP1/Base, in this order.
 2. Release allocation of the shared disk and logical IP address.

3.3.2 Registering into the cluster software (in UNIX)

This subsection describes how to register JP1/IM - EG for NNMi and JP1/Base on the logical host into the cluster software in a UNIX environment.

(1) Creating scripts to be registered into the cluster software

When you use UNIX cluster software, you normally create a tool to control applications by a method such as scripts and then you register the scripts into the cluster software. In general, you need scripts to provide the *Start*, *Stop*, *Operation monitoring*, and *Forced stop* functions.

This subsection describes the JP1/IM - EG for NNMi information that is needed for designing scripts. Use this information to create scripts that control JP1/IM - EG for NNMi according to the cluster software specifications and then register the scripts into the cluster software.

Table 3–3: Detailed information needed for designing scripts for cluster registration

Function to be registered	Description
Start	<p>Starts JP1/IM - EG for NNMi.</p> <ul style="list-style-type: none"> • Command to be used <code>jegn_start.cluster logical-host-name</code> • Command termination timing The start command waits until JP1/IM - EG for NNMi has started before it terminates itself. However, if startup processing is not completed within the timeout period (60 seconds is the default), the command terminates without completing the startup processing. In such a case, the command terminates with the startup processing still underway (the command does not cancel the startup processing). • Checking the command execution result You can determine the JP1/IM - EG for NNMi startup result by means of the operation monitoring method described below. Normally, the result is determined by the cluster software's operation monitoring. The return values of the start command are 0 (normal termination) and 1 (argument error); therefore, result details cannot be determined from the return value.
Stop	<p>Terminates JP1/IM - EG for NNMi.</p> <ul style="list-style-type: none"> • Command to be used <code>jegn_stop.cluster logical-host-name</code> • Command termination timing The stop command waits until JP1/IM - EG for NNMi has terminated before it terminates itself. However, if stop processing is not completed within the timeout period (60 seconds is the default), the command terminates without completing the stop processing. In such a case, the command terminates with the stop processing still underway (the command does not cancel the stop processing). • Checking the command execution result You can determine the JP1/IM - EG for NNMi termination result by means of the operation monitoring method described below. The return values of the stop command are 0 (normal termination) and 1 (argument error); therefore, result details cannot be determined from the return value. <p>We recommend that you execute the forced termination command described below after the stop command has terminated. This enables you to terminate the process and prevent a failover error even in the event of a problem.</p>
Operation monitoring [#]	<p>Monitors normal operation of JP1/IM - EG for NNMi.</p> <p>To determine whether JP1/IM - EG for NNMi is running normally, check the return value of the <code>jegn_spm�_status</code> command. This command determines the status from the operating status of each process. Note that some cluster software does not provide the operation monitoring function. If there is no need to perform failover in the event of a JP1/IM - EG for NNMi failure, you need not register this function.</p> <ul style="list-style-type: none"> • Command to be used <code>jegn_spm�_status -h logical-host-name</code> • Checking the result of operation monitoring The following describes how to interpret the return value: Return value = 0 (all running): JP1/IM - EG for NNMi is running normally. Return value = 1 (error): An unrecoverable error has occurred. Treat this as an error. <i>Note:</i> If you execute the <code>jegn_spm�_status</code> command on the standby server whose shared disk is offline, the return value will be 1 because the shared disk is not available. Return value = 4 (partially stopped): Some JP1/IM - EG for NNMi processes are stopped due to a problem. Treat this as an error. Return value = 8 (all stopped):

Function to be registered	Description
Operation monitoring [#]	<p>The JP1/IM - EG for NNMi processes have all stopped due to a problem. Treat this as an error.</p> <p>Return value = 12 (retriable error):</p> <p>While the <code>jegn_spm�_status</code> command was checking the operating status, an error that can be recovered by retries has occurred. Retry checking of the operating status as many times as specified.</p>
Forced stop	<p>Forcibly terminates JP1/IM - EG for NNMi and releases the current resources.</p> <ul style="list-style-type: none"> Command to be used <p>The <code>jegn_killall.cluster</code> command forcibly terminates each process without performing JP1/IM - EG for NNMi termination processing.</p> <p><i>Note:</i></p> <p>Before you execute forced stop, use the stop command to terminate JP1/IM - EG for NNMi.</p>

#

With respect to JP1 operation checking, the same commands are used in both UNIX and Windows, but they function differently.

Windows operation differs from UNIX operation due to its association with Windows service control. In Windows, when any process terminates, JP1 process management automatically terminates all processes and places the service in stopped status. Assume such a service stop is the result of an error or assume an error has occurred when a command such as `jegn_spm�_status` returns a value of 8.

About restart of JP1

In the case of cluster operation, do not restart JP1 by JP1 process management. Restart JP1 by the cluster software.

(2) Setting the resource start and stop sequence

To execute JP1/IM - EG for NNMi and JP1/Base on the logical host, the shared disk and logical IP address must be available for use.

Set the start and stop sequence or dependencies in such a manner that they are controlled by the cluster software as described below.

- When the logical host starts
 - Allocate the shared disk and logical IP address and make them available for use.
 - Start JP1/Base, NNMi and JP1/IM - EG for NNMi, in this order.
- When the logical host terminates
 - Terminate JP1/IM - EG for NNMi, NNMi and JP1/Base, in this order.
 - Release allocation of the shared disk and logical IP address.

3.4 Deleting the logical host

This subsection describes how to delete the logical host. The logical host deletion procedure depends on the OS.

In Windows

Use the `jp1bshasetup` command of JP1/Base.

To delete the logical host:

1. Execute `jp1bshasetup.exe`.
2. In the Settings for Base Node Switching System window, click the **Delete Logical Host** button.
3. Select the name of the logical host that you want to delete.
4. Click the **Next** button.
5. Check that the deletion details are correct and click the **Finish** button.

In UNIX

Use the `jbsunsetcnf` command of JP1/Base. Execute the following command:

```
/opt/jp1base/bin/jbsunsetcnf -i -h logical-host-name
```

Note that when you delete the logical host, the logical hosts for JP1/Base and for those products that require JP1/Base are also deleted in the batch mode. When you delete only JP1/IM - EG for NNMi from a logical host, you must execute the following commands to delete common definitions on the primary node and the secondary node.

- [*logical-host-name*\JP1EG4NNMI\] key
`jbsunsetcnf -h logical-host-name -c JP1EG4NNMI`

If you are using Windows, execute the following command to delete the JP1/IM - EG for NNMi service from a logical host:

```
sc delete JP1_IM-EG_for_NNMI_logical-host-name
```

The `sc` command is a Windows command. For more details on the `sc` command, see documentation provided by Microsoft.

Shared files (shared folders) on the shared disk are not deleted; you must delete them manually.

For details about the `jp1bshasetup` and `jbsunsetcnf` commands, see the *JP1/Base User's Guide*.

3.5 Notes about cluster operation

The notes in this section apply to cluster operation.

- If you run multiple logical hosts concurrently in a cluster system, you need as many system resources as there are logical hosts running concurrently.
- If node switching occurs while a JP1 event is being issued, duplicate JP1 events might be registered.
- Before you uninstall JP1/IM - EG for NNMi in a cluster system, first delete the logical host.
For details, see [3.4 Deleting the logical host](#).

4

Converting NNMi Incidents into JP1 Events

This chapter describes the settings in the definition files that are used to convert NNMi incidents into JP1 events.

4.1 Creating an NNMi incident forwarding filter definition file

The *NNMi incident forwarding filter definition file* is used to specify conditions for converting NNMi incidents acquired from NNMi into JP1 events. This file defines the following information:

- Conditions for determining the NNMi incidents that are to be converted into JP1 events (filter conditions)
- Correspondences between NNMi incident attributes and JP1 event attributes (mapping conditions)

Only those NNMi incidents that satisfy the filter conditions are converted into JP1 events according to the specified mapping conditions and then registered into the event database of JP1/Base.

Creating an NNMi incident forwarding filter definition file

There is no NNMi incident forwarding filter definition file at the time of installation. You must copy the sample file, rename it, and then edit the sample definitions in the file. If you do not create an NNMi incident forwarding filter definition file, NNMi incidents will not be converted into JP1 events.

The name and storage location of the sample NNMi incident forwarding filter definition file are shown below.

File name

`imevtgw_nnmi_forward_filter.conf`
`imevtgw_nnmi_forward_filter.conf.sample` (sample file)

Storage location

In Windows:

- Physical host: *E-for-NNMi-path*\conf
- Logical host: *shared-folder*\JP1EG4NNMI\conf

In UNIX:

- Physical host: `/etc/opt/jpleg4nnmi/conf`
- Logical host: *shared-directory*/jpleg4nnmi/conf

Note

Each attribute value of an NNMi incident converted to a JP1 event reflects the value at the time that JP1/IM - EG for NNMi obtained the NNMi incident. Keep in mind that if any NNMi incident information is updated after the incident is converted to a JP1 event, the updated information will not be reflected with the JP1 event.

4.1.1 Format of the NNMi incident forwarding filter definition file

The NNMi incident forwarding filter definition file consists of the following two blocks:

- Filter condition block
This block specifies conditions for the NNMi incidents that are to be converted into JP1 events (filter conditions). Specification of a filter condition block is mandatory.
- Mapping block
This block specifies correspondences between NNMi incident attributes and JP1 event attributes (mapping conditions). Specification of a mapping block is optional.

The filter condition block and the mapping block constitute a forwarding condition block. When multiple forwarding condition blocks are specified in the NNMi incident forwarding filter definition file, comparison processing is performed

as specified in the file (from top down). If any condition in the forwarding condition block is satisfied, following comparison processing is not performed. If all conditions in the forwarding condition blocks are not satisfied, NNMI incidents are not converted into JP1 events.

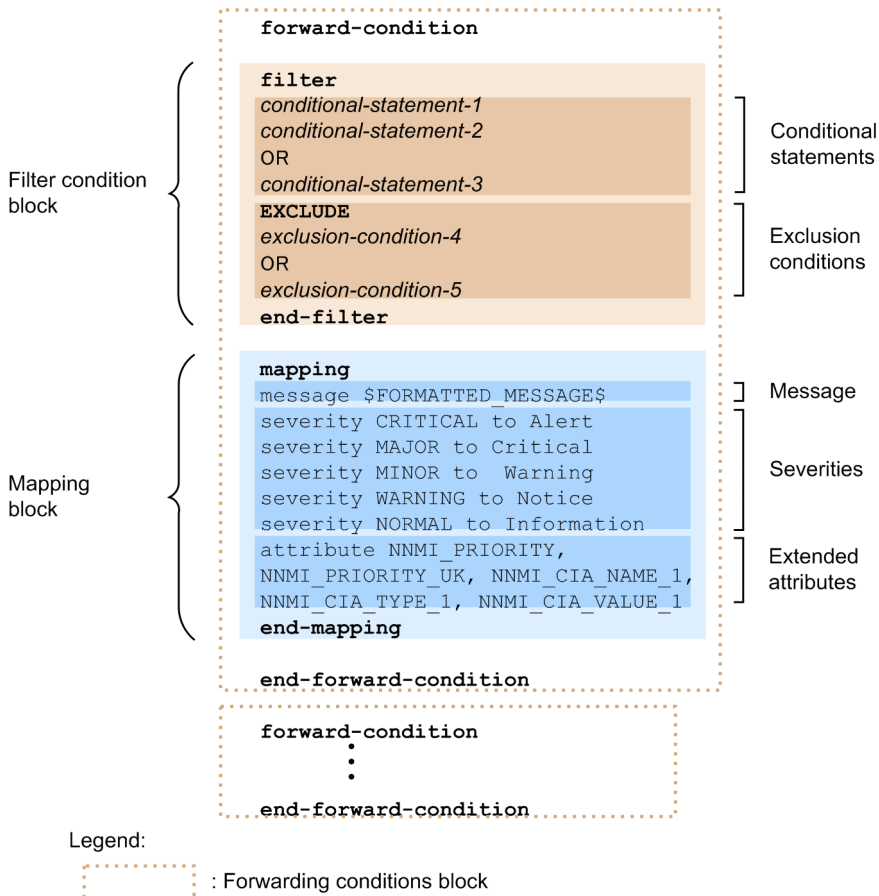
The following table shows the structure of an NNMI incident forwarding filter definition file.

Table 4–1: Structure of an NNMI incident forwarding filter definition file

Block		Setting item	Description
Forwarding condition block	Filter condition block	Conditional statement	Specifies a condition for determining NNMI incidents that are to be converted into JP1 events.
		Exclusion condition	Specifies a condition for determining NNMI incidents that are not to be converted into JP1 events.
	Mapping block	Message	Specifies the mapping of messages.
		Severity	Specifies the mapping of severities.
		Extended attribute	Specifies the mapping of extended attributes.

The following figure shows an example of an NNMI incident forwarding filter definition file.

Figure 4–1: Example of an NNMI incident forwarding filter definition file



forward-condition: Declares the beginning of a forwarding condition block.

filter: Declares the beginning of a filter condition block.

EXCLUDE: Indicates exclusion conditions.

`end-filter`: Declares the end of a filter condition block.

`mapping`: Declares the beginning of a mapping block.

`end-mapping`: Declares the end of a mapping block.

`end-forward-condition`: Declares the end of a forwarding condition block.

Rules for the NNMi incident forwarding filter definition file

The following rules apply to the NNMi incident forwarding filter definition file:

- The maximum size of the NNMi incident forwarding filter definition file is 10 megabytes.
- You can specify a maximum of 100 forwarding condition blocks.
- Do not specify multiple filter condition blocks or mapping blocks in a single forwarding condition block. An error results if one forwarding condition block contains multiple filter condition blocks or multiple mapping blocks.
- You can specify multiple conditions by using `OR` to link multiple conditional statements or exclusion conditions.
- Specify each message or extended attribute mapping setting on a single line without inserting a linefeed code.
- A line beginning with a hash mark (`#`) is treated as a comment line.

4.1.2 Defining a filter condition block

A filter condition block specifies filtering conditional statements for the NNMi incidents that are to be converted into JP1 events. The filtering conditional statements consist of conditional statements and exclusion conditions. Specification of a filter condition block is mandatory.

(1) Format of a filter condition block

Specify a filter condition block in the following format:

attribute-name Δ *operator* Δ *operand-1* Δ *operand-2* Δ . . .

Δ indicates one or more consecutive spaces or tabs.

- *attribute-name*
Specifies an attribute name of NNMi incidents.
- *operator*
Specifies a condition for filtering the NNMi incidents.
- *operand*
Specifies a value for filtering the NNMi incidents.

When the attribute value corresponding to the attribute name is compared with the value specified in the operand in a case sensitive manner, if the operator condition is satisfied, the filter condition is established.

For example, if you want to convert into JP1 events those NNMi incidents whose name (`NAME`) is `SNMPLinkDown`, specify the following filtering conditional statement:

```
NAME IN SNMPLinkDown
```

Details about the attribute names, operators, and operands are provided in the following subsections.

(2) Operators

The following table lists and describes the operators that can be specified in filtering conditional statements.

Table 4–2: Operators permitted in filtering conditional statements

Operator	Permitted number of operands	Condition
IN	One or more	The attribute's value matches the character string, integer, or date specified in an operand.
NOTIN	One or more	The attribute's value does not match the character string, integer, or date specified in any operand.
SUBSTR	One or more	The attribute's value contains a character string specified in an operand.
NOTSUBSTR	One or more	The attribute's value does not contain any of the character strings specified in an operand.
BEGIN	One or more	The attribute's value begins with one of the character strings specified in an operand.
REGEX #	One or more	The attribute's value matches one of the regular expressions specified in an operand. For details about the supported regular expressions, see <i>E. Regular Expressions</i> .
RANGE	Two	The attribute's value satisfies the condition: $operand-1 \leq attribute-value \leq operand-2$.

#

A regex that compares keywords can be used in filter conditional statements. Such expressions find perfect matches. As a result, when comparing prefixes, use a regular expression that allows the prefixes to be compared by, for example, adding a period followed by an asterisk (.*) after the regular expression.

(3) Operands

Specify in the operands the values to be used to filter the NNMi incidents; an operand value can be a character string, integer, or date.

This subsection explains special formats.

(a) When specifying two-digit hexadecimal numbers

An operand cannot contain a space, tab, CR, LF, or percent sign. However, except when the operator is REGEX, you can represent each of these items with a two-digit hexadecimal number in the format *%ASCII-code*, as shown below:

- Space: %20
- Tab: %09
- CR: %0d
- LF: %0a
- %: %25

Characters other than the above can also be expressed in the format *%ASCII-code* (2-digit hexadecimal number).

(b) When the data type of an attribute value is a date

If the data type of an attribute value is a date, specify the operand in the format shown in the table below.

Table 4–3: Operand format (for date type)

Operator	Format	Description
IN NOTIN	<ul style="list-style-type: none"> • <i>yyyyMMddHHmmssSSS</i> 	Specify a value in the range from 200001010000000000 to 20991231235959999 according to the locale of the OS.
RANGE	<ul style="list-style-type: none"> • <i>yyyyMMddHHmmssSSS</i> • <i>yyyyMMddHHmmss</i> • <i>yyyyMMddHHmm</i> • <i>yyyyMMddHH</i> • <i>yyyyMMdd</i> 	Specify a value in the range from 200001010000000000 to 20991231235959999 according to the locale of the OS.

Legend:

yyyy: Year (specify a value from 2000 to 2099)

MM: Month (specify a value from 01 to 12)

dd: Date (specify a value from 01 to 31)

HH: Hour (specify a value from 00 to 23)

mm: Minute (specify a value from 00 to 59)

ss: Second (specify a value from 00 to 59)

SSS: Millisecond (specify a value from 000 to 999)

If the operator is RANGE, the values following *yyyyMMdd* (year-month-date) can be omitted. If they are omitted, the values shown in the following table are set:

Operand	Hour (HH)	Minute (mm)	Second (ss)	Millisecond (SSS)
Operand 1	00	00	00	000
Operand 2	23	59	59	999

(4) Attributes of NNMi incidents

The table below lists the attributes of NNMi incidents and the operators that can be used in conjunction with those attributes. For details about the attributes, see the documentation for each NNMi product.

Table 4–4: Attributes of NNMi incidents and the operators that can be used

Attribute	Attribute name	Data type	Operator		
			IN NOTIN	SUBSTR NOTSUBSTR BEGIN REGEX	RANGE
Source	SRC_NAME	Character string	Y	Y	N
Source Type	SRC_TYPE	Character string	Y	Y	N
Source Node	SRC_NODE_NAME ^{#1}	Character string	Y	Y	N
Source Node (correlation conversion)	SRC ^{#1}	Character string	Y	N	N
Name	NAME	Character string	Y	Y	N
Severity	SEVERITY_UK ^{#2}	Character string	Y	N	Y ^{#3}
Priority	PRIORITY_UK ^{#2}	Character string	Y	N	Y ^{#3}

Attribute	Attribute name	Data type	Operator		
			IN NOTIN	SUBSTR NOTSUBSTR BEGIN REGEX	RANGE
Lifecycle State	LIFECYCLE_STATE_UK#2	Character string	Y	Y	N
Assigned To	ASSIGNED_TO	Character string	Y	Y	N
Category	CATEGORY_UK#2	Character string	Y	Y	N
Family	FAMILY_UK#2	Character string	Y	Y	N
Origin	ORIGIN_UK#2	Character string	Y	Y	N
Correlation Nature	NATURE_UK#2	Character string	Y	Y	N
Duplicate Count	DUPLICATE_COUNT	Integer	Y	N	Y
Message	FORMATTED_MESSAGE	Character string	Y	Y	N
Notes	NOTES	Character string	Y	Y	N
RCA Active	RCA_ACTIVE	Character string	Y	N	N
Origin Occurrence Time	ORIGIN_OCCUR_TIME	Date	Y	N	Y
First Occurrence Time	FIRST_OCCUR_TIME	Date	Y	N	Y
Last Occurrence Time	LAST_OCCUR_TIME	Date	Y	N	Y
Created	CREATED	Date	Y	N	Y
Last Update Time	MODIFIED	Date	Y	N	Y
Number of Custom Attributes	CIANUM	Integer	Y	N	Y
Custom Attribute Name	CIANAME_ \$n#4	Character string	Y	Y	N
Custom Attribute Type	CIATYPE_ \$n#4	Character string	Y	Y	N
Custom Attribute Value	CIAValue_ \$n#4	Character string	Y	Y	N

Legend:

- Y: Can be used
- N: Cannot be used

#1

When SRC is used in a conditional statement, correlation conversion is performed on the host name or IP address specified in the operand as required, and then the result is compared with the attribute value.

When SRC_NODE_NAME is used in a conditional statement, the host name or IP address specified in the operand is compared as is with the attribute value, without performing correlation conversion.

#2

The attribute value is predefined. For details about the attribute value, see (5) *Attribute values of NNMi incidents*.

#3

For the value range of Severity and Priority, see *SEVERITY_UK* and *PRIORITY_UK* in *Table 4-5 Attribute names, attribute values, and labels of NNMi incidents* in (5) *Attribute values of NNMi incidents*. The attribute values of *SEVERITY_UK* and *PRIORITY_UK* are listed in ascending order.

#4

\$n indicates the index of a custom attribute. It will be replaced with a number in the range from 1 to the number of custom attributes (CIANUM).

Example: In the case of the fourth custom attribute value, define as CIAVALUE_4.

(5) Attribute values of NNMi incidents

Some of the attributes of NNMi incidents have predefined attribute values (Unique Key). The following table lists the attribute names, attribute values, and display names (labels) in the NNMi windows of the attributes whose attribute values are predefined.

Table 4–5: Attribute names, attribute values, and labels of NNMi incidents

Attribute name	Attribute value (Unique Key)	Label
SEVERITY_UK	NORMAL	Normal
	WARNING	Warning
	MINOR	Minor
	MAJOR	Major
	CRITICAL	Critical
PRIORITY_UK	com.hp.nms.incident.priority.None	None
	com.hp.nms.incident.priority.Low	Low
	com.hp.nms.incident.priority.Medium	Medium
	com.hp.nms.incident.priority.High	High
	com.hp.nms.incident.priority.Top	Top
LIFECYCLE_STATE_UK	com.hp.nms.incident.lifecycle.Registered	Registered
	com.hp.nms.incident.lifecycle.InProgress	InProgress
	com.hp.nms.incident.lifecycle.Completed	Completed
	com.hp.nms.incident.lifecycle.Closed	Closed
CATEGORY_UK [#]	com.hp.nms.incident.category.Accounting	Accounting
	com.hp.nms.incident.category.Alert	Alert
	com.hp.nms.incident.category.Status	Status
	com.hp.nms.incident.category.Security	Security
	com.hp.nms.incident.category.Performance	Performance
	com.hp.nms.incident.category.Fault	Fault
	com.hp.nms.incident.category.Config	Config
	jp.co.Hitachi.soft.jp1.sso.incident.category.Resource	Resource
	jp.co.Hitachi.soft.jp1.sso.incident.category.Process	Process
	jp.co.Hitachi.soft.jp1.sso.incident.category.Service	Service
jp.co.Hitachi.soft.jp1.sso.incident.category.Applicat ion	Application	
FAMILY_UK [#]	com.hp.nms.incident.family.BGP	BGP
	com.hp.nms.incident.family.HSRP	HSRP
	com.hp.nms.incident.family.OSPF	OSPF

Attribute name	Attribute value (Unique Key)	Label
FAMILY_UK#	com.hp.nms.incident.family.RAMS	RAMS
	com.hp.nms.incident.family.RMON	RMON
	com.hp.nms.incident.family.RRP	RRP
	com.hp.nms.incident.family.STP	STP
	com.hp.nms.incident.family.Syslog	Syslog
	com.hp.nms.incident.family.VLAN	VLAN
	com.hp.nms.incident.family.VRRP	VRRP
	com.hp.nms.incident.family.Address	Address
	com.hp.nms.incident.family.Interface	Interface
	com.hp.nms.incident.family.ComponentHealth	Component Health
	com.hp.nms.incident.family.Chassis	Chassis
	com.hp.nms.incident.family.trap.Analysis	Trap Analysis
	com.hp.nms.incident.family.Node	Node
	com.hp.nms.incident.family.Board	Board
	com.hp.nms.incident.family.License	License
	com.hp.nms.incident.family.AggregatePort	Aggregate port
	com.hp.nms.incident.family.Connection	Connection
	com.hp.nms.incident.family.Correlation	Correlation
	jp.co.Hitachi.soft.jp1.sso.incident.family.SSO	SSO
	jp.co.Hitachi.soft.jp1.sso.incident.family.APM	APM
ORIGIN_UK	MANAGEMENTSOFTWARE	Management software
	MANUALLYCREATED	Manually created
	REMOTELYGENERATED	Remotely generated
	SNMPTRAP	SNMP trap
	SYSLOG	System log
	OTHER	Other
NATURE_UK	ROOTCAUSE	Root Cause
	SECONDARYROOTCAUSE	Secondary root cause
	SYMPTOM	Symptom
	STREAMCORRELATION	Stream Correlation
	NONE	None

#

If Category and Family have not only the NNMi-provided attribute values but also user-defined attribute values, you must create a mapping definition file. For details, see [4.2 Creating a mapping definition file](#).

(6) Examples of filter condition blocks

This subsection presents examples of filter condition blocks.

This example selects those NNMi incidents whose source node is `host1` (IP address is `10.0.0.1`):

```
SRC_NODE_NAME IN host1 10.0.0.1
or
SRC IN host1
or
SRC IN 10.0.0.1
```

This example selects those NNMi incidents whose message begins with `Hello, world`, where `%20` between `,` and `w` indicates a space:

```
FORMATTED_MESSAGE BEGIN Hello,%20world
```

This example selects those NNMi incidents whose source node is not `host2` (IP address is `10.0.0.2`) and whose name begins with `SNMP`:

```
SRC NOTIN host2
NAME BEGIN SNMP
```

This example selects those NNMi incidents that have `TASK_NAME` as the name of the second custom attribute and `Inventory_Management` as its value:

```
CIANAME_2 IN TASK_NAME
CIAVALUE_2 IN Inventory_Management
```

This example selects those NNMi incidents that occurred on or after January 1, 2010:

```
ORIGIN_OCCUR_TIME RANGE 20100101 20991231
```

This example selects the following NNMi incidents:

- NNMi incidents whose severity falls in the range from `MINOR` to `CRITICAL` and whose `Priority` is `Low`
- NNMi incidents whose priority is `Low` and whose `NAME` contains `Interface`

```
SEVERITY_UK RANGE MINOR CRITICAL
PRIORITY_UK NOTIN com.hp.nms.incident.priority.Low
OR
PRIORITY_UK IN com.hp.nms.incident.priority.Low
NAME SUBSTR Interface
```

This example selects those NNMi incidents whose category is `Fault` or `Security` or whose severity is `CRITICAL`, but excludes those NNMi incidents whose source node name is `host3` (IP address is `10.0.0.3`):

```
CATEGORY_UK IN
com.hp.nms.incident.category.Fault com.hp.nms.incident.category.Security
OR
SEVERITY_UK IN CRITICAL
EXCLUDE
SRC IN host3
```

4.1.3 Defining a mapping block

A mapping block specifies the correspondences between NNMi incident attributes and JP1 event attributes (mapping conditions). You can specify the following attributes in a mapping block:

- Message
- Severity
- Extended attribute

Specification of mapping blocks is optional.

(1) Message mapping

You can specify mapping of messages between NNMi incidents and JP1 events. The format of a message in a mapping block is as follows:

```
message $\Delta$ any-message
```

Δ indicates one or more consecutive spaces or tabs.

If message mapping is omitted, any message in an NNMi incident is mapped as is into a message in the JP1 event.

(a) Editing messages

A message cannot contain a space, tab, CR, LF, or percent sign. However, you can represent each of these items with a two-digit hexadecimal number in the format *%ASCII-code*, as shown below:

- Space: %20
- Tab: %09
- CR: %0d
- LF: %0a
- %: %25

Characters other than the above can also be expressed in the format *%ASCII-code* (2-digit hexadecimal number).

You can display the attribute value corresponding to an attribute name in a message by embedding the attribute name of the NNMi incident in the message. To display an attribute value, enclose the attribute name in dollar signs (\$) and then embed it in the message.

For example, if you want to display the severity and the source node name in addition to the message in the format *[severity] message (source-node-name)*, specify as follows:

```
message [$SEVERITY$] $FORMATTED_MESSAGE$ ($SRC_NODE_NAME$)
```

The following table lists the attribute names of the NNMi incidents that can be embedded in messages.

Table 4–6: Attribute names of NNMi incidents that can be embedded in messages

Attribute	Attribute name
Source	SRC_NAME
Source Type	SRC_TYPE

Attribute	Attribute name
Source Node	SRC_NODE_NAME
Name	NAME
Severity ^{#1}	SEVERITY
Priority ^{#1}	PRIORITY
Lifecycle State ^{#1}	LIFECYCLE_STATE
Assigned To	ASSIGNED_TO
Category ^{#1}	CATEGORY
Family ^{#1}	FAMILY
Origin ^{#1}	ORIGIN
Correlation Nature ^{#1}	NATURE
Duplicate Count	DUPLICATE_COUNT
Message	FORMATTED_MESSAGE
Notes	NOTES
RCA Active	RCA_ACTIVE
Origin Occurrence Time	ORIGIN_OCCUR_TIME
First Occurrence Time	FIRST_OCCUR_TIME
Last Occurrence Time	LAST_OCCUR_TIME
Created	CREATED
Last Update Time	MODIFIED
Number of Custom Attributes	CIANUM
Custom Attribute Name	CIANAME_ \$n ^{#2}
Custom Attribute Type	CIATYPE_ \$n ^{#2}
Custom Attribute Value	CIAValue_ \$n ^{#2}

#1

Displays the label, not the attribute value. For details about the labels, see *Table 4-5 Attribute names, attribute values, and labels of NNMi incidents in 4.1.2(5) Attribute values of NNMi incidents.*

#2

\$n indicates the index of a custom attribute. It will be replaced with a number in the range from 1 to the number of custom attributes (CIANUM).
Example: In the case of the fourth custom attribute value, define as CIAVALUE_4.

(b) Maximum size of a message

You can register a maximum of 1,023 bytes of a message as a JP1 event. If a message that is to be converted into a JP1 event exceeds 1,023 bytes, the excess portion of the message is discarded.

(2) Severity mapping

You can specify mapping of severities between NNMi incidents and JP1 events. The format of a severity in the mapping block is as follows:

severity Δ severity-of-NNMi-incident Δ to Δ severity-of-JP1-event

Δ indicates one or more consecutive spaces or tabs.

For example, if you want to map the severity CRITICAL of NNMi incidents to the severity Emergency of JP1 events, specify as follows:

```
severity CRITICAL to Emergency
```

If severity mapping is omitted, the severities are mapped as shown in the following table.

Table 4–7: Severity mapping (defaults)

NNMi incident	JP1 event
--	Emergency
CRITICAL	Alert
MAJOR	Critical
--	Error
MINOR	Warning
WARNING	Notice
NORMAL	Information
--	Debug

Legend:

--: Not applicable

Reference:

- The severity values are all case sensitive.
- The same NNMi incident severity value cannot be specified more than once. However, you can map multiple NNMi incident severity values into the same JP1 event severity value.

(3) Extended attribute mapping

If you want to add attributes specific to JP1/IM - EG for NNMi (extended attributes), you can specify mapping of extended attributes.

For details about the attributes of the JP1 events that are obtained by converting NNMi incidents, see [8.2 JP1 events obtained by converting NNMi incidents](#). You can add a maximum of 70 attributes whose *Mapping* column is Y in the attributes listed in [Table 8-1 Attributes of JP1 events obtained by converting NNMi incidents](#).

The following shows the format of extended attributes in the mapping block:

```
attribute $\Delta$ extended-attribute-name-1,  $\Delta$ extended-attribute-name-2,  $\Delta$ ...
```

Δ indicates one or more consecutive spaces or tabs.

For example, if you want to add the priority NNMI_PRIORITY as an extended attribute, specify as follows:

```
attribute NNMI_PRIORITY
```

If you omit mapping of extended attributes, extended attributes cannot be added.

(a) Total size of extended attributes

The maximum total size of the extended attributes that can be added is 10,000 bytes. Any extended attributes beyond byte 10,000 are not mapped. Therefore, select the extended attributes to be added so that their total size does not exceed 10,000 bytes.

You can use the following formula to determine the size of one extended attribute:

Size of extended attribute = Length of attribute name in characters + 1 + size of attribute value

For details about the sizes of attribute values, see *Table 8-1 Attributes of JP1 events obtained by converting NNMI incidents*. We recommend that you estimate the size of attribute values based on the maximum size. If the size is fixed or the maximum size is known, use that size.

Example:

The size of the priority (NNMI_PRIORITY) extended attribute is determined as follows:

$269 = 13$ (length of attribute name in characters) + 1 + 255 (maximum size of attribute value)

For example, if it is known that only those NNMI incidents whose priority attribute values are the highest (com.hp.nms.incident.priority.Top) are to be converted into JP1 events, you can use 32 as the size of the attribute value.

(b) Checking the result of extended attribute mapping

You can determine the result of extended attribute mapping by checking the attribute value of the NNMI_EM_RESULT extended attribute. The following explains the attribute values of the NNMI_EM_RESULT extended attribute:

ALL

Indicates that all the specified attributes have been added as JP1 event extended attributes. The result is also shown as ALL when there are no attributes to be added (extended attribute mapping has been omitted).

numeric-value

Indicates the number of attributes that have been added as JP1 event extended attributes. For example, if you issued a JP1 event with 10 attributes specified in the mapping block, and the attribute value of the NNMI_EM_RESULT extended attribute is 8, then the last two attributes specified in the mapping block were not added.

4.1.4 Definition example (sample file)

This subsection describes a definition example of an NNMI incident forwarding filter definition file based on using the sample file.

Shown below are the contents of the sample file. Note that line numbers are added for explanation purposes.

```
1 forward-condition
2 filter
3 #An incident whose severity level is MINOR or higher
4 SEVERITY_UK RANGE MINOR CRITICAL
5 end-filter
6 mapping
7 message $FORMATTED_MESSAGE$
8 severity CRITICAL to Alert
9 severity MAJOR to Critical
```



```
10 severity MINOR to Warning
11 severity WARNING to Notice
12 severity NORMAL to Information
13 end-mapping
14 end-forward-condition
```

Filter condition block (lines 2 to 5)

Those NNMi incidents whose severity (`SEVERITY_UK`) is in the range from `MINOR` to `CRITICAL` are to be converted into JP1 events.

Mapping block (lines 6 to 13)

- Message mapping (line 7)
Defines that messages in the NNMi incidents are to be mapped as is into messages in the JP1 events.
- Severity mapping (lines 8 to 12)
Defines severity mapping between NNMi incidents and JP1 events.

4.2 Creating a mapping definition file

You can display in the Event Details window the attribute value labels of the NNMI incident attributes Category and Family. The *mapping definition file* is used to specify the mapping needed to display these labels in the Event Details window.

You must create a mapping definition file when the attribute values of Category and Family include user-defined values in addition to the NNMI-provided attribute values. You must also define a mapping definition file when you want to display in the Event Details window labels that are different from the attribute value labels provided by NNMI.

4.2.1 Name and storage location of the mapping definition file

There is no mapping definition file at the time of installation. If you need to create a mapping definition file, you must copy the sample file, rename it, and then edit the sample definitions in the file.

The name and storage location of the sample mapping definition file are shown below.

File name

For Category

```
imevtgw_nnmi_label_mapping_category_en.conf  
imevtgw_nnmi_label_mapping_category_en.conf.sample (sample file)
```

For Family

```
imevtgw_nnmi_label_mapping_family_en.conf  
imevtgw_nnmi_label_mapping_family_en.conf.sample (sample file)
```

Storage location

In Windows:

- Physical host: *E-for-NNMi-path*\conf
- Logical host: *shared-folder*\JP1EG4NNMI\conf

In UNIX:

- Physical host: /etc/opt/jpleg4nnmi/conf
- Logical host: *shared-directory*/jpleg4nnmi/conf

4.2.2 Format of the mapping definition file

Following is the definition format used in the mapping definition file:

unique-key=label

The following example creates the attribute value `Hardware Failure` in NNMI:

- *label*: `Hardware Failure`
- *unique-key*: `com.hp.nms.incident.category.HardwareFault`

For this example, the following line is added to the mapping definition file:

```
com.hp.nms.incident.category.HardwareFault=Hardware Failure
```

When the above specification has been added, `Hardware Failure` will be displayed in the Event Details window of JP1/IM - View. If no mapping definition file is created, the unique key `com.hp.nms.incident.category.HardwareFault` is displayed.

The default labels provided by NNMi are displayed for the attribute values of Category and Family, unless a mapping definition file is created.

For details about the default attribute values (unique keys) and labels, see *CATEGORY_UK* and *FAMILY_UK* in [Table 4-5 Attribute names, attribute values, and labels of NNMi incidents](#) in [4.1.2\(5\) Attribute values of NNMi incidents](#).

Mapping definition file rules

The following rule applies to the mapping definition file:

- The maximum size of the mapping definition file is 10 megabytes.

4.3 Creating a custom attribute mapping definition file

This section describes the mapping of custom attributes.

If JP1/IM-EG for NNMI is connected to NNMI, the acquisition sequence of custom attributes might become indeterminate in JP1/IM-EG for NNMI when there are multiple custom attributes.

By using a custom attribute mapping definition file, the sequence of custom attribute mapping that is used in the NNMI incident forwarding filter definition file can be fixed.

Custom attribute mapping takes effect on the following attribute names defined in the NNMI incident forwarding filter definition file:

Custom attributes defined in filter condition blocks

```
CIANAME_ $n
CIATYPE_ $n
CIAVALUE_ $n
```

Custom attributes defined in message mapping

```
CIANAME_ $n
CIATYPE_ $n
CIAVALUE_ $n
```

Custom attributes defined in extended attribute mapping

```
NNMI_CIA_NAME_ $n
NNMI_CIA_TYPE_ $n
NNMI_CIA_VALUE_ $n
```

4.3.1 Name and storage location of the custom attribute mapping definition file

The custom attribute mapping definition file defines which sequence custom attributes are mapped in when JP1/IM-EG for NNMI handles the custom attributes of NNMI incidents.

You can establish correspondence between the index (\$n) of the JP1 event custom attribute and any NNMI incident custom attribute to determine the sequence of registering them.

There is no custom attribute mapping definition file at the time of installation. You must create a new custom attribute mapping definition file.

The name and storage location of the custom attribute mapping definition file are shown below.

File name

```
imevtgw_nnmi_cia_map.conf
```

Storage location

In Windows:

- Physical host: *E-for-NNMi-path*\conf
- Logical host: *shared-folder*\JP1EG4NNMI\conf

In UNIX:

- Physical host: `/etc/opt/jpleg4nnmi/conf`
- Logical host: `shared-directory/jpleg4nnmi/conf`

4.3.2 Format of the custom attribute mapping definition file

Specify a custom attribute mapping definition file in the following format:

Format

```
cia-map
name=NNMi-incident-name-1
cia_1=custom-attribute-name-1
cia_2=custom-attribute-name-2
...
cia-map-end
```

Information to be specified

`cia-map`

Indicates the beginning of the custom attribute mapping definition.

A custom attribute mapping definition continues to `cia-map-end`.

`name`

Defines the name of an NNMI incident. You must define an exact match character string that is case sensitive.

If two or more names are specified between `cia-map` and `cia-map-end`, the same mapping processing is executed at the time of the conversion of each NNMI incident name.

An error occurs if you specify the same name more than once in the entire custom attribute mapping definition file, not only between `cia-map` and `cia-map-end` but also in any other areas.

`cia_ $n`

Defines a custom attribute name to be set at the index `$n` of a custom attribute.

You must define an exact match character string that is case sensitive. `$n` specifies the numbers 1 to 28 and there is no need to specify consecutive numbers.

You can also define this item in random order. (Example: The definition of only `cia_15` is acceptable.)

If the same index `$n` is specified multiple times between `cia-map` and `cia-map-end`, search for a custom attribute name in the defined order and the matched attribute is mapped.

If you define this item as `cia_3=.1.3.6.1.2.1.2.2.1.1.2`, the name, type, and value of a custom attribute whose custom attribute name is `.1.3.6.1.2.1.2.2.1.1.2` are set in `NNMI_CIA_NAME_3`, `NNMI_CIA_TYPE_3`, and `NNMI_CIA_VALUE_3` respectively.

`cia-map-end`

Indicates the end of the custom attribute mapping definition.

A custom attribute mapping definition continues from `cia-map` to this item.

Example

```
1:  cia-map
2:  name=SNMPLinkUp
3:  cia_1=.1.3.6.1.2.1.2.2.1.1.2
4:  cia_2=cia.address
5:  cia-map-end
```

```
6:
7:  cia-map
8:  name=SNMPColdStart
9:  name=SNMPWarmStart
10:  cia_5=cia.address
11:  cia-map-end
```

Definitions in line 1 to line 5

When NNMi incidents whose name is `SNMPLinkUP` are converted, the name, type, and value of a custom attribute whose custom attribute name is `.1.3.6.1.2.1.2.2.1.1.2` are set in `NNMI_CIA_NAME_1`, `NNMI_CIA_TYPE_1`, and `NNMI_CIA_VALUE_1` respectively.

In the same way, the name, type, and value of a custom attribute whose custom attribute name is `cia.address` are set in `NNMI_CIA_NAME_2`, `NNMI_CIA_TYPE_2`, and `NNMI_CIA_VALUE_2` respectively.

Definitions in line 7 to line 11

When NNMi incidents whose name is `SNMPColdStart` or `SNMPWarmStart` are converted, the name, type, and value of a custom attribute whose custom attribute name is `cia.address` are set in `NNMI_CIA_NAME_5`, `NNMI_CIA_TYPE_5`, and `NNMI_CIA_VALUE_5` respectively.

When the definitions are applied

When you start a service or execute the reload command (`jegn_spmc_reload`), the settings take effect.

If an error occurs during service startup, the service fails to start.

If an error occurs when the reload command is executed, the changes are not applied and the system operates according to the definitions before the execution of the command.

Note

- A line beginning with a hash mark (#) is treated as a comment line.
- The maximum size of the custom attribute mapping definition file is 10 MB.

4.4 Editing the JP1/IM - Manager definition files

The following JP1/IM - Manager definition files are related to JP1/IM - EG for NNMi:

- Definition file for extended event attributes
This definition file is used to display product-specific extended attributes in the Event Details window of JP1/IM - View.
- Definition file for opening monitor windows
This definition file is used to open the windows of the products that are associated with the JP1 events displayed in JP1/IM - View.

The definition file for extended event attributes and the definition file for opening monitor windows for JP1/IM - EG for NNMi are required in order to display extended attributes associated specifically with JP1/IM - EG for NNMi in the Event Details window of JP1/IM - View and to open NNMi windows from JP1/IM - View.

These definition files are included in JP1/IM - Manager. *Normally, there is no need to edit the included definition files.*

If you want to add attributes to display in the Event Details window of JP1/IM - View, edit the definition file for extended event attributes. If you want to change the Web browser to open NNMi windows, edit the definition file for opening monitor windows.

For details about the definition file for extended event attributes and the definition file for opening monitor windows, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.4.1 Definition file for extended event attributes

This subsection describes the definition file for extended event attributes for JP1/IM - EG for NNMi.

(1) File name and storage location

The following shows the name and storage location of the definition files for extended event attributes for JP1/IM - EG for NNMi.

File name

```
hitachi_jp1_im_egn_attr_ja.conf  
hitachi_jp1_im_egn_attr_en.conf  
hitachi_jp1_im_egn_attr_zh.conf
```

Storage in JP1/IM - Manager

In Windows:

- Physical host: *Console-path*\conf\console\attribute
- Logical host: *shared-folder*\JP1Cons\conf\console\attribute

In UNIX:

- Physical host: /etc/opt/jp1cons/conf/console/attribute
- Logical host: *shared-directory*/jp1cons/conf/console/attribute

(2) Definition

The following shows the definitions in the definition file for extended event attributes for JP1/IM - EG for NNMI:

```
@file type="extended-attributes-definition", version="0300";
@product name="/HITACHI/JP1/IM/NNMI_INCIDENT";
@define-block type="event-attr-def";
block lang="Japanese", platform="base", extended="false";
attr name="E.NNMI_EM_RESULT", title="Result of Mapping";
attr name="E.NNMI_ID", title="Incident ID";
attr name="E.NNMI_UUID", title="Incident UUID";
attr name="E.NNMI_SRC_UUID", title="Source Object UUID";
attr name="E.NNMI_SRC_NAME", title="Source Object";
attr name="E.NNMI_SRC_TYPE", title="Source Type";
attr name="E.NNMI_SRC_NODE_UUID", title="Source Node UUID";
attr name="E.NNMI_SRC_NODE_NAME", title="Source Node";
attr name="E.NNMI_NAME", title="Name";
attr name="E.NNMI_SEVERITY", title="Severity of NNMI Incident";
attr name="E.NNMI_PRIORITY", title="Priority";
attr name="E.NNMI_LIFECYCLE_STATE", title="Lifecycle State";
attr name="E.NNMI_ASSIGNED_TO", title="Assigned To";
attr name="E.NNMI_CATEGORY", title="Category";
attr name="E.NNMI_FAMILY", title="Family";
attr name="E.NNMI_ORIGIN", title="Orign";
attr name="E.NNMI_NATURE", title="Correlation Nature";
attr name="E.NNMI_DUPLICATE_COUNT", title="Duplicate Count";
attr name="E.NNMI_FORMATTED_MESSAGE", title="Message";
attr name="E.NNMI_NOTES", title="Notes";
attr name="E.NNMI_RCA_ACTIVE", title="RCA Active";
attr name="E.NNMI_ORIGIN_OCCUR_TIME", title="Origin Occurrence Time", type="elapsed_time/date_format:CLIENT";
attr name="E.NNMI_ORIGIN_OCCUR_TIME_MS", title="Origin Occurrence Time(ms)";
attr name="E.NNMI_FIRST_OCCUR_TIME", title="First Occurrence Time", type="elapsed_time/date_format:CLIENT";
attr name="E.NNMI_FIRST_OCCUR_TIME_MS", title="First Occurrence Time(ms)";
attr name="E.NNMI_LAST_OCCUR_TIME", title="Last Occurrence Time", type="elapsed_time/date_format:CLIENT";
attr name="E.NNMI_LAST_OCCUR_TIME_MS", title="Last Occurrence Time(ms)";
attr name="E.NNMI_CREATED", title="Created", type="elapsed_time/date_format:CLIENT";
attr name="E.NNMI_CREATED_MS", title="Created(ms)";
attr name="E.NNMI_MODIFIED", title="Last Modified", type="elapsed_time/date_format:CLIENT";
attr name="E.NNMI_MODIFIED_MS", title="Last Modified(ms)";
attr name="E.NNMI_SEVERITY_UK", title="Severity UK of NNMI Incident ";
attr name="E.NNMI_PRIORITY_UK", title="Priority UK";
attr name="E.NNMI_LIFECYCLE_STATE_UK", title="Lifecycle State UK";
attr name="E.NNMI_CATEGORY_UK", title="Category UK";
attr name="E.NNMI_FAMILY_UK", title="Family UK";
attr name="E.NNMI_ORIGIN_UK", title="Origin UK";
attr name="E.NNMI_NATURE_UK", title="Correlation Nature UK";
attr name="E.NNMI_CIA_NUM", title="Number of Custom Attributes";
attr name="E.NNMI_CIA_NAME_1", title="Custom Attribute Name 1";
attr name="E.NNMI_CIA_NAME_2", title="Custom Attribute Name 2";
attr name="E.NNMI_CIA_NAME_3", title="Custom Attribute Name 3";
attr name="E.NNMI_CIA_NAME_4", title="Custom Attribute Name 4";
attr name="E.NNMI_CIA_NAME_5", title="Custom Attribute Name 5";
```



```
attr name="E.NNMI_CIA_NAME_6", title="Custom Attribute Name 6";
attr name="E.NNMI_CIA_NAME_7", title="Custom Attribute Name 7";
attr name="E.NNMI_CIA_NAME_8", title="Custom Attribute Name 8";
attr name="E.NNMI_CIA_NAME_9", title="Custom Attribute Name 9";
attr name="E.NNMI_CIA_NAME_10", title="Custom Attribute Name 10";
attr name="E.NNMI_CIA_NAME_11", title="Custom Attribute Name 11";
attr name="E.NNMI_CIA_NAME_12", title="Custom Attribute Name 12";
attr name="E.NNMI_CIA_NAME_13", title="Custom Attribute Name 13";
attr name="E.NNMI_CIA_NAME_14", title="Custom Attribute Name 14";
attr name="E.NNMI_CIA_NAME_15", title="Custom Attribute Name 15";
attr name="E.NNMI_CIA_NAME_16", title="Custom Attribute Name 16";
attr name="E.NNMI_CIA_NAME_17", title="Custom Attribute Name 17";
attr name="E.NNMI_CIA_NAME_18", title="Custom Attribute Name 18";
attr name="E.NNMI_CIA_NAME_19", title="Custom Attribute Name 19";
attr name="E.NNMI_CIA_NAME_20", title="Custom Attribute Name 20";
attr name="E.NNMI_CIA_TYPE_1", title="Custom Attribute Type 1";
attr name="E.NNMI_CIA_TYPE_2", title="Custom Attribute Type 2";
attr name="E.NNMI_CIA_TYPE_3", title="Custom Attribute Type 3";
attr name="E.NNMI_CIA_TYPE_4", title="Custom Attribute Type 4";
attr name="E.NNMI_CIA_TYPE_5", title="Custom Attribute Type 5";
attr name="E.NNMI_CIA_TYPE_6", title="Custom Attribute Type 6";
attr name="E.NNMI_CIA_TYPE_7", title="Custom Attribute Type 7";
attr name="E.NNMI_CIA_TYPE_8", title="Custom Attribute Type 8";
attr name="E.NNMI_CIA_TYPE_9", title="Custom Attribute Type 9";
attr name="E.NNMI_CIA_TYPE_10", title="Custom Attribute Type 10";
attr name="E.NNMI_CIA_TYPE_11", title="Custom Attribute Type 11";
attr name="E.NNMI_CIA_TYPE_12", title="Custom Attribute Type 12";
attr name="E.NNMI_CIA_TYPE_13", title="Custom Attribute Type 13";
attr name="E.NNMI_CIA_TYPE_14", title="Custom Attribute Type 14";
attr name="E.NNMI_CIA_TYPE_15", title="Custom Attribute Type 15";
attr name="E.NNMI_CIA_TYPE_16", title="Custom Attribute Type 16";
attr name="E.NNMI_CIA_TYPE_17", title="Custom Attribute Type 17";
attr name="E.NNMI_CIA_TYPE_18", title="Custom Attribute Type 18";
attr name="E.NNMI_CIA_TYPE_19", title="Custom Attribute Type 19";
attr name="E.NNMI_CIA_TYPE_20", title="Custom Attribute Type 20";
attr name="E.NNMI_CIA_VALUE_1", title="Custom Attribute Value 1";
attr name="E.NNMI_CIA_VALUE_2", title="Custom Attribute Value 2";
attr name="E.NNMI_CIA_VALUE_3", title="Custom Attribute Value 3";
attr name="E.NNMI_CIA_VALUE_4", title="Custom Attribute Value 4";
attr name="E.NNMI_CIA_VALUE_5", title="Custom Attribute Value 5";
attr name="E.NNMI_CIA_VALUE_6", title="Custom Attribute Value 6";
attr name="E.NNMI_CIA_VALUE_7", title="Custom Attribute Value 7";
attr name="E.NNMI_CIA_VALUE_8", title="Custom Attribute Value 8";
attr name="E.NNMI_CIA_VALUE_9", title="Custom Attribute Value 9";
attr name="E.NNMI_CIA_VALUE_10", title="Custom Attribute Value 10";
attr name="E.NNMI_CIA_VALUE_11", title="Custom Attribute Value 11";
attr name="E.NNMI_CIA_VALUE_12", title="Custom Attribute Value 12";
attr name="E.NNMI_CIA_VALUE_13", title="Custom Attribute Value 13";
attr name="E.NNMI_CIA_VALUE_14", title="Custom Attribute Value 14";
attr name="E.NNMI_CIA_VALUE_15", title="Custom Attribute Value 15";
attr name="E.NNMI_CIA_VALUE_16", title="Custom Attribute Value 16";
attr name="E.NNMI_CIA_VALUE_17", title="Custom Attribute Value 17";
attr name="E.NNMI_CIA_VALUE_18", title="Custom Attribute Value 18";
attr name="E.NNMI_CIA_VALUE_19", title="Custom Attribute Value 19";
attr name="E.NNMI_CIA_VALUE_20", title="Custom Attribute Value 20";
attr name="E.NNMI_PROTOCOL", title="NNMi Protocol";
attr name="E.NNMI_SERVER", title="NNMi Server";
attr name="E.NNMI_PORT", title="NNMi Port";
```

```

@define-block-end;
@define-block type="event-attr-group-def";
block platform="base", extended="false";
group name="_COMMON", attrs="E.NNMI_EM_RESULT|E.NNMI_ID|E.NNMI_UUID|
E.NNMI_SRC_UUID|E.NNMI_SRC_NAME|E.NNMI_SRC_TYPE|E.NNMI_SRC_NODE_UUID|
E.NNMI_SRC_NODE_NAME|E.NNMI_NAME|E.NNMI_SEVERITY|E.NNMI_PRIORITY|
E.NNMI_LIFECYCLE_STATE|E.NNMI_ASSIGNED_TO|E.NNMI_CATEGORY|E.NNMI_FAMILY|
E.NNMI_ORIGIN|E.NNMI_NATURE|E.NNMI_DUPLICATE_COUNT|E.NNMI_FORMATTED_MESSAGE|
E.NNMI_NOTES|E.NNMI_RCA_ACTIVE|E.NNMI_ORIGIN_OCCUR_TIME|
E.NNMI_ORIGIN_OCCUR_TIME_MS|E.NNMI_FIRST_OCCUR_TIME|
E.NNMI_FIRST_OCCUR_TIME_MS|E.NNMI_LAST_OCCUR_TIME|E.NNMI_LAST_OCCUR_TIME_MS|
E.NNMI_CREATED|E.NNMI_CREATED_MS|E.NNMI_MODIFIED|E.NNMI_MODIFIED_MS|
E.NNMI_SEVERITY_UK|E.NNMI_PRIORITY_UK|E.NNMI_LIFECYCLE_STATE_UK|
E.NNMI_CATEGORY_UK|E.NNMI_FAMILY_UK|E.NNMI_ORIGIN_UK|E.NNMI_NATURE_UK|
E.NNMI_CIA_NUM|E.NNMI_CIA_NAME_1|E.NNMI_CIA_NAME_2|E.NNMI_CIA_NAME_3|
E.NNMI_CIA_NAME_4|E.NNMI_CIA_NAME_5|E.NNMI_CIA_NAME_6|E.NNMI_CIA_NAME_7|
E.NNMI_CIA_NAME_8|E.NNMI_CIA_NAME_9|E.NNMI_CIA_NAME_10|E.NNMI_CIA_NAME_11|
E.NNMI_CIA_NAME_12|E.NNMI_CIA_NAME_13|E.NNMI_CIA_NAME_14|E.NNMI_CIA_NAME_15|
E.NNMI_CIA_NAME_16|E.NNMI_CIA_NAME_17|E.NNMI_CIA_NAME_18|E.NNMI_CIA_NAME_19|
E.NNMI_CIA_NAME_20|E.NNMI_CIA_TYPE_1|E.NNMI_CIA_TYPE_2|E.NNMI_CIA_TYPE_3|
E.NNMI_CIA_TYPE_4|E.NNMI_CIA_TYPE_5|E.NNMI_CIA_TYPE_6|E.NNMI_CIA_TYPE_7|
E.NNMI_CIA_TYPE_8|E.NNMI_CIA_TYPE_9|E.NNMI_CIA_TYPE_10|E.NNMI_CIA_TYPE_11|
E.NNMI_CIA_TYPE_12|E.NNMI_CIA_TYPE_13|E.NNMI_CIA_TYPE_14|E.NNMI_CIA_TYPE_15|
E.NNMI_CIA_TYPE_16|E.NNMI_CIA_TYPE_17|E.NNMI_CIA_TYPE_18|E.NNMI_CIA_TYPE_19|
E.NNMI_CIA_TYPE_20|E.NNMI_CIA_VALUE_1|E.NNMI_CIA_VALUE_2|E.NNMI_CIA_VALUE_3|
E.NNMI_CIA_VALUE_4|E.NNMI_CIA_VALUE_5|E.NNMI_CIA_VALUE_6|E.NNMI_CIA_VALUE_7|
E.NNMI_CIA_VALUE_8|E.NNMI_CIA_VALUE_9|E.NNMI_CIA_VALUE_10|
E.NNMI_CIA_VALUE_11|E.NNMI_CIA_VALUE_12|E.NNMI_CIA_VALUE_13|
E.NNMI_CIA_VALUE_14|E.NNMI_CIA_VALUE_15|E.NNMI_CIA_VALUE_16|
E.NNMI_CIA_VALUE_17|E.NNMI_CIA_VALUE_18|E.NNMI_CIA_VALUE_19|
E.NNMI_CIA_VALUE_20|E.NNMI_PROTOCOL|E.NNMI_SERVER|E.NNMI_PORT";
@define-block-end;
@define-block type="event-attr-order-def";
block platform="base", extended="false";
order id="00006100", attrs="_COMMON";
@define-block-end;

```

(3) Displaying internal attributes in the Event Details window

If the version of JP1/IM - Manager is 11-10 or earlier, because the internal attributes of NNMI incidents are not normally used during operation, the default is that these attributes are not displayed in the Event Details window of JP1/IM - View even when they are converted into JP1 events.

If you wish to display these internal attributes, place the JP1/IM - EG for NNMI definition files for extended event attributes under JP1/IM - Manager.

Storage in JP1/IM - EG for NNMI

In Windows:

installation folder\conf\event

In UNIX:

/etc/opt/jpleg4nnmi/conf/event

File name

hitachi_jp1_im_egn_attr_ja.conf

hitachi_jp1_im_egn_attr_en.conf

hitachi_jpl_im_egn_attr_zh.conf

(4) Displaying custom attributes in the Event Details window

If the custom attributes listed below are converted into JP1 events, the default is that \$n is displayed in the Event Details window of JP1/IM - View for a maximum of 20 attributes:

- Custom Attribute Name (NNMI_CIA_NAME_\$n)
- Custom Attribute Type (NNMI_CIA_TYPE_\$n)
- Custom Attribute Value (NNMI_CIA_VALUE_\$n)

To display attributes whose \$n value is greater than 20, you must add appropriate definitions in the definition block for extended event attributes and the definition block for attribute groups in the definition file for extended event attributes.

Furthermore, when adding definitions to a definition file for extended event attributes, you must add definitions to the definition files for extended event attributes for all languages. If you have not added the definitions to the definition files for extended event attributes for some languages, the definitions will not be enabled. Also, since the definition file for extended event attributes is updated when performing an overwrite installation for JP1/IM - Manager, if you have edited the definition file for extended event attributes, you should remove it before the overwrite installation then replace it after the overwrite installation.

For details about how to edit the definition file for extended event attributes, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.4.2 Definition file for opening monitor windows

This subsection describes the definition file for opening monitor windows for JP1/IM - EG for NNMi.

(1) File name and storage location

The following shows the name and storage location of the definition file for opening monitor windows for JP1/IM - EG for NNMi.

File name

hitachi_jpl_im_egn_mon.conf

Storage in JP1/IM - Manager

In Windows:

- Physical host: *Console-path*\conf\console\monitor
- Logical host: *shared-folder*\JP1Cons\conf\console\monitor

In UNIX:

- Physical host: /etc/opt/jplcons/conf/console/monitor
- Logical host: *shared-directory*/jplcons/conf/console/monitor

(2) Definition

The following shows the definitions in the definition file for opening monitor windows for JP1/IM - EG for NNMi:

```
DESC_VERSION=0300
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/IM/NNMI_INCIDENT EVENT_ID=00006100 INTERFA
CE=NNMI_VIEW_WEB
DEF_MTR_CALL_NAME=NNMI_VIEW_WEB EXEC_ID=default_browser
PATH="%IM_EVC_PARAMETER_1%:/%IM_EVC_PARAMETER_2%:%IM_EVC_PARAMETER_3%/
nnm/launch?cmd=showForm&objtype=Incident&menus=true&objuuid=
%IM_EVC_PARAMETER_4%" PARAM=E.NNMI_PROTOCOL,E.NNMI_SERVER,E.NNMI_PORT,
E.NNMI_UUID
```

(3) Changing the Web browser to open NNMI windows

To change the Web browser to open NNMI windows:

1. In JP1/IM - Manager's definition file for executing applications, specify the path for the executable file of the Web browser that is used by NNMI and the ID for linking from other definition files.
2. Register the ID specified in the definition file for executing applications into the EXEC_ID argument in the definition file for opening monitor windows.

For details, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5

Startup and Termination

This chapter describes how to start and terminate JP1/IM - EG for NNMi.

5.1 Starting JP1/IM - EG for NNMi

This section describes how to start JP1/IM - EG for NNMi. You must start the services of NNMi and JP1/Base before you can start the JP1/IM - EG for NNMi services.

Automatic startup in a cluster system

For details about starting JP1/IM - EG for NNMi automatically in a cluster system, see [3.3 Registering into the cluster software](#).

The startup method depends on the OS.

5.1.1 In Windows

In Windows, the procedure depends on whether JP1/Base's startup control is used.

When startup control is used to start JP1/IM - EG for NNMi

Specify the definition of JP1/IM - EG for NNMi in the start sequence definition file of JP1/Base. For details, see [2.4.4\(1\) In Windows](#).

When startup control is not used to start JP1/IM - EG for NNMi

From **Control Panel**, choose **Administrative Tools** and then **Services**, and then start the services of JP1/IM - EG for NNMi.

5.1.2 In UNIX

In UNIX, the procedure depends on whether an automated startup script is used.

When an automated startup script is used to start JP1/IM - EG for NNMi

Specify settings so that an automated startup script is called during system startup. For details, see [2.4.4\(2\) In UNIX](#).

When an automated startup script is not used to start JP1/IM - EG for NNMi

Execute the `/etc/opt/jpleg4nnmi/jegn_start.model` script or a file that contains a copy of this script.

Important

If automatic startup and automatic termination are set in Linux 7, Oracle Linux 7, CentOS 7, or SUSE Linux 12, execute the following command to start JP1/IM - EG for NNMi:

```
systemctl start jp1_eg4nnmi
```

5.2 Terminating JP1/IM - EG for NNMi

This section describes how to terminate JP1/IM - EG for NNMi. You must terminate the JP1/IM - EG for NNMi services before you terminate the services of NNMi and JP1/Base.

Automatic termination in a cluster system

For details about terminating JP1/IM - EG for NNMi automatically in a cluster system, see [3.3 Registering into the cluster software](#).

The termination method depends on the OS.

5.2.1 In Windows

In Windows, the procedure depends on whether JP1/Base's startup control is used.

When startup control is used to start JP1/IM - EG for NNMi

If JP1/Power Monitor has been installed, you can use JP1/Base's startup control to stop the service. If you use startup control, specify the definition of JP1/IM - EG for NNMi in the start sequence definition file of JP1/Base. For details, see [2.4.4\(1\) In Windows](#).

When startup control is not used to terminate JP1/IM - EG for NNMi

From **Control Panel**, choose **Administrative Tools** and then **Services**, and then stop the services of JP1/IM - EG for NNMi.

5.2.2 In UNIX

In UNIX, the procedure depends on whether an automated stop script is used.

When an automated stop script is used to terminate JP1/IM - EG for NNMi

Specify settings so that an automated stop script is called during system termination. For details, see [2.4.4\(2\) In UNIX](#).

When an automated stop script is not used to terminate JP1/IM - EG for NNMi

Execute the `/etc/opt/jpleg4nnmi/jegn_stop.model` script or a file that contains a copy of this script.

Important

If automatic startup and automatic termination are set in Linux 7 or later, Oracle Linux 7 or later, or SUSE Linux 12 or later, execute the following command to terminate JP1/IM - EG for NNMi:

```
systemctl stop jpl_eg4nnmi
```

6

JP1/IM - EG for NNMi Operations

This chapter describes backup and restoration of JP1/IM - EG for NNMi and how to change settings.

6.1 Backup and restoration

This section describes backup and restoration of JP1/IM - EG for NNMi.

If a problem occurs in JP1/IM - EG for NNMi and you have made a backup of the settings, you can configure the system in the same environment and restart operation. Immediately after you set up JP1/IM - EG for NNMi and whenever you make changes to the system, it is important that you make a backup of the settings.

For details about backing up and restoring NNMi, see the documentation for the NNMi product.

6.1.1 Managing the configuration information

The restoration here means to return the files to the state when their backups were taken. Note that the backup and restoration process described in this section is not available for duplication between servers and file migration.

When you perform backup and restoration, all of the following items must match on the backup source and the restoration destination:

- Host name
- IP address
- PP model name
- PP version (match the format of *VVRRZZ*)
- Directory structure used by the product (permissions and the like must match)

It is assumed that OS and hardware on the source and the destination are able to perform the same operations.

If the above conditions are not met, you will need to move files.

OS commands or backup software can be used for a full backup of the entire system. However, we recommend that you back up or restoration data by using the commands provided with individual JP1/IM - EG for NNMi functions that do not depend on the OS commands or backup software. If you use OS commands or backup software, the following conditions must be met:

- Data is backed up when all JP1/IM - EG for NNMi services, including the IM database, have been stopped.
- Data is backed up when all file and registry information, including the information registered in the OS, is consistent.
- The backup target files are not sparse files.

6.1.2 Backing up the settings

(1) Backing up JP1/IM - EG for NNMi setup information

This subsection describes backup of the JP1/IM - EG for NNMi settings.

Whenever you make a backup of JP1/IM - EG for NNMi, you should also make a backup of JP1/Base. For details about backing up the definition files set by the JP1/Base user, see the *JP1/Base User's Guide*.

You can use any appropriate method to make a backup, such as by copying the files. You can make a backup while JP1/IM - EG for NNMi is running.

The following table lists the JP1/IM - EG for NNMI files to be backed up.

Table 6–1: JP1/IM - EG for NNMI files to be backed up

File name	Description
<code>imevtgw_nnmi.conf</code>	Operation definition file
<code>imevtgw_nnmi_cia_map.conf</code>	Custom attribute mapping definition file [#]
<code>imevtgw_nnmi_forward_filter.conf</code>	NNMI incident forwarding filter definition file
<code>imevtgw_nnmi_label_mapping_category_en.conf</code>	Mapping definition file (for category)
<code>imevtgw_nnmi_label_mapping_family_en.conf</code>	Mapping definition file (for family)

#

If custom attribute mapping is not set, this file does not exist.

The files to be backed up are stored at the following locations:

In Windows:

- Physical host: *EG-for-NNMI-path*\conf
- Logical host: *shared-folder*\JP1EG4NNMI\conf

In UNIX:

- Physical host: */etc/opt/jp1eg4nnmi/conf*
- Logical host: *shared-directory/jp1eg4nnmi/conf*

(2) Backing up common definition information

JP1/IM - EG for NNMI, 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/IM - EG for NNMI:

```
jbsgetcnf -c JP1EG4NNMI > backup-file
```

When you run JP1/Base in a cluster system, execute the following command to acquire only the common definition information for JP1/IM - EG for NNMI:

```
jbsgetcnf -h logical-host-name -c JP1EG4NNMI > 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.

6.1.3 Restoring the settings

(1) Restoring JP1/IM - EG for NNMi setup information

This subsection describes restoration of the JP1/IM - EG for NNMi settings.

Before you restore from a backup of JP1/IM - EG for NNMi, you must first restore JP1/Base. Prior to restoring backup files to their original locations, make sure that all the following conditions are satisfied:

Conditions

- JP1/IM - EG for NNMi and JP1/Base have both been terminated.
- JP1/IM - EG for NNMi and JP1/Base were both installed and the cluster setup command has already been executed (applicable in the case of cluster operation).
- JP1/Base was set up in a logical host environment (applicable in the case of cluster operation).
- The shared disk is online (applicable in the case of cluster operation).

(2) Restoring common definition information

In addition to restoring backup files, you must also restore common definition information.

To restore common definition information on a set-up host, execute the following command to temporarily delete the common definition information for JP1/IM - EG for NNMi.

Physical host:

```
jbsunsetcnf -i -h JP1_DEFAULT -c JP1EG4NNMI
```

Logical host:

```
jbsunsetcnf -i -h logical-host-name -c JP1EG4NNMI
```

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-6.1.2(2)
```

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.

6.2 Changing settings

This section describes how to edit the definition files for JP1/IM - EG for NNMi and the procedures required in order to change the system environment for the computer on which JP1/IM - EG for NNMi is running.

If you have changed the NNMi system environment, you must execute `overwrite setup`; for details, see [2.4.1 Executing the setup command](#).

6.2.1 Editing the definition files

You can edit the following definition files for JP1/IM - EG for NNMi (this editing can be performed while the services of JP1/IM - EG for NNMi are running):

- Operation definition file[#]
- NNMi incident forwarding filter definition file
- Mapping definition file (for category)
- Mapping definition file (for family)
- Extended startup process definition file

#

You cannot edit the operation definition file directly. Instead, you must use the `jegn_setup` command to edit it. For details about the `jegn_setup` command, see [jegn_setup](#) in *7. Commands*.

If you have edited any of the definition files listed above while the JP1/IM - EG for NNMi services were running, you must execute the `jegn_spmd_reload` command to reload the definition files in order to apply the changes. The changes in the definition files are not applied immediately after execution of the `jegn_spmd_reload` command, but they are applied when the next Acquiring of NNMi incidents occurs after the reload.

If an error occurs while the `jegn_spmd_reload` command checks the definition, operations continue using the definitions that were in effect before the change. For details about the `jegn_spmd_reload` command, see [jegn_spmd_reload](#) in *7. Commands*.

For details about the settings in the definition files, see [4. Converting NNMi Incidents into JPI Events](#) and [F.1 Extended startup process definition file \(jegn_service_0700.conf\)](#).

Reference:

If you edit definition files while the JP1/IM - EG for NNMi services are stopped, the new settings take effect the next time the services are started.

6.2.2 Changing the settings of the host name, IP address, and port number on which JP1/IM - EG for NNMi is running

This subsection describes the procedures for changing the settings of the host name, IP address, and port number on which JP1/IM - EG for NNMi is running.

For details about how to change the JP1/Base settings, see the *JPI/Base User's Guide*.

(1) Procedure for changing the host name, IP address, or port number

To change the host name, IP address, or port number:

1. Terminate JP1/IM - EG for NNMi.
2. Change the host name, IP address, or port number, as necessary.
3. Restart JP1/IM - EG for NNMi.

(2) Procedure for editing the hosts file, jp1hosts definition file, and jp1hosts2 definition file

This subsection describes how to change the host information specified in the `hosts` file, `jp1hosts` definition file, or `jp1hosts2` definition file while JP1/IM - EG for NNMi is running.

Changing information of a host on which JP1/IM - EG for NNMi is installed

After you have changed the host information, restart JP1/IM - EG for NNMi.

Adding or changing information of a host on which JP1/IM - EG for NNMi is not installed

If you have added or changed host information, you must either restart JP1/IM - EG for NNMi or execute the `jegn_spmd_reload` command to reload the new settings. For details about the `jegn_spmd_reload` command, see *jegn_spmd_reload* in *7. Commands*.

(3) In the case of cluster operation

If you change the logical host name in a cluster system, delete the logical host that was in effect before the change. Then set up the logical host again that will be in effect after the change so that cluster operation is enabled.

For details about how to delete the logical host, see *3.4 Deleting the logical host*. For details about how to set up the logical host, see *3.2 Installing and setting up the logical host*.

If the logical host name to be changed is specified in the NNMi incident forwarding filter definition file and the custom attribute mapping definition file, check and revise the settings in these files.

For details about the settings of these files, see *4. Converting NNMi Incidents into JP1 Events*.

6.2.3 Changing the date and time of the system on which JP1/IM - EG for NNMi is running

This subsection describes the procedures for changing the system date and time while JP1/IM - EG for NNMi is running.

(1) Procedures for changing the system date and time

This subsection describes the procedures for changing the system date and time.

Setting the system date and time to an earlier time

Avoid changing the system date and time to an earlier time. If you do so, JP1 events might not be issued or duplicate JP1 events might be issued.

To set the system date and time to an earlier time:

1. Terminate JP1/IM - EG for NNMi.

2. Set the system date and time.
3. Delete the `imevtgw_nnmi_last_forwarded.conf` file[#].
4. Keep JP1/IM - EG for NNMI stopped until the system date and time that was in effect before the change is reached (until the date and time at which step 2 was performed).
5. Execute the following command to check the value of the `startup` option:


```
jegn_setup -list [-h logical-host-name]
```
6. Execute the following command:


```
jegn_setup -update [-h logical-host-name] -startup 0
```
7. Start JP1/IM - EG for NNMI.
8. Execute the following command to restore the value of the `startup` option:


```
jegn_setup -update [-h logical-host-name] -startup the-value-checked-in-step-5
```
9. Execute the following command to apply the value of the `startup` option specified in step 8:


```
jegn_spmd_reload [-h logical-host-name]
```

Advancing the system date and time to a point in the future

To advance the system date and time to a point in the future:

1. Terminate JP1/IM - EG for NNMI.
2. Set the system date and time.
3. Delete the `imevtgw_nnmi_last_forwarded.conf` file[#].
4. Execute the following command to check the value of the `startup` option:


```
jegn_setup -list [-h logical-host-name]
```
5. Execute the following command:


```
jegn_setup -update [-h logical-host-name] -startup 0
```
6. Start JP1/IM - EG for NNMI.
7. Execute the following command to restore the value of the `startup` option:


```
jegn_setup -update [-h logical-host-name] -startup the-value-checked-in-step-4
```
8. Execute the following command to apply the value of the `startup` option specified in step 7:


```
jegn_spmd_reload [-h logical-host-name]
```

#

The `imevtgw_nnmi_last_forwarded.conf` file is stored at the following locations:

In Windows

- Physical host: *installation folder*\JP1EG4NNMI\dat
- Logical-host: *shared-folder*\JP1EG4NNMI\dat

In UNIX

- Physical host: `/var/opt/jpleg4nnmi/dat`
- Logical-host: *shared-directory*/jpleg4nnmi/dat

(2) Procedure for changing the time zone in the system

This subsection describes the procedure for changing the time zone in the system. For details about the procedures and notes for NNMI, see the appropriate documentation for the specific NNMI products.

1. Terminate JP1/IM - EG for NNMi.
2. Change the time zone in the system.
3. Delete the `imevtgw_nnmi_last_forwarded.conf` file#.
4. Execute the following command to check the value of the startup option:
`jegn_setup -list [-h logical-host-name]`
5. Execute the following command:
`jegn_setup -update [-h logical-host-name] -startup 0`
6. Start JP1/IM - EG for NNMi.
7. Execute the following command to restore the value of the startup option:
`jegn_setup -update [-h logical-host-name] -startup the-value-checked-in-step-4`
8. Execute the following command to apply the value of the startup option specified in step 7:
`jegn_spmc_reload [-h logical-host-name]`

#

The `imevtgw_nnmi_last_forwarded.conf` file is stored at the following locations:

In Windows

- Physical host: *installation folder*\JP1EG4NNMI\dat
- Logical-host: *shared-folder*\JP1EG4NNMI\dat

In UNIX

- Physical host: `/var/opt/jp1eg4nnmi/dat`
- Logical-host: *shared-directory*/jp1eg4nnmi/dat

6.3 Notes regarding operation

- Please invalidate the dampening function of the NNMi incident by the following commands.
`nnmsetdampenedinterval.ovpl -hours 0 -minutes 0 -seconds 0`
When the dampenin function is effective, the incident not displayed in an incident view of NNMi might be displayed in an integrated console of JP1/IM-Manager.
- When this product is used in an IPv4/IPv6 dual-stack environment, the comparison keywords that can be used for source nodes (correlation conversion) (attribute name: SRC) in the NNMi incident forwarding filter definition file can be used only for NNMi incidents in the IPv4 stack. These comparison keywords cannot be used for NNMi incidents in the IPv6 stack.
- When the OS is shut down, the following error message might be output to logs such as the event log or integrated trace log:
KAVB3737-E The JP1_EGN jegneg4nnmi terminated abnormally.
When the OS is shut down, the jegneg4nnmi process might be forcibly stopped by the OS. In this case, the KAVB3737-E message is output, but there are no operation problems.
- When using antivirus software, exclude the JP1/IM - EG for NNMi installation directory, all files and folders under the installation directory, the logical host directory, and all files and folders under the logical host directory from the scope of virus scans.

7

Commands

This chapter describes the syntax of the commands that can be used in JP1/IM - EG for NNMi.

Format of command explanations

This section describes the format of the explanations of the commands.

The explanation of each command consists of the items described below. Note that not all items are applicable to all commands.

Function

Describes the function of the command.

Format

Describes the command's format.

Execution permission

Describes the user permissions required in order to execute the command.

Storage directory

Describes the command's storage location.

Arguments

Describes the command's arguments.

Arguments are case sensitive.

Notes

Provides additional information about the command.

Return values

Describes the command's return values.

For details about the messages that are displayed during command execution, see [9. Messages](#).

Lists of commands

This section provides lists of the commands that can be used in JP1/IM - EG for NNMi. The tables indicate each command's support under Windows and UNIX as follows:

Legend:

Y: Supported

--: Not supported

#

For commands that are also available in Windows, read the footnoted instances of *Superuser permissions* in the *Required execution permissions* column of the first table below as *Administrator permissions*.

Following the tables, the commands are described in alphabetical order.

Commands related to startup, termination, and setup

Overview of function	Command name	Windows	UNIX	Required execution permissions
Sets up JP1/IM - EG for NNMi	<code>jegn_setup</code>	Y	Y	Superuser permissions [#]
Starts JP1/IM - EG for NNMi automatically	<code>jegn_start (UNIX only)</code>	--	Y	Superuser permissions
Terminates JP1/IM - EG for NNMi automatically	<code>jegn_stop (UNIX only)</code>	--	Y	Superuser permissions
Checks the status of JP1/IM - EG for NNMi processes	<code>jegn_spmd_status</code>	Y	Y	Superuser permissions [#]
Updates the status of JP1/IM - EG for NNMi processes	<code>jegn_spmd_reload</code>	Y	Y	Superuser permissions [#]
Specifies settings required for operation in a cluster system	<code>jegn_setup_cluster</code>	Y	Y	Superuser permissions [#]
Starts JP1/IM - EG for NNMi in a cluster system	<code>jegn_start.cluster (UNIX only)</code>	--	Y	Superuser permissions
Terminates JP1/IM - EG for NNMi in a cluster system	<code>jegn_stop.cluster (UNIX only)</code>	--	Y	Superuser permissions
Forcibly terminates JP1/IM - EG for NNMi in a cluster system	<code>jegn_killall.cluster (UNIX only)</code>	--	Y	Superuser permissions

Commands used for troubleshooting

Overview of function	Command name	Windows	UNIX	Required execution permission
Collects data after a problem has occurred in JP1/IM - EG for NNMi	<code>jegn_log.bat (Windows only)</code>	Y	--	Administrator permissions
	<code>jegn_log.sh (UNIX only)</code>	--	Y	Superuser permissions

jegn_killall.cluster (UNIX only)

Function

This command executes forcible termination of the JP1/IM - EG for NNMi processes when you are operating in a cluster system.

If you execute the `jegn_stop.cluster` command while node switching is underway, the processes might not stop and node switching might fail. Because this command terminates processes forcibly, use it only when processes cannot be terminated by the normal method of stopping the JP1/IM - EG for NNMi services.

The command is able to terminate the following processes:

- Process management (`jegn_spmd`)
- Main service (`jegn4nnmi`)

Format

```
jegn_killall.cluster [logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

`/etc/opt/jp1eg4nnmi`

Arguments

logical-host-name

Specifies the name of the logical host on which this command is to be executed. The permitted length is from 1 to 32 characters (bytes). If this option is omitted, the command assumes the logical host specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host.

Notes

This command checks only the first 32 bytes of logical host names and then forcibly terminates processes at any host with a matching name. It cannot forcibly terminate processes at a logical host whose name consists of more than 32 bytes.

Return values

0	Normal termination
1	No logical host name was specified
2	There is no log directory

jegn_log.bat (Windows only)

Function

This is a tool for collecting data in the event of a problem in JP1/IM - EG for NNMi. The data collected by this tool includes JP1/IM - EG for NNMi maintenance data, OS system information, and integrated trace logs.

This tool is a batch file. It cannot be customized by the user.

When you execute this tool, the data is classified into primary and secondary data categories and stored directly under the specified *data storage folder*.

Primary data is collected for purposes such as identifying an error and investigating the causes of a minor problem. It consists of the minimum amount of log information and settings files. Secondary data provides the detailed information needed for an in-depth investigation of an error. It consists of data such as the Windows event log, a crash dump, and the JP1/Base event database.

If necessary, use a program such as a compression tool to compress the collected data.

For details about the data that can be collected by this tool, see [10.3.1 Data to be collected \(in Windows\)](#).

Format

```
jegn_log.bat -f data-storage-folder-name
              [-h logical-host-name]
              [-t]
              [-n]
              [-p]
              [-r]
              [-q]
```

Execution permission

Administrator permissions. If UAC is enabled, however, execute the command from the administrator console.

Storage directory

EG-for-NNMi-path\tools

Arguments

-f data-storage-folder-name

Specifies the name of the folder to which the collected data is to be output, expressed as an absolute path or a path relative to the location where the command is executed. If the path contains a space, enclose the entire path in double-quotation marks ("). This option is mandatory.

If a nonexistent folder is specified, a new folder is created with the specified name. If an existing folder is specified, the contents of that folder are deleted and then the specified folder is created. Do not specify the name of a folder that contains files that you do not want to delete.

-h logical-host-name

Specifies the name of the logical host when you are operating in a cluster system. The permitted length is from 1 to 255 characters (bytes). When this option is specified, the command collects data for the logical host as well as for the physical

host. If this option is omitted, the command collects data for the physical host only. If you are not using a cluster system, there is no need to specify this option.

If this option is omitted when you are not operating in a cluster system, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. However, if you omit this option while you are operating in a cluster system, the logical host name specified in the `JP1_HOSTNAME` environment variable will not be assumed. Therefore, when you use a cluster system, you must specify the logical host name in this option.

`-t`

Specifies that the `hosts` and `services` files are not to be collected.

`-n`

Specifies that the maintenance data for JP1/Base is not to be collected.

`-p`

Specifies that the JP1/Base event database is not to be collected.

`-r`

Specifies that the command execution log files for JP1/Base are not to be collected.

`-q`

Specifies that there is no need to wait for a response confirming that data collection processing is to be resumed.

If the `-q` option is omitted, the system waits for a response when it displays a message asking whether the processing is to be resumed.

Notes

- A huge amount of data can be collected by this tool. Before you execute this tool, you must estimate the amount of storage space that will be required and check the available space on your machine. For details about the amount of data that can be collected, see the Release Notes for JP1/IM - EG for NNMi.
- Do not execute this tool more than once. If it is executed multiple times, the collected data might be overwritten or data collection might fail.
- If a file to be collected cannot be found, the tool might display a message such as `The file was not found;` however, no action is necessary in such a case.
- If you execute the data collection command in Windows, the prompt `Refreshing System Information...` appears, but do not click the **Cancel** button. If you click the **Cancel** button, part of the information cannot be collected.

Return values

0	Normal termination
8	Abnormal termination

jegn_log.sh (UNIX only)

Function

This is a tool for collecting data in the event of a problem in JP1/IM - EG for NNMi. The data collected by this tool includes JP1/IM - EG for NNMi maintenance data, OS system information, and integrated trace logs.

This tool is a shell script. It cannot be customized by the user.

When you execute this tool, it classifies the target directories or files used for data collection into primary data and secondary data categories, archives the data directly under the specified *data storage directory*, and then creates compressed files.

Primary data is collected for purposes such as identifying an error and investigating the causes of a minor problem. It consists of the minimum amount of log information and settings files. Secondary data provides the detailed information needed for an in-depth investigation of an error. It consists of data such as core analysis information and the JP1/Base event database.

If a core dump of JP1/IM - EG for NNMi exists at the time you execute this command, the tool displays the KNAG1044-I message asking whether the core dump is to be deleted. If you enter *y* or *yes*, the tool deletes the core dump.

For details about the data that can be collected by this tool, see [10.3.2 Data to be collected \(in UNIX\)](#).

Format

```
jegn_log.sh -f data-storage-directory-name
             [-h logical-host-name]
             [-t]
             [-u]
             [-n]
             [-p]
             [-r]
             [-q]
             [directory-name-or-file-name...]
```

Execution permission

Superuser permissions

Storage directory

/opt/jpleg4nnmi/tools

Arguments

-f *data-storage-directory-name*

Specifies the absolute path (without any spaces) of the directory for storing the collected data. This option is mandatory.

If the specified directory already contains data, the tool displays a message asking whether the existing data is to be overwritten by the collected data. Note that if you specify the -q option, the existing data will be overwritten without requesting confirmation.

If you have specified the name of a device file such as tape, the tool stores the collected data on the device without compressing it.

-h *logical-host-name*

Specifies the name of the logical host when you are operating in a cluster system. The permitted length is from 1 to 255 characters (bytes). When this option is specified, the command collects data for the logical host as well as for the physical host. If this option is omitted, the command collects data for the physical host only. If you are not using a cluster system, there is no need to specify this option.

If this option is omitted when you are not operating in a cluster system, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. However, if you omit this option while you are operating in a cluster system, the logical host name specified in the `JP1_HOSTNAME` environment variable will not be assumed. Therefore, when you use a cluster system, you must specify the logical host name in this option.

-t

Specifies that the `hosts`, `services`, and `passwd` files are not to be collected.

-u

Specifies that core analysis information is not to be collected.

-n

Specifies that the maintenance data for JP1/Base is not to be collected.

-p

Specifies that the JP1/Base event database is not to be collected.

-r

Specifies that the command execution log files for JP1/Base are not to be collected.

-q

Specifies that there is no need to wait for a response confirming that data collection processing is to be resumed.

If the `-q` option is omitted, the system waits for a response when it displays a message asking whether the processing is to be resumed.

directory-name-or-file-name

Specifies the name of a file or directory to be collected by this tool. Specify an absolute path name. If you specify multiple names, separate them with the space character.

Note that this option must be the last option specified in the command; it can be specified only after you have specified all other options that you need to specify. The collected data is stored as primary data for the physical host.

Notes

- A huge amount of data can be collected by this tool. Before you execute this tool, you must estimate the amount of storage space that will be required and check the available space on your machine. For details about the size of the data that can be collected, see the Release Notes for JP1/IM - EG for NNMi.
- Do not execute this tool more than once. If it is executed multiple times, the collected data might be overwritten or data collection might fail.

- If a file to be collected cannot be found, the tool might display a message such as `The file was not found`; however, no action is necessary in such a case.

Return values

0	Normal termination
8	Abnormal termination

jegn_setup

Function

This command sets up an operating environment for JP1/IM - EG for NNMi.

Format

To perform a new setup

```
jegn_setup [-h logical-host-name]  
           -user NNMi-user-name  
           -passwd NNMi-password  
           [-port NNMi-port-number]  
           [-lang NNMi-language]  
           [-interval NNMi-incident-reacquisition-interval]  
           [-startup NNMi-incident-acquisition-method]  
           [-ssl availability-of-TLS]
```

To perform an overwrite setup

```
jegn_setup -update  
           [-h logical-host-name]  
           [-user NNMi-user-name]  
           [-passwd NNMi-password]  
           [-port NNMi-port-number]  
           [-lang NNMi-language]  
           [-interval NNMi-incident-reacquisition-interval]  
           [-startup NNMi-incident-acquisition-method]  
           [-ssl availability-of-TLS]
```

To check the operating environment

```
jegn_setup -list  
           [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions. If UAC is enabled, however, execute the command from the administrator console.

In UNIX: Superuser permissions

Storage directory

In Windows:

EG-for-NNMi-path\bin

In UNIX:

/opt/jpleg4nnmi/bin

Arguments

-h *logical-host-name*

Specifies the name of the logical host for which an operating environment is to be set up. This argument is applicable when you are operating in a cluster system. The permitted length is from 1 to 196 characters (bytes) in Windows and from 1 to 255 characters (bytes) in UNIX. If this option is omitted, the command assumes the logical host specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host. If you are not using a cluster system, there is no need to specify this argument.

`-user NNMi-user-name`

Specifies the user name of the Web service client of NNMi. The permitted length is from 1 to 40 characters. The characters permitted for the user name are alphanumeric characters, symbols, and the space. If the user name contains a space, enclose the entire name in double-quotation marks (").

If this is a new setup, this option is mandatory.

`-passwd NNMi-password`

Specifies the password for the Web service client of NNMi. The permitted length is from 1 to 40 characters. The characters permitted for the password are alphanumeric characters, symbols, and the space. If the password contains a space, enclose the entire password in double-quotation marks (").

If this is a new setup, this option is mandatory.

`-port NNMi-port-number`

Specifies the port number for connection of the NNMi. The permitted value is from 1 to 65535.

If you omit this option and specify `true` in the `-ssl` option, the command assumes 20481; if you omit this option and specify `false` in the `-ssl` option, the command assumes 20480.

`-lang NNMi-language`

Specifies the language of the NNMi that is to be connected. Specify `en` in this argument.

If you omit this option, the command sets `en` as the language type specified in JP1/Base.

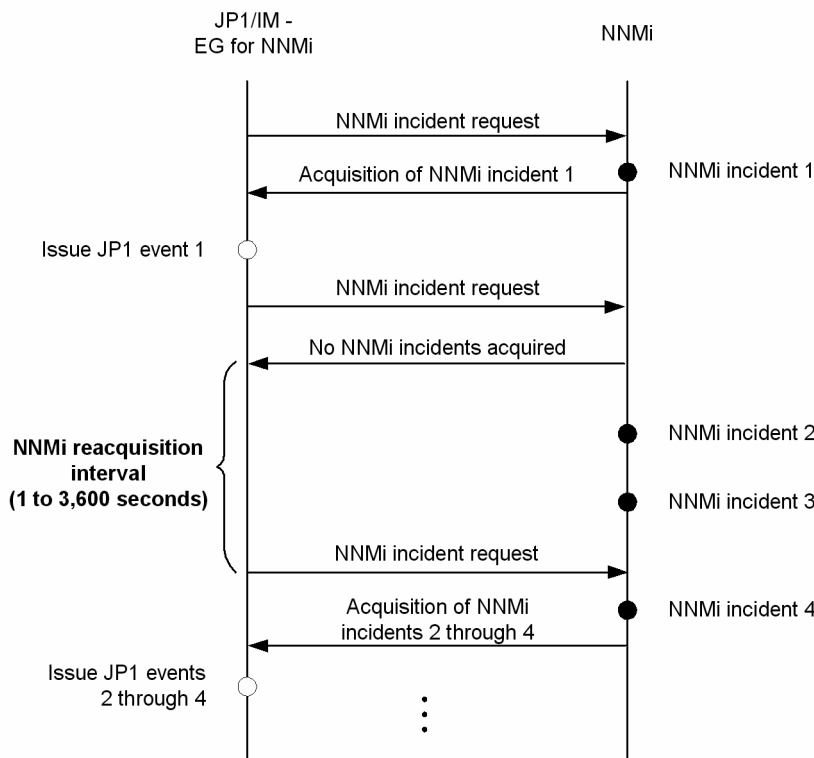
`-interval NNMi-incident-reacquisition-interval`

Specifies the interval after which an NNMi incident acquisition attempt is to be made again when there were no NNMi incidents to be acquired or in the event of an exception such as a communication error. The permitted value is from 1 to 3600 (seconds).

If this option is omitted, 30 is set.

The following figure illustrates the concept of the NNMi incident re-acquisition interval.

Figure 7–1: NNMi incident re-acquisition interval



JP1/IM - EG for NNMi issues to NNMi a request to acquire NNMi incidents. If there are NNMi incidents waiting to be acquired, they are acquired. After the acquired NNMi incidents have been converted into JP1 events and the JP1 events have been issued, JP1/IM - EG for NNMi issues the next request to acquire NNMi incidents.

If there are no NNMi incidents to be acquired, JP1/IM - EG for NNMi issues the next request after the amount of time specified in this option has elapsed.

`-startup NNMi-incident-acquisition-method`

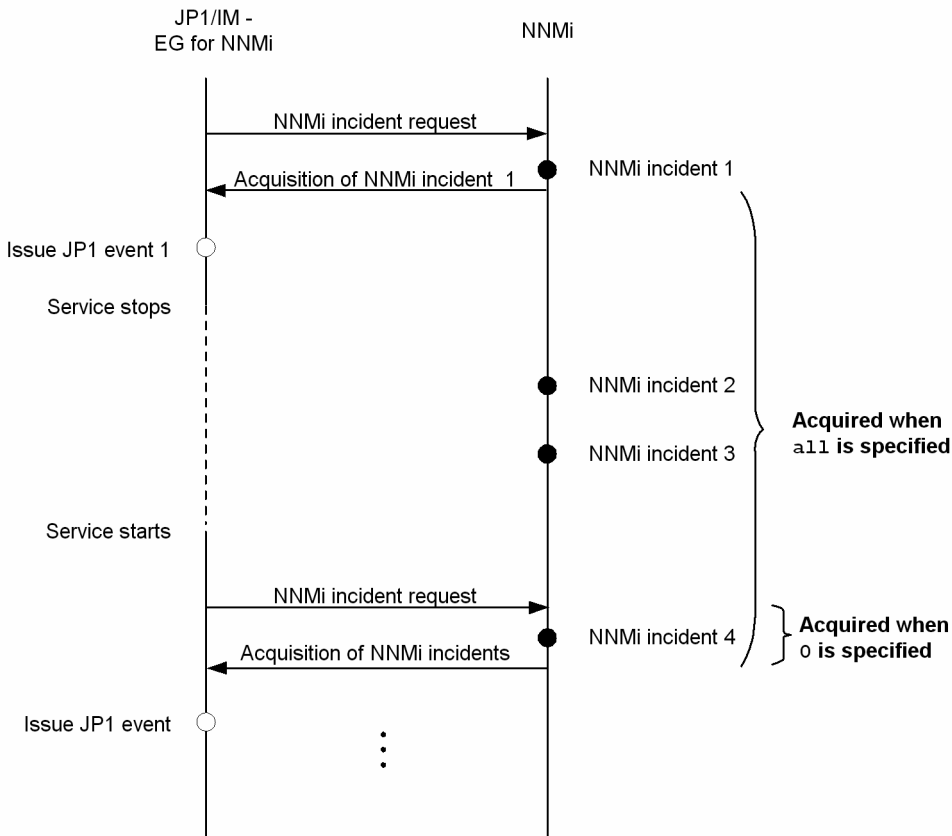
Specifies the first NNMi incident that is to be acquired in the case where NNMi incidents were issued while the service of JP1/IM - EG for NNMi was stopped and those incidents are to be acquired when the service starts (except during the first startup). The permitted values are `all` and integers in the range from 0 to 240 (hours).

If `all` is specified, the command acquires all NNMi incidents that have been issued up to the current time since the last NNMi incident was acquired. If an integer other than 0 is specified, the command acquires all the NNMi incidents beginning from the specified number of hours ago. If 0 is specified, the command does not acquire any of the NNMi incidents that were issued while the service was stopped.

If this option is omitted, 0 is set.

The following figure shows the range of NNMi incidents that are acquired when the service starts.

Figure 7–2: Range of NNMi incidents that are acquired when the service starts



`-ssl availability-of-TLS`

Specifies whether TLS is to be used when connection is established with NNMi. To use TLS, specify `true`. To not use TLS, specify `false`.

If this option is omitted, `false` is set.

If `true` is specified for this option, a connection is established by using the TLS protocol, among the protocol versions that can be used for JP1/IM - EG for NNMi, with the highest version number that can be used for the connection-destination JP1/NNMi.

For information about the TLS versions that JP1/IM - EG for NNMi can use, see "[2.4.1 Executing the setup command](#)".

`-update`

Specifies that this is an overwrite setup, and only the information in the specified options is to be changed. For the omitted options, the existing information is to be inherited.

If you have executed the `jegn_setup` command while the services of JP1/IM - EG for NNMi were running, either execute the `jegn_spmc_reload` command or restart the JP1/IM - EG for NNMi services in order to apply the new information. If you execute the `jegn_setup` command while the JP1/IM - EG for NNMi services are stopped, the specified information will take effect the next time the services start.

`-list`

Specifies that the current settings are to be displayed. When you specify this option, each option setting is displayed in the format `option-name:setting`. However, the password is always displayed as `*****`. The following shows an example of the display:

```
user:hitachi
passwd:*****
port:80
lang:ja
interval:30
startup:0
ssl:false
```

Return values

0	Normal termination
1	Abnormal termination

jegn_setup_cluster

Function

This command sets up an operating environment for JP1/IM - EG for NNMi when it is used in a cluster system.

Format

To set up an operating environment for the active server:

```
jegn_setup_cluster -h logical-host-name -d shared-directory-name
```

To set up an operating environment for the standby server (Windows only):

```
jegn_setup_cluster -h logical-host-name
```

Execution permission

In Windows: Administrator permissions. If UAC is enabled, however, execute the command from the administrator console.

In UNIX: Superuser permissions

Storage directory

In Windows:

EG-for-NNMi-path\bin

In UNIX:

/opt/jpleg4nnmi/bin

Arguments

-h *logical-host-name*

Specifies the name of the logical host for which the operating environment is to be set up. The permitted length is from 1 to 196 characters (bytes) in Windows and from 1 to 255 characters (bytes) in UNIX.

-d *shared-directory-name*

Specifies the name of the shared directory that is to be used during operation in the cluster system. Specify this option when you are setting up the operating environment for the active server; when this option is omitted, this command sets up the operating environment for the standby server.

Notes

When you specify the -d option (to set up an operating environment for the active server), the shared disk must be mounted before command execution.

Return values

0	Normal termination
1	Abnormal termination

jegn_spmd_reload

Function

This command updates the status of the JP1/IM - EG for NNMi processes. Whenever you change definition information for JP1/IM - EG for NNMi, you must reload the new information in order to apply it.

For details about the definition files that are enabled by execution of the `jegn_spmd_reload` command, see [6.2.1 Editing the definition files](#).

Format

```
jegn_spmd_reload [-h logical-host-name]  
                 [-t monitoring-period]
```

Execution permission

In Windows: Administrator permissions. If UAC is enabled, however, execute the command from the administrator console.

In UNIX: Superuser permissions

Storage directory

In Windows:

EG-for-NNMi-path\bin

In UNIX:

/opt/jp1eg4nnmi/bin

Arguments

-h *logical-host-name*

Specifies the name of the logical host when you are operating in a cluster system. The permitted length is from 1 to 255 characters (bytes). If this option is omitted, the command assumes the logical host specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host. If you are not using a cluster system, there is no need to specify this argument.

-t *monitoring-period*

Specifies in seconds the amount of time to wait for termination of the `jegn_spmd_reload` command. The permitted value range is from 0 to 32,767 (seconds). If this option is omitted, 60 is assumed. If the `jegn_spmd_reload` command does not terminate within the specified amount of time, the system assumes that the `jegn_spmd_reload` command has failed, in which case operations continue using the definitions that were in effect before the change.

Notes

- The `jegn_spmd_reload` and the `jegn_spmd_status` commands cannot be executed more than once concurrently on the same host.
- If a definition file[#] of this product contains an error, a timeout error occurs when the `jegn_spmd_reload` command is executed. In such a case, check the integrated trace log for a log related to the error in the definition file. If a definition file contains an error, correct the definition file and then execute the `jegn_spmd_reload` command.

#

For details about definition files, see [6.2.1 Editing the definition files](#) in the manual for this product.

Return values

0	Normal termination
Other than 0	Abnormal termination

jegn_spm�_status

Function

This command checks whether processes managed by JP1/IM - EG for NNMi are running or have terminated. If the processes are running normally when the `jegn_spm�_status` command executes, the command displays the main service process name (`jegn4nnmi`) and the process ID.

For details about the processes managed by JP1/IM - EG for NNMi, see [B. Lists of Processes](#).

Format

```
jegn_spm�_status [-h logical-host-name]  
                 [-t monitoring-period]
```

Execution permission

In Windows: Administrator permissions. If UAC is enabled, however, execute the command from the administrator console.

In UNIX: Superuser permissions

Storage directory

In Windows:

EG-for-NNMi-path\bin

In UNIX:

/opt/jp1eg4nnmi/bin

-h *logical-host-name*

Specifies the name of the logical host when you are operating in a cluster system. The permitted length is from 1 to 255 characters (bytes). If this option is omitted, the command assumes the logical host specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host. If you are not using a cluster system, there is no need to specify this argument.

-t *monitoring-period*

Specifies in seconds the amount of time to wait for termination of the `jegn_spm�_status` command. The permitted value range is from 0 to 32,767 (seconds). If this option is omitted, 60 is assumed. If the `jegn_spm�_status` command does not terminate within the specified amount of time, the system assumes that the `jegn_spm�_status` command has failed.

Notes

The `jegn_spm�_reload` and `jegn_spm�_status` commands cannot be executed more than once concurrently on the same host.

Return values

0	All processes are running.
---	----------------------------

1	An error occurred during communication (such as with process management); or, the shared folder (shared directory) is not mounted in the case of operation in a cluster system.
4	Some processes are running.
8	All processes are stopped.
12	Requested processing is underway or has timed out (retriable).

jegn_start (UNIX only)

Function

This command is a script for starting JP1/IM - EG for NNMi automatically.

To use this script, you must execute the following commands after you have installed and set up JP1/IM - EG for NNMi:

```
# cd /etc/opt/jpleg4nnmi
# cp -p jegn_start.model jegn_start
```

Once these commands have been executed, JP1/IM - EG for NNMi will start automatically at the time of system startup.

Before you execute these commands, make sure that NNMi and JP1/Base are running. If you execute these commands while the event service of JP1/Base is not running, the commands terminate abnormally with a return value of 1.

The command terminates with a return value of 0 after issuing a startup request to the processes of JP1/IM - EG for NNMi. You can use the `jegn_spm�_status` command to check whether the processes have started successfully.

Format

```
jegn_start
```

Execution permission

Superuser permissions

Storage directory

/etc/opt/jpleg4nnmi

Note

The system takes a long time to display the execution results if the `jegn_start` command is executed when the NNMi incident forwarding filter definition file includes an incorrect definition. This problem occurs because the system internally checks the service start state by issuing the `jegn_spm�_status` command multiple times, even when the service fails to start. If the KAVB3662-I message is displayed after the command terminates, check the integrated trace log. Follow the instructions of the output message, and then execute the command again.

Return values

0	Normal termination
1	Arguments are specified; or, the event service is not running.
2	There is no log directory

jegn_start.cluster (UNIX only)

Function

This command starts JP1/IM - EG for NNMi on the logical host when you are operating in a cluster system. If you register this command into the cluster software, JP1/IM - EG for NNMi will start.

Be sure to start NNMi and JP1/Base on the same logical host before you execute this command. If you execute this command while the event service of JP1/Base is not running, the command terminates abnormally with a return value of 1.

The command terminates with a return value of 0 after issuing a startup request to the processes of JP1/IM - EG for NNMi. You can use the `jegn_spmc_status` command to check whether the processes have started successfully.

Format

```
jegn_start.cluster [logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

/etc/opt/jpleg4nnmi

Arguments

logical-host-name

Specifies the name of the logical host on which this command is to be executed. The permitted length is from 1 to 63 characters (bytes). If this option is omitted, the command assumes the logical host specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host.

Return values

0	Normal termination
1	More than one argument is specified; or, the event service is not running.
2	There is no log directory

jegn_stop (UNIX only)

Function

This command is a script for terminating JP1/IM - EG for NNMi automatically.

To use this script, you must execute the following commands after you have installed and set up JP1/IM - EG for NNMi:

```
# cd /etc/opt/jpleg4nnmi
# cp -p jegn_stop.model jegn_stop
```

Once these commands have been executed, JP1/IM - EG for NNMi will terminate automatically when the system terminates.

Format

```
jegn_stop
```

Execution permission

Superuser permissions

Notes

Terminate JP1/IM - EG for NNMi before terminating NNMi. If NNMi stops before JP1/IM - EG for NNMi does, the KNAG2032-E message or the KNAG2033-E message is written in integrated trace logs.

Storage directory

/etc/opt/jpleg4nnmi

Return values

0	Normal termination
1	Arguments are specified; or, the termination request resulted in a timeout.

jegn_stop.cluster (UNIX only)

Function

This command terminates JP1/IM - EG for NNMi on the logical host when you are operating in a cluster system. If you will be executing this command, you must register it into the cluster software.

Format

```
jegn_stop.cluster [logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

/etc/opt/jp1eg4nnmi

Arguments

logical-host-name

Specifies the name of the logical host on which this command is to be executed. The permitted length is from 1 to 63 characters (bytes). If this option is omitted, the command assumes the logical host specified in the JP1_HOSTNAME environment variable. If the JP1_HOSTNAME environment variable is not specified, the command assumes the physical host.

Notes

- This command cannot be executed more than once concurrently.
- Terminate JP1/IM - EG for NNMi before terminating NNMi. If NNMi stops before JP1/IM - EG for NNMi does, the KNAG2032-E message or the KNAG2033-E message is written in integrated trace logs.

Return values

0	Normal termination
1	More than one argument is specified; or, the termination request resulted in a timeout.

8

JP1 Events

This chapter describes the types and attributes of the JP1 events that can be obtained by converting NNMi incidents and the JP1 events that are issued by JP1/IM - EG for NNMi.

8.1 Attributes of JP1 events

JP1/IM - EG for NNMi handles the following two types of JP1 events:

- JP1 events obtained by converting NNMi incidents
- JP1 events issued by JP1/IM - EG for NNMi

For details about each type of JP1 event, see the subsequent sections in this chapter. This section describes the attributes of JP1 events.

JP1 events have two types of attributes, basic attributes and extended attributes.

Basic attributes

All JP1 events have basic attributes.

Extended attributes

Extended attributes are assigned by individual programs that issue JP1 events. The extended attributes include the following two types of information:

- **Common information**
The common information is common to all JP1 programs.
- **Program-specific information**
The program-specific information is extended attribute information other than common information.

8.2 JP1 events obtained by converting NNMi incidents

When NNMi incidents are converted into JP1 events, the attributes of the NNMi incidents are mapped into JP1 event attributes. Two types of attributes are mapped:

- Attributes that are mapped by default
- Additional attributes that are mapped according to settings in the NNMi incident forwarding filter definition file

The following table lists and describes the attributes of JP1 events that are obtained by converting NNMi incidents.

Table 8–1: Attributes of JP1 events obtained by converting NNMi incidents

Attribute type		Item	Attribute name	Description	Size	Mapping
Basic attribute		Event ID	None	Value indicating the event or the program of the application that issued the JP1 event. In NNMi: 0x00006100	--	D
		Message	None	Character string describing the details of the event. By default, the message in the NNMi incident is set. The NNMi incident forwarding filter definition file can be used to set mapping.	--	D
Extended attribute	Common information	Event level	SEVERITY	JP1 event severity obtained by converting the severity of the NNMi incident. The NNMi incident forwarding filter definition file can be used to set mapping.	5-11 bytes	D
		Product name	PRODUCT_NAME	Name of the program that issued the JP event. In NNMi: / HITACHI/JP1/IM/NNMI_INCIDENT	29 bytes	D
		Object type	OBJECT_TYPE	Name indicating the type of object that resulted in issuance of the event. In NNMi: NNMI_INCIDENT	13 bytes	D
		Object name	OBJECT_NAME	Name of the object that resulted in issuance of the event (such as a job or a jobnet). In NNMi: Name set by NNMi (NNMI_NAME)	1-64 characters	D

Attribute type		Item	Attribute name	Description	Size	Mapping
Extended attribute	Common information	Root object type	ROOT_OBJECT_TYPE	Type of object. In NNMi: NNMI_INCIDENT	13 bytes	D
		Root object name	ROOT_OBJECT_NAME	Name used to issue an execution instruction during a user operation. In NNMi: Name set by NNMi (NNMI_NAME)	1-64 characters	D
		Occurrence	OCCURRENCE	Event that occurred on the object indicated by its object name. In NNMi: RECEIVE	7 bytes	D
Program-specific information	Program-specific information	Result of Mapping	NNMI_EM_RESULT	Execution result of mapping processing on added extended attributes. For details, see 4.1.3(3)(b) Checking the result of extended attribute mapping.	1-19 bytes	D ^{#1}
		Incident UUID	NNMI_UUID	UUID of the NNMi incident	1-36 characters	D ^{#1}
		Source Name	NNMI_SRC_NAME	Source name of the NNMi incident	1-255 characters	A
		Source Type	NNMI_SRC_TYPE	Source type of the NNMi incident	1-50 characters	A
		Source Node	NNMI_SRC_NODE_NAME	Source node of the NNMi incident	1-255 characters	D
		Name	NNMI_NAME	Name of the NNMi incident	1-64 characters	D
		Severity of NNMi incident	NNMI_SEVERITY	Severity of the NNMi incident	1-255 characters	D
		Priority	NNMI_PRIORITY	Priority of the NNMi incident	1-255 characters	A
		Lifecycle State	NNMI_LIFECYCLE_STATE	Lifecycle state of the NNMi incident	1-255 characters	A
		Assigned To	NNMI_ASSIGNED_TO	NNMi incident assignment target	1-255 characters	A
		Category	NNMI_CATEGORY	Category of the NNMi incident	1-255 characters	A
		Family	NNMI_FAMILY	Family of the NNMi incident	1-255 characters	A
		Origin	NNMI_ORIGIN	Origin of the NNMi incident	1-255 characters	A
		Correlation Nature	NNMI_NATURE	Correlation nature of the NNMi incident	1-255 characters	A
		Duplicate Count	NNMI_DUPLICATE_COUNT	Duplicate count of the NNMi incident	1-10 bytes	A

Attribute type		Item	Attribute name	Description	Size	Mapping
Extended attribute	Program-specific information	Message	NNMI_FORMATTED_MESSAGE	Message in the NNMi incident	1-1,024 characters	D
		Notes	NNMI_NOTES	Notes in the NNMi incident	1-256 characters	A ^{#5}
		RCA Active	NNMI_RCA_ACTIVE	RCA active of the NNMi incident	4-5 characters	A
		Origin Occurrence Time	NNMI_ORIGIN_OCCUR_TIME	Occurrence time at the origin of the NNMi incident ^{#2}	1-17 bytes	D
		Origin Occurrence Time (ms)	NNMI_ORIGIN_OCCUR_TIME_MS	Occurrence time at the origin of the NNMi incident (milliseconds) ^{#3}	1-19 bytes	A
		First Occurrence Time	NNMI_FIRST_OCCUR_TIME	Occurrence time of the first NNMi incident ^{#2}	1-17 bytes	A
		First Occurrence Time (ms)	NNMI_FIRST_OCCUR_TIME_MS	Occurrence time of the first NNMi incident (milliseconds) ^{#3}	1-19 bytes	A
		Last Occurrence Time	NNMI_LAST_OCCUR_TIME	Occurrence time of the last NNMi incident ^{#2}	1-17 bytes	A
		Last Occurrence Time (ms)	NNMI_LAST_OCCUR_TIME_MS	Occurrence time of the last NNMi incident (milliseconds) ^{#3}	1-19 bytes	A
		Created	NNMI_CREATED	Date and time the NNMi incident was created ^{#2}	1-17 bytes	A
		Created (ms)	NNMI_CREATED_MS	Date and time the NNMi incident was created (milliseconds) ^{#3}	1-19 bytes	A
		Last Update Time	NNMI_MODIFIED	Last date and time the NNMi incident acquisition time was updated ^{#2}	1-17 bytes	A
		Last Update Time (ms)	NNMI_MODIFIED_MS	Last date and time the NNMi incident acquisition time was updated (milliseconds) ^{#3}	1-19 bytes	A
		Severity Unique Key	NNMI_SEVERITY_UK	Unique key of the NNMi incident severity	5-8 bytes	D ^{#1}
		Priority Unique Key	NNMI_PRIORITY_UK	Unique key of the NNMi incident priority	1-80 characters	A ^{#1}
		Lifecycle State Unique Key	NNMI_LIFECYCLE_STATE_UK	Unique key of the NNMi incident lifecycle state	1-80 characters	A ^{#1}
		Category Unique Key	NNMI_CATEGORY_UK	Unique key of the NNMi incident category	1-80 characters	A ^{#1}
Family Unique Key	NNMI_FAMILY_UK	Unique key of the NNMi incident family	1-80 characters	A ^{#1}		

Attribute type		Item	Attribute name	Description	Size	Mapping
Extended attribute	Program-specific information	Origin Unique Key	NNMI_ORIGIN_UK	Unique key of the NNMi incident origin	5-18 bytes	A ^{#1}
		Correlation Nature Unique Key	NNMI_NATURE_UK	Unique key of the NNMi incident correlation nature	4-18 bytes	A ^{#1}
		Number of Custom Attributes	NNMI_CIA_NUM	Number of custom attributes of the NNMi incident	1-10 bytes	A
		Custom Attribute Name	NNMI_CIA_NAME_§n	Name of a custom attribute of the NNMi incident. §n indicates the index of the custom attribute. ^{#4}	1-80 characters	A
		Custom Attribute Type	NNMI_CIA_TYPE_§n	Type of the custom attribute of the NNMi incident. §n indicates the index of the custom attribute. ^{#4}	6-15 bytes	A
		Custom Attribute Value	NNMI_CIA_VALUE_§n	Value of the custom attribute of the NNMi incident. §n indicates the index of the custom attribute. ^{#4}	1-2,000 characters	A
		NNMi connection protocol	NNMI_PROTOCOL	Protocol used to connect to NNMi	4-5 bytes	D ^{#6}
		NNMi server name	NNMI_SERVER	Host name of the connection-target NNMi	1-255 bytes	D ^{#1}
		NNMi port number	NNMI_PORT	Port number of the connection-target NNMi	1-5 bytes	D ^{#1}

Legend:

--: There is no need to take this size into consideration.

D: Attribute mapped by default

A: Additional attribute that is mapped when it is defined in the NNMi incident forwarding filter definition file

#1

This is an internal attribute of NNMi incidents. If the version of JP1/IM - Manager is 11-10 or earlier, the default is that they are not displayed in the Event Details window of JP1/IM - View even when NNMi incidents are converted into JP1 events. If you need to display these attributes, see [4.4.1\(3\) Displaying internal attributes in the Event Details window](#). Furthermore, when adding definitions to a definition file for extended event attributes, you must add definitions to the definition files for extended event attributes for all languages. If you have not added the definitions to the definition files for extended event attributes for some languages, the definitions will not be enabled.

#2

Displayed as the elapsed time in seconds since 1970-01-01 at 00:00:00 (world standard time). When the attribute is displayed in the Event Details window of JP1/IM - View, the value is displayed in the time format based on the time specified in the local time zone of the viewer host.

#3

Displayed as the elapsed time in milliseconds since 1970-01-01 at 00:00:00 (world standard time).

#4

§n is replaced with a number in the range from 1 to the number of custom attributes (NNMI_CIA_NUM). Attributes whose §n is from 1 to 20 are displayed in the Event Details window of JP1/IM - View by default. If you want to display attributes whose §n is greater than 20, see [4.4.1\(4\) Displaying custom attributes in the Event Details window](#).

Example: In the case of the fourth custom attribute value, define as NNMI_CIA_VALUE_4.

#5

Even when a value is entered into the *Notes* attribute of an NNMi incident that has been converted into a JP1 event, the attribute value is not mapped into the JP1 event attribute. Only NNMi incident attributes in which values have been entered before JP1/IM - EG for NNMi obtains NNMi incidents from NNMi can be mapped to JP1 event attributes.

#6

The following values will be used based on the `-ssl` option set for the `jegn_setup` command of JP1/IM - EG for NNMi:

- If `false` is specified for the `-ssl` option: `http`

- If `true` is specified for the `-ssl` option: `https`

8.3 JP1 events issued by JP1/IM - EG for NNMI

The following table lists and describes the attributes of JP1 events that are issued by JP1/IM - EG for NNMI.

Table 8–2: Attributes of JP1 events issued by JP1/IM - EG for NNMI

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	None	Value indicating the event or the program of the application that issued the JP1 event.
		Message	None	Character string describing the details of the event.
Extended attribute	Common information	Event level	SEVERITY	Severity of the JP1 event. The following values are assigned, shown here in descending order of severity: Emergency Alert Critical Error Warning Notice Information Debug
		Product name	PRODUCT_NAME	Name of the program that issued the JP event. In the case of JP1/IM - EG for NNMI, the following program name is displayed: /HITACHI/JP1/IM/NNMI/SPMD
		Object type	OBJECT_TYPE	Name indicating the type of object that resulted in issuance of the event.
		Object name	OBJECT_NAME	Name of the object that resulted in issuance of the event (such as a job or a jobnet).
		Occurrence	OCCURRENCE	Event that occurred on the object indicated by the object name.

8.4 Details of JP1 events issued by JP1/IM - EG for NNMi

This section provides the details of the events that are issued by JP1/IM - EG for NNMi.

8.4.1 List of JP1 events issued by JP1/IM - EG for NNMi

The following table lists and describes the JP1 events that are issued by JP1/IM - EG for NNMi.

Table 8–3: List of JP1 events issued by JP1/IM - EG for NNMi

Event ID	Timing of occurrence	Message
0x00006100	When an NNMi incident is converted into a JP1 event.	--
0x000061F0 [#]	When a process has terminated abnormally.	KAVB3737-E The <i>component-name name-of-managed-process</i> terminated abnormally.
0x000061F1 [#]	When process start processing has resulted in a timeout.	KAVB3613-W A <i>component-name</i> timeout occurred in <i>name-of-managed-process</i> . Processing continues.
0x000061F2 [#]	When a process that terminated abnormally has restarted successfully.	KAVB3616-I Restart of the <i>component-name name-of-managed-process</i> has finished.

Legend:

--: The message mapped in the NNMi incident forwarding filter definition file is displayed.

#

This JP1 event is issued only if it is set to be issued in response to a process error. For details about the settings for issuing JP1 events, see [2.4.5\(4\) Setting JP1 event issuance in the event of an abnormal process termination](#).

8.4.2 Details of JP1 events

This subsection provides the details of the JP1 events by event ID.

(1) Details of event ID 0x00006100

This JP1 event is obtained by converting an NNMi incident. For details, see [8.2 JP1 events obtained by converting NNMi incidents](#).

(2) Details of event ID 0x000061F0

Attribute type	Item	Attribute name	Description	
Basic attribute	Event ID	None	0x000061F0	
	Message	None	KAVB3737-E The <i>component-name name-of-managed-process</i> terminated abnormally.	
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/NNMI/SPMD
		Object type	OBJECT_TYPE	SPMD
		Object name	OBJECT_NAME	Name of the process that terminated abnormally

Attribute type		Item	Attribute name	Description
Extended attribute	Common information	Occurrence	OCCURRENCE	NOTICE

(3) Details of event ID 0x000061F1

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	None	0x000061F1
		Message	None	KAVB3613-W A <i>component-name</i> timeout occurred in <i>name-of-managed-process</i> . Processing continues.
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/NNMI/SPMD
		Object type	OBJECT_TYPE	SPMD
		Object name	OBJECT_NAME	Name of the process whose start processing timed out
		Occurrence	OCCURRENCE	NOTICE

(4) Details of event ID 0x000061F2

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	None	0x000061F2
		Message	None	KAVB3616-I Restart of the <i>component-name name-of-managed-process</i> has finished.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/NNMI/SPMD
		Object type	OBJECT_TYPE	SPMD
		Object name	OBJECT_NAME	Name of the restarted process
		Occurrence	OCCURRENCE	NOTICE

9

Messages

This chapter describes the messages that are issued by JP1/IM - EG for NNMi.

9.1 Message output destinations

This section lists the output destinations of the messages that are issued by JP1/IM - EG for NNMi.

9.1.1 Output destinations of messages related to installation (KNAG0001 to KNAG0999)

The following table lists the output destinations of the messages that are related to installation of JP1/IM - EG for NNMi.

Legend:

Y: Output

--: Not output

Table 9–1: Output destinations of messages related to installation

Message ID	Output destination	
	Trace log for the process	Dialog box
KNAG0001 to KNAG0002	Y	Y
KNAG0003	--	Y
KNAG0004 to KNAG0013	Y	Y
KNAG0014	--	Y

9.1.2 Output destinations of messages related to execution of commands (KNAG1000 to KNAG1999)

The following table lists the output destinations of the messages that are related to execution of JP1/IM - EG for NNMi commands.

Legend:

Y: Output

--: Not output

Table 9–2: Output destinations of messages related to execution of commands

Message ID	Output destination			
	Integrated trace log	Trace log for the process	Standard output	Standard error
KNAG1000 to KNAG1002	--	Y	Y	--
KNAG1004	--	--	Y	--
KNAG1005 to KNAG1007	--	Y	--	Y
KNAG1008	--	--	--	Y
KNAG1009 to KNAG1023	--	Y	--	Y
KNAG1024	--	Y	Y	--

Message ID	Output destination			
	Integrated trace log	Trace log for the process	Standard output	Standard error
KNAG1025	--	Y	--	Y
KNAG1026 to KNAG1027	--	Y	Y	--
KNAG1028	--	Y	--	Y
KNAG1029 to KNAG1033	--	Y	Y	--
KNAG1034	--	--	Y	--
KNAG1035	--	Y	--	Y
KNAG1036	--	--	--	Y
KNAG1037	--	--	Y	--
KNAG1039 to KNAG1041	--	--	--	Y
KNAG1042	--	Y	--	Y
KNAG1043	--	Y	Y	--
KNAG1044 to KNAG1045	--	--	Y	--
KNAG1046	--	--	--	Y
KNAG1047 to KNAG1048	--	--	Y	--
KNAG1050	--	Y	--	Y
KNAG1051	--	Y	--	Y
KNAG1052 to KNAG1054	--	--	--	Y
KNAG1055	--	Y	Y	--
KNAG1056	--	Y	--	Y
KNAG1057 to KNAG1058	Y	--	--	Y
KNAG1059	Y	Y	--	Y
KNAG1060	Y	--	--	Y
KNAG1061	--	Y	--	Y
KNAG1063 to KNAG1064	--	Y	--	Y
KNAG1066 to KNAG1067	--	Y	--	Y
KNAG1900 to KNAG1901	--	Y	--	Y

9.1.3 Output destinations of messages related to services (KNAG2000 to KNAG2999)

The following table lists the output destinations of the messages that are related to the services of JP1/IM - EG for NNMi.

Legend:

Y: Output

--: Not output

Table 9–3: Output destinations of messages related to services

Message ID	Output destination		
	Integrated trace log	Trace log for the process	Standard error
KNAG2000 to KNAG2004	Y	Y	--
KNAG2006	Y	Y	--
KNAG2008 to KNAG2013	Y	Y	--
KNAG2015 to KNAG2021	Y	Y	--
KNAG2032 to KNAG2034	Y	Y	--
KNAG2036 to KNAG2043	Y	Y	--
KNAG2046 to KNAG2053	Y	Y	--
KNAG2055	Y	Y	--
KNAG2057 to KNAG2062	Y	Y	--
KNAG2064 to KNAG2070	Y	Y	--
KNAG2071	Y	Y	--
KNAG2072	Y	Y	--
KNAG2900 to KNAG2901	Y	Y	--

9.1.4 Output destinations of messages related to process management (KAVB3501 to KAVB3999)

The following table lists the output destinations of the messages that are related to process management of JP1/IM - EG for NNMi.

Legend:

Y: Output

--: Not output

Notes:

In addition to the messages listed in the table, other messages with message IDs (such as internal error messages) might also be displayed.

Table 9–4: Output destinations of messages related to process management

Message ID	Output destination					
	syslog	Event log	Integrated trace log	Standard output	Standard error	JP1 event
KAVB3501	Y	Y	--	--	--	--
KAVB3502	--	--	Y	--	Y	--
KAVB3503	--	--	--	--	Y	--
KAVB3504	--	--	Y	--	Y	--
KAVB3516	Y	--	--	--	Y	--

Message ID	Output destination					
	syslog	Event log	Integrated trace log	Standard output	Standard error	JP1 event
KAVB3552 to KAVB3554	--	--	Y	--	--	--
KAVB3564	--	--	Y	--	--	--
KAVB3574	--	--	Y	--	--	--
KAVB3577 to KAVB3578	--	--	Y	--	--	--
KAVB3586	--	--	Y	--	--	--
KAVB3597	--	--	Y	--	--	--
KAVB3599	--	--	Y	--	--	--
KAVB3602 to KAVB3605	--	--	Y	--	--	--
KAVB3608 to KAVB3610	--	--	Y	--	--	--
KAVB3612	--	--	Y	--	--	--
KAVB3613	Y	Y	Y	--	--	Y
KAVB3614	Y	Y	Y	--	--	--
KAVB3616	--	--	--	--	--	Y
KAVB3620	Y	Y	Y	Y	--	--
KAVB3621	Y	--	Y	--	--	--
KAVB3623	Y	--	Y	--	--	--
KAVB3624	Y	Y	Y	--	--	--
KAVB3625	--	--	Y	Y	--	--
KAVB3626	Y	Y	Y	Y	--	--
KAVB3627	--	--	Y	--	--	--
KAVB3631	--	--	Y	--	--	--
KAVB3642	--	--	Y	--	--	--
KAVB3643 to KAVB3644	Y	Y	Y	--	--	--
KAVB3645 to KAVB3646	--	--	Y	--	--	--
KAVB3647	--	--	Y	--	--	--
KAVB3649	Y	Y	Y	Y	--	--
KAVB3651 to KAVB3662	--	--	Y	Y	--	--
KAVB3663	--	--	--	--	Y	--
KAVB3672	--	--	Y	Y	--	--

Message ID	Output destination					
	syslog	Event log	Integrated trace log	Standard output	Standard error	JP1 event
KAVB3674 to KAVB3678	--	--	Y	Y	--	--
KAVB3680 to KAVB3684	--	--	Y	Y	--	--
KAVB3685	--	--	--	Y	--	--
KAVB3690 to KAVB3694	--	--	--	Y	--	--
KAVB3705	--	--	Y	--	--	--
KAVB3732	--	--	Y	--	--	--
KAVB3736	--	--	Y	--	--	--
KAVB3737	Y	Y	Y	--	--	Y
KAVB3743 to KAVB3745	--	--	Y	--	--	--
KAVB3752	Y	Y	Y	--	--	--
KAVB3760 to KAVB3769	--	--	Y	--	--	--
KAVB3777 to KAVB3779	--	--	Y	--	--	--
KAVB3786	--	--	Y	--	--	--
KAVB3788	Y	Y	Y	--	--	--
KAVB3802	--	--	Y	--	--	--
KAVB3840 to KAVB3841	--	--	Y	--	--	--
KAVB3846	--	--	Y	--	--	--
KAVB3855	--	--	Y	--	--	--
KAVB3862	Y	Y	Y	--	--	--
KAVB3863	--	--	Y	--	--	--
KAVB3870	Y	Y	--	Y	--	--
KAVB3871	--	--	--	Y	--	--
KAVB3872	Y	Y	--	Y	--	--
KAVB3873	--	--	--	Y	--	--
KAVB3874 to KAVB3875	Y	Y	--	Y	--	--
KAVB3899	--	--	--	Y	--	--
KAVB3905	--	--	Y	--	--	--
KAVB3908	--	--	Y	--	--	--
KAVB3910	--	--	Y	--	--	--

Message ID	Output destination					
	syslog	Event log	Integrated trace log	Standard output	Standard error	JP1 event
KAVB3911 to KAVB3914	--	--	Y	Y	--	--
KAVB3935	--	--	Y	--	--	--
KAVB3960	--	--	--	Y	--	--
KAVB3961	--	--	Y	Y	--	--
KAVB3981	--	--	Y	--	--	--
KAVB3984	--	--	Y	--	--	--
KAVB3986	--	--	Y	Y	--	--

9.2 Message format

This section describes the format of messages issued by JP1/IM - EG for NNMi.

9.2.1 Output format of messages

A message consists of a message ID and a message text. The following shows the format of the displayed messages:

KAVBnnnn-Z message-text

KNAGnnnn-Z message-text

The message ID consists of the following components:

K

System identifier.

AVB or NAG

Identifier of a message as a JP1/IM - EG for NNMi message.

nnnn

Message's serial number.

Z

Type of message:

E: Error message. Processing is canceled.

W: Warning message. Processing resumes after the message is displayed.

I: Information message. Provides information to the user.

Q: Notification message. Requests the user to make a choice regarding execution.

9.2.2 Format of message explanations

The following shows the format used in this manual to explain the messages.

message-ID

message-text

Explanation of the message.

S:

Indicates the system's processing.

O:

Indicates the action that should be taken by the operator when the message is displayed.

9.2.3 For system administrators

When an error occurs during operation, refer to *10. Troubleshooting*, collect the necessary log information, and perform an initial investigation.

Perform an initial investigation to identify the cause of an error by checking the OS's log information (event log in Windows, syslog in UNIX) and various log information output by JP1/IM - EG for NNMi. Use this log information to determine details about the error, how to prevent recurrence of the error, and the appropriate action to be taken.

You need to also record information such as the operational procedure that led to the error and whether the error can be replicated.

9.3 Messages

This section explains messages that have message IDs that are issued by JP1/IM - EG for NNMi.

9.3.1 Messages related to installation (KNAG0001 to KNAG0999)

KNAG0001-E

You do not have the necessary permissions to perform an installation with the current login account. Use an administrator account. The installation will now be canceled.

The login account does not have the permissions required for installation.

S:

Cancels processing.

O:

Use an administrator account to perform installation.

KNAG0002-E

A prerequisite version of JP1/Base is not installed. The installation will now be canceled.

A prerequisite version of JP1/Base has not been installed.

S:

Cancels processing.

O:

Install the prerequisite version of JP1/Base.

KNAG0003-W

This platform is not supported. Do you want to cancel the installation?

This message asks whether the processing is to be canceled.

S:

Cancels the processing if the **Yes** button is clicked and resumes processing if the **No** button is clicked.

O:

Install the product on a supported OS.

KNAG0004-E

The installation will be canceled because the service "*service-name*" is running.

Installation is being canceled because the service is already running.

S:

Cancels processing.

O:
Stop the service and then perform installation.

KNAG0005-E

An attempt to create a file has failed.

An attempt to create a file required for installation failed.

S:
Cancels processing.

O:
In the case of an overwrite installation or upgrade installation, check that you have write permissions for the folders and files under the installation folder, and then re-install the product. Otherwise, contact the system administrator.

KNAG0006-E

An attempt to register shared definition information has failed.

An attempt to register common definition information failed.

S:
Cancels processing.

O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0007-E

There is not enough memory. Stop any unnecessary applications, and then reattempt the installation.

Installation cannot be performed because of insufficient memory.

S:
Cancels processing.

O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0008-E

An attempt to acquire the product information failed because there are not enough resources. (details = *function-name, return-value*)

An attempt to acquire product information failed because of insufficient resources.

S:
Cancels processing.

O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0009-E

An attempt to acquire the product information failed because the environment is invalid. (details = *character-string, return-value*)

An attempt to acquire product information failed because of an invalid environment.

- S:
Cancels processing.
- O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0010-E

Code 9999: The media might be defective. Please contact the vendor.

The medium might be defective.

- S:
Cancels processing.
- O:
Contact the distributor.

KNAG0011-E

An internal error occurred. Use the data acquisition command to acquire data, and then contact the system administrator.

An internal error occurred.

- S:
Cancels processing.
- O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0012-E

Information could not be acquired from the registry.

Information could not be acquired from the registry.

- S:
Cancels processing.
- O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0013-E

An attempt to open a file has failed. Unopened file : *file-name*

An attempt to open a file has failed.

S:
Cancels processing.

O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG0014-E

This platform is unsupported. Installation will now be cancelled.

This platform is unsupported.

S:
Cancels processing.

O:
Install the product on a supported OS.

9.3.2 Messages related to execution of commands (KNAG1000 to KNAG1999)

KNAG1000-I

The setup command ended successfully.

The setup command terminated normally.

KNAG1001-I

The cluster setup command ended successfully.

The cluster setup command terminated normally.

KNAG1002-E

A folder could not be created on the shared disk.

An attempt to create a folder on the shared disk failed.

S:
Cancels command processing.

O:
Make sure that the shared disk is accessible.
When the shared disk is accessible, re-execute cluster setup of JP1/IM - EG for NNMi.

KNAG1004-I

The cluster setup command will start.

The cluster setup command has executed.

KNAG1005-E

A command option is invalid.

The format of a command argument is invalid.

S:

 Cancels command processing.

O:

 Check and revise the command arguments, as necessary.

KNAG1006-E

The option "*option-name*" has been duplicated.

The indicated command option was specified more than once.

S:

 Cancels command processing.

O:

 Specify the arguments correctly, according to the Usage description that is output after the error message.

KNAG1007-E

The specified logical host "*logical-host-name*" does not exist.

The specified logical host name does not exist.

S:

 Cancels command processing.

O:

 Correct the logical host name specification and then re-execute the data collection tool.

KNAG1008-E

A host has not been specified for the -h option.

A host name is missing in the -h option.

S:

 Cancels command processing.

O:

 Correct the logical host name specification and then re-execute the data collection tool.

KNAG1009-E

The shared directory "*shared-directory-path*" used by the specified logical host "*logical-host-name*" cannot be found.

The shared directory used by the indicated logical host cannot be found.

S:

Resumes command processing.

O:

If the host is at the primary node, mount the shared directory and then re-execute the data collection tool. If the host is at the secondary node, there is no problem because the shared directory is not mounted.

KNAG1010-E

The specified directory "*data-storage-directory-name*" is invalid.

The specification of the indicated directory is not valid. The directory might not exist.

S:

Cancels command processing.

O:

Specify the correct data storage directory and then re-execute the data collection tool.

In Windows, check the following:

- The specification does not include a reserved device name (AUX, CON, NUL, PRN, COM1 through COM9, LPT1 through LPT9) or any of the symbols ; % & ^ !.
- The length of the specified directory name does not exceed 128 bytes.

KNAG1011-W

A file (*file-name*) with the same name as the directory already exists.

A file with the same name as the directory already exists.

S:

Cancels command processing.

O:

Delete the file with the same name and then re-execute the data collection tool.

KNAG1012-E

The directory "*directory-name*" could not be written to.

The execution user does not have the permissions to write to the indicated directory.

S:

Cancels command processing.

O:

Make sure that the following are true and then re-execute the command:

- The execution user has write permissions for the directory.
- The disk has sufficient capacity.

KNAG1013-W

The directory "*directory-path*" used by a physical host does not exist.

The indicated directory used by the physical host does not exist.

S:

Resumes processing without collecting data under the directory path.

O:

Make sure that the directory path is not disconnected temporarily.

KNAG1014-E

The command "*command-name*" does not exist.

The indicated command does not exist.

S:

Cancels command processing.

O:

Check if the command has been deleted. If the command does not exist, re-install JP1/IM - EG for NNMi.

KNAG1015-W

The command "*command-name*" does not exist.

The indicated command does not exist.

S:

Resumes command processing.

O:

Check if the command has been deleted. If the command does not exist, re-install JP1/IM - EG for NNMi.

KNAG1016-E

There is not enough disk space to execute the command.

There is not enough disk space to execute the command.

S:

Cancels command processing.

O:

Check the available disk space, provide more free space by deleting unneeded files, and then re-execute the data collection tool. Delete data collected previously by the tool if it still remains on the disk.

KNAG1017-E

There is not enough memory to execute the command.

There is not enough memory to execute the command.

S:

Cancels command processing.

O:

Check the available system memory, provide more memory by terminating unneeded processes, and then re-execute the data collection tool.

KNAG1018-W

An attempt to acquire the Windows event log "*type-of-event-log*" has failed.

An attempt to collect the Windows event log failed.

type-of-event-log: System or Application

S:

Resumes command processing.

O:

Use the Event Viewer to collect the Windows event log manually.

KNAG1019-E

The specified file "*file-name*" cannot be read.

The specified file cannot be read.

S:

Cancels command processing.

O:

Make sure that you have read permissions for the specified file and then re-execute the command.

KNAG1020-E

The specified file "*file-name*" does not exist.

The specified file does not exist.

S:

Cancels command processing.

O:

Specify a file that exists and then re-execute the data collection tool.

KNAG1021-E

A file (*file-name*) with the same name as the directory already exists.

A file with the same name as the specified data storage directory already exists.

S:

Cancels command processing.

O:

Specify another directory or delete the file with the same name, and then re-execute the data collection tool.

KNAG1022-E

The specified directory "*directory-name*" cannot be written to.

An attempt to write to the specified data storage directory failed.

S:

Cancels command processing.

O:

Specify another directory, or check and revise (if necessary) the execution user's write permissions for the higher directory of the specified directory, and then re-execute the data collection tool.

KNAG1023-E

An attempt to create the directory "*directory-name*" has failed.

An attempt to create the indicated directory failed.

S:

Cancels command processing.

O:

Specify another directory, or check and revise (if necessary) the execution user's write permissions for the higher directory of the specified directory, and then re-execute the data collection tool.

KNAG1024-I

Data was successfully acquired.

This message reports that data has been collected successfully.

KNAG1025-E

Some of the data could not be acquired.

Some data could not be acquired. This message is displayed after the message that was displayed during execution.

S:

Terminates command processing.

O:

Take appropriate action according to the information in the message that was displayed during execution.

KNAG1026-I

information will be acquired.

This message reports that the indicated information is being acquired.

S:

Resumes command processing.

KNAG1027-I

"*information*" has been acquired.

This message reports that the indicated information has been acquired.

S:

Resumes command processing.

KNAG1028-W

"*information*" could not be acquired.

This is a warning message reporting that the indicated information was not acquired.

S:

Resumes command processing.

O:

If there is data to be collected, collect it manually by referencing *10.3 Data to be collected in the event of an error*.

KNAG1029-I

The directory "*directory-name*" already exists. The directory will be re-created.

The specified directory already exists and will be re-created.

S:

In Windows: If the user replies, the system deletes the directory and resumes processing.

In UNIX: The system resumes processing.

O:

In Windows: To continue the processing, press any key. To cancel the processing, press the **Ctrl + C** keys.

In UNIX: No action is required.

KNAG1030-I

The directory "*directory-name*" does not exist. The directory will be created.

The indicated directory does not exist and will be created.

S:

In Windows: If the user replies, the system creates the directory and resumes processing.

In UNIX: The system resumes processing.

O:

In Windows: To continue the processing, press any key. To cancel the processing, press the **Ctrl + C** keys.

In UNIX: No action is required.

KNAG1031-I

Data acquisition will now start.

Data acquisition is starting.

S:
Resumes command processing.

KNAG1032-I

Execution of the command "*command-name*" will now start.

Execution of the indicated command is starting.

S:
Resumes command processing.

KNAG1033-I

Execution of the command "*command-name*" will now end. (error level = *error-level*)

Execution of the indicated command has ended.

error-level: Command's return code

S:
Resumes command processing.

KNAG1034-I

"*information*" will be acquired. Please wait...

The indicated information is being acquired. Wait a while.

S:
Resumes command processing.

KNAG1035-E

An attempt to delete the directory "*directory-name*" has failed.

The attempt to delete the indicated directory failed.

S:
Cancels command processing.

O:
Make sure that the specified directory is not being used by another process or specify another directory, and then re-execute the data collection tool.

KNAG1036-E

An attempt to access the *information* registry has failed. (details = *detailed-information*)

An attempt to access the indicated information registry failed.

detailed-information: Argument passed to the RegOpenKeyEx/RegEnumKeyEx function and the return code

S:
Cancels command processing.

O:
Contact the system administrator.

KNAG1037-I

The following logical hosts are on this host: *logical-host-name* To acquire information about a logical host, execute the following command:

```
command-name -f output-directory-name -h logical-host-name
```

There are one or more logical hosts on this computer.

Execute *command-name -h logical-host-name* to obtain information about the logical host.

S:
Resumes command processing.

O:
Execute *command-name -h logical-host-name* to obtain information about the logical host.

KNAG1039-W

An attempt to create the directory "*directory-name*" has failed.

The attempt to create the indicated directory failed.

S:
Resumes command processing.

O:
Check and revise (if necessary) the execution user's write permissions for the higher directory of the specified directory, and then re-execute the data collection tool.

KNAG1040-W

An attempt to execute the command "*command-name*" has failed. (details = *detailed-information*)

An attempt to execute the indicated command failed.

detailed-information: Command's return code

S:
Resumes command processing.

O:
Take appropriate action according to the message that was displayed immediately before this message.

KNAG1041-I

The command "*command-name*" was successfully executed.

Execution of the indicated command was successful.

S:
Resumes command processing.

KNAG1042-E

You do not have the permission necessary to execute the command "*command-name*".

The user does not have the permissions required to execute the indicated command.

S:
Cancels command processing.

O:
Check the command execution permissions.

KNAG1043-I

The thread dump file has been deleted.

Deletion of the thread dump file has been completed.

S:
Resumes command processing.

KNAG1044-I

Do you want to delete all the core dump files in the directory "*directory-name*"? [yes/no]

This is a confirmation message asking whether the core dump files under the indicated directory are to be deleted.

S:
If the user enters *yes* or *y*, the system deletes the core dump files and then terminates command processing. If the user enters *no* or *n*, the system terminates command processing without deleting the core dump files.

O:
To delete the core dump files, enter *yes* or *y*. To cancel deletion of the core dump files, enter *no* or *n*.

KNAG1045-I

Do you want to delete all the thread dump files in the directory "*directory-name*"? [yes/no]

This is a confirmation message asking whether the thread dump files under the indicated directory are to be deleted.

S:
If the user enters *yes* or *y*, the system deletes the thread dump files and then terminates command processing. If the user enters *no* or *n*, the system terminates command processing without deleting the thread dump files.

O:
To delete the thread dump files, enter *yes* or *y*. To not delete the thread dump files, enter *no* or *n*.

KNAG1046-E

The file cannot be written to because a file with the name "*file-name*" already exists.

A write operation failed because the specified file already exists.

S:

Resumes processing without creating a file.

O:

Check the write permissions for the file. If the file is not needed, delete it and then re-execute the data collection tool.

KNAG1047-I

"file-name" already exists. Do you want to overwrite it? [yes/no]

This is a configuration message asking whether the indicated file, which already exists, is to be overwritten.

S:

If the user enters `yes` or `y`, the system overwrites the file and resumes command processing. If the user enters `no` or `n`, the system resumes command processing without overwriting the file.

O:

To overwrite the file, enter `yes` or `y`. To not overwrite the file, enter `no` or `n`.

KNAG1048-I

Is the device *"device-name"* ready? [yes/no]

This is a confirmation message asking whether the device is ready.

S:

If the user enters `yes` or `y`, the system performs data collection on the device and then resumes command processing. If the user enters `no` or `n`, the system resumes command processing without performing data collection on the device.

O:

To perform data collection on the device, enter `yes` or `y`. To not perform data collection on the device, enter `no` or `n`.

KNAG1050-E

The value of the option *"option-name"* is invalid.

The specified option value is invalid.

S:

Cancels command processing.

O:

Check and revise (if necessary) the option value and then re-execute the command.

KNAG1051-E

Setup has not been performed yet.

The `-list` or the `-update` option cannot be specified before setup has been completed.

S:

Cancels command processing.

O:
Execute new setup and then re-execute the command.

KNAG1052-E

The operation information file "*file-name*" already exists.

The shared directory specified in the `-d` option of the `jegn_setup_cluster` command already contains the operation information file.

S:
Cancels command processing.

O:
Either delete the existing operation information file or change the shared directory, and then re-execute the command.

KNAG1053-E

The file "*file-name*" could not be written to.

An attempt to write to the indicated file failed because the execution user did not have the required permissions.

S:
Cancels command processing.

O:
Check and revise (if necessary) the execution user's write permissions for the file and then re-execute the command.

KNAG1054-E

An attempt to update the registry information "*registry-key*" has failed.

An attempt to update the indicated registry information (such as common definition information or service registration) has failed.

S:
Cancels command processing.

O:
Use the data collection tool to collect data and then contact the system administrator.

KNAG1055-I

The core dump file "*file-name*" has been successfully deleted.

Deletion of the core dump file has been completed.

S:
Resumes command processing.

KNAG1056-E

Setup has already been performed.

Setup has already been performed, but an attempt was made to perform a new setup.

S:

Cancels command processing.

O:

Use the `-list` option to check the settings, specify the `-update` option and the options whose settings are to be changed, and then re-execute the command.

KNAG1057-E

Administrator permissions are required to execute the command.

This command must be executed by a user who has Administrator permissions.

S:

Cancels command processing.

O:

Check that the user has the Administrator permissions and then re-execute the command.

KNAG1058-E

Execute the command from the administrator console.

This command must be executed at the administrator console.

S:

Cancels command processing.

O:

Re-execute the command at the administrator console.

KNAG1059-E

The system environment is invalid. (*location, reason-code*)

The command cannot be executed because the system environment is invalid.

S:

Cancels command processing.

O:

Execute installation and setup again.

KNAG1060-E

An attempt to open a message file has failed.

An attempt to open a message file failed.

S:

Cancels command processing.

O:

In Windows:

Use the data collection tool to collect data and then contact the system administrator.

In UNIX:

Possible causes are listed below. Check the environment.

- The user might not have read permissions for the files under `/opt/jpleg4nnmi/lib/nls`. Grant the read permissions.
- The number of open files might have reached the maximum permitted in the system. If necessary, revise the kernel parameter.
- A temporary memory shortage might have occurred. Re-execute the command. Or, terminate any unneeded process.
- The directory or file might have been deleted. Re-install it.

If the problem cannot be resolved, use the data collection tool to collect data and then contact the system administrator.

KNAG1061-E

The specified logical host name is invalid.

The specified logical host name is invalid.

S:

Cancels command processing.

O:

Check and revise (if necessary) the logical host name or specify the correct logical host name, and then re-execute the command.

KNAG1063-E

An attempt to register shared definition information has failed.

An attempt to register common definition information failed.

S:

Cancels command processing.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG1064-E

The logical host name specified for the argument does not exist.

The logical host specified in the argument does not exist.

S:

Cancels command processing.

O:

Check if the specified logical host was set correctly.

KNAG1066-E

A setting in the shared definition information is invalid.

A setting in the common definition information is invalid.

S:

 Cancels command processing.

O:

 Make sure that the common definition information set at the primary node has been migrated to the secondary node, and then re-execute the `jegn_setup_cluster` command.

KNAG1067-E

An attempt to create the file "*file-name*" has failed.

An attempt to create the indicated file failed.

S:

 Cancels command processing.

O:

 Use the data collection tool to collect data and then contact the system administrator.

KNAG1900-E

There is not enough memory. (*maintenance-information*)

A memory shortage has occurred.

S:

 Cancels command processing.

O:

 Use the data collection tool to collect data and then contact the system administrator.

KNAG1901-E

A system error occurred. (*maintenance-information*)

A system error occurred.

S:

 Cancels command processing.

O:

 Use the data collection tool to collect data and then contact the system administrator.

9.3.3 Messages related to services (KNAG2000 to KNAG2999)

KNAG2000-I

The JP1/IM-EG for NNMi service has started. (logical host name = *logical-host-name*)

The JP1/IM - EG for NNMi service has started.

In the case of the physical host, JP1_DEFAULT is displayed as the logical host name.

S:

The system started the JP1/IM - EG for NNMi service.

KNAG2001-E

An attempt to start the JP1/IM-EG for NNMi service has failed. (logical host name = *logical-host-name*)

An attempt to start the JP1/IM - EG for NNMi service has failed.

In the case of the physical host, JP1_DEFAULT is displayed as the logical host name.

S:

An attempt by the system to start the JP1/IM - EG for NNMi service has failed.

O:

Check the immediately preceding error message, eliminate the cause of the error, and then start the service again.

KNAG2002-E

Setup has not been performed yet.

An attempt to start the JP1/IM - EG for NNMi service has failed because the setup command (`jegn_setup`) has not been executed.

S:

An attempt by the system to start the JP1/IM - EG for NNMi service has failed.

O:

Execute the setup command (`jegn_setup`), make sure that setup is completed successfully, and then re-execute the command to start the service.

KNAG2003-I

The JP1/IM-EG for NNMi service has stopped. (logical host name = *logical-host-name*)

The JP1/IM - EG for NNMi service has stopped.

In the case of the physical host, JP1_DEFAULT is displayed as the logical host name.

S:

The system stopped the JP1/IM - EG for NNMi service.

KNAG2004-E

An attempt to stop the JP1/IM-EG for NNMi service has failed. (logical host name = *logical-host-name*)

An attempt to stop the JP1/IM - EG for NNMi service has failed.

In the case of the physical host, JP1_DEFAULT is displayed as the logical host name.

S:

An attempt by the system to stop the JP1/IM - EG for NNMi service has failed.

O:

Check the immediately preceding error message, eliminate the cause of the error, and then re-execute the command to stop the service.

KNAG2006-E

The JP1/IM-EG for NNMi service ended abnormally. (logical host name = *logical-host-name*)

The JP1/IM - EG for NNMi service terminated abnormally.

In the case of the physical host, JP1_DEFAULT is displayed as the logical host name.

S:

The system terminated the JP1/IM - EG for NNMi service abnormally.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2008-E

An attempt to read the forwarded NNMi incident information file has failed.

An attempt to read the NNMi incident forwarding information file resulted in an error.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2009-E

The file size of the forwarded NNMi incident information file has exceeded the limit (*file-size*).

The size of the NNMi incident forwarding information file exceeds the maximum size.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2010-E

An invalid item key has been specified. (line = *line-number*, item key = *item-key-name*)

The transferred NNMi incident information file contains an invalid item key.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2011-E

An invalid value has been specified. (line = *line-number*, item key = *item-key-name*, value = *item-value*)

An invalid value is specified for the item key in the transferred NNMi incident information file.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2012-E

An item key has been duplicated. (line = *line-number*, item key = *item-key-name*)

The same item key is specified more than once in the transferred NNMi incident information file.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2013-E

The format is invalid. (line = *line-number*)

The transferred NNMi incident information file contains a line in an invalid format.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2015-E

An attempt to read the action definition file has failed.

An attempt to read the operation definition file resulted in an error.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2016-E

The file size of the action definition file has exceeded the limit (*file-size*).

The size of the operation definition file has exceeded the maximum value.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2017-E

An invalid item key has been specified. (line = *line-number*, item key = *item-key-name*)

The operation definition file contains an invalid item key.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2018-E

An invalid value has been specified. (line = *line-number*, item key = *item-key-name*, value = *item-value*)

An invalid value is specified for an item key in the operation definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2019-E

A required item key has not been specified. (item key = *item-key-name*)

A required item key is missing in the operation definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2020-E

An item key has been duplicated. (line = *line-number*, item key = *item-key-name*)

The same item is specified more than once in the operation definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2021-E

The format is invalid. (line = *line-number*)

The operation definition file contains a line in an invalid format.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2032-E

An attempt to connect to the NNMi server has failed. (NNMi server name = *NNMi-server-name*)

An attempt to connect to the NNMi server failed.

S:

After the NNMI incident re-acquisition interval specified in the `jegn_setup` command has elapsed, the system will attempt to connect to the NNMi server again.

O:

Check that the NNMi server is running.

In the NNMi server is running, check the NNMi port number specified in the `jegn_setup` command for any errors. If the specified information is not correct, re-execute the `jegn_setup` command with the correct information specified, and then execute the `jegn_spm�_reload` command.

KNAG2033-E

An attempt to authenticate the NNMi server has failed. (NNMi server name = *NNMi-server-name*)

NNMi server authentication has failed.

S:

After the NNMI incident re-acquisition interval specified in the `jegn_setup` command has elapsed, the system will attempt to connect to the NNMi server again.

O:

Check that the NNMi server is running.

In the NNMi server is running, check the NNMi user name and password specified in the `jegn_setup` command for any errors. If the specified information is not correct, re-execute the `jegn_setup` command with the correct information specified, and then execute the `jegn_spmd_reload` command.

KNAG2034-E

An attempt to analyze an NNMi incident has failed. (*maintenance-information*)

Analysis of an NNMi incident has failed.

S:

After the NNMI incident re-acquisition interval specified in the `jegn_setup` command has elapsed, the system will connect to the NNMi server again in order to acquire NNMi incidents.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2036-E

An attempt to read the forwarded NNMi incident information file has failed.

An attempt to read the NNMi incident forwarding filter definition file resulted in an error.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2037-E

The file size of the forwarded NNMi incident information file has exceeded the limit (*file-size*).

The size of the NNMi incident forwarding filter definition file has exceeded the maximum size.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the NNMi incident forwarding filter definition file and correct its size so that it does not exceed the maximum. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2038-E

The number of exclusion condition blocks has exceeded the limit (*maximum-value*).

The number of forwarding condition blocks in the NNMi incident forwarding filter definition file has exceeded the maximum.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Revise the NNMi incident forwarding filter definition file so that the number of forwarding condition blocks does not exceed the maximum. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2039-E

An exclusion condition block has been duplicated. (line = *line-number*)

An exclusion condition block is duplicated in the NNMi incident forwarding filter definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2040-E

An invalid item key has been specified. (line = *line-number*, item key = *item-key-name*)

The NNMi incident forwarding filter definition file contains an invalid item key.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the item key indicated by *line-number* and *item-key-name* in the message, and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2041-E

An invalid operator has been specified. (line = *line-number*, operator = *operator-name*)

The NNMi incident forwarding filter definition file contains an invalid operator.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the operator indicated by *line-number* and *operator-name* in the message, and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2042-E

The number of operands is invalid. (line = *line-number*, operator = *operator-name*, number of operands = *operands-count*)

The number of operands in a conditional statement is invalid in the NNMi incident forwarding filter definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the operand indicated by *line-number* and *operator-name* in the message, and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2043-E

An invalid operand has been specified. (line = *line-number*, operator = *operator-name*)

An operand is invalid in the NNMi incident forwarding filter definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the operand indicated by *line-number* and *operator-name* in the message, and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2046-E

The message mapping definition has been duplicated. (line = *line-number*)

The message mapping definition is duplicated in the NNMi incident forwarding filter definition file

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and delete the duplicate message mapping definition. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2047-E

An invalid item key has been specified in the message mapping definition. (line = *line-number*, item key = *item-key-name*)

The message mapping definition in the NNMi incident forwarding filter definition file contains an invalid item key name.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the item key indicated by *line-number* and *item-key-name* in the message, and correct the item key. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2048-E

The severity-level mapping definition has been duplicated. (line = *line-number*)

The severity-level mapping definition is duplicated in the NNMi incident forwarding filter definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and delete the duplicate severity-level mapping definition. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2049-E

An invalid item key has been specified in the severity level mapping definition. (line = *line-number*, item key = *item-key-name*)

The severity-level mapping definition in the NNMi incident forwarding filter definition file contains an invalid item key name.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.

- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the item key indicated by *line-number* and *item-key-name* in the message, and correct the item key. Then start the service or re-execute the `jegn_spm�_reload` command.

KNAG2050-E

An extended attribute mapping definition has been duplicated. (line = *line-number*)

An extended attribute mapping definition is duplicated in the NNMi incident forwarding filter definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and delete the duplicate extended attribute mapping definition. Then start the service or re-execute the `jegn_spm�_reload` command.

KNAG2051-E

An invalid item key has been specified in an extended attribute mapping definition. (line = *line-number*, item key = *item-key-name*)

The extended attribute mapping definition in the NNMi incident forwarding filter definition file contains an invalid item key name.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the item key indicated by *line-number* and *item-key-name* in the message, and then correct the item key. Then start the service or re-execute the `jegn_spm�_reload` command.

KNAG2052-E

An item key has been duplicated in an extended attribute mapping definition. (line = *line-number*, item key = *item-key-name*)

An item key specified in an extended attribute mapping definition is duplicated in the NNMi incident forwarding filter definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the item key indicated by *line-number* and *item-key-name* in the message, and delete the duplicate item key. Then start the service or re-execute the `jegn_spm�_reload` command.

KNAG2053-E

The format is invalid. (line = *line-number*)

The NNMi incident forwarding filter definition file contains a line with an invalid format.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spm�_reload` command.

KNAG2055-E

An attempt to register a JP1 event failed. (*maintenance-information*)

An attempt to register a JP1 event resulted in an error.

S:

Cancels the JP1 event registration processing. When the NNMI incident re-acquisition interval specified in the `jegn_setup` command has elapsed, the system attempts again to acquire NNMi incidents and perform JP1 event issuance processing.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2057-E

An attempt to read the category-label mapping file has failed.

An attempt to read the mapping definition file (for category) resulted in an error.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2058-E

The file size of the category-label mapping file has exceeded the limit (*file-size*).

The size of the mapping definition file (for category) has exceeded the maximum size.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the mapping definition file (for category) and revise it so that the maximum size is not exceeded. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2059-E

An invalid key has been specified. (line = *line-number*, item key = *key-name*)

An invalid key is specified in the mapping definition file (for category).

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the key indicated by *line-number* and *key-name* in the message, and then correct the mapping definition file (for categories). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2060-E

An invalid display name has been specified. (line = *line-number*, item key = *key-name*, display name = *display-name*)

An invalid display name (label) is specified in the mapping definition file (for category).

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the display name indicated by *line-number*, *key-name*, and *display-name* in the message, and then correct the mapping definition file (for category). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2061-E

Keys have been duplicated. (line = *line-number*, key = *key-name*)

The same key is specified more than once in the mapping definition file (for category).

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the key indicated by *line-number* and *key-name* in the message, and then correct the mapping definition file (for category). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2062-E

The format is invalid. (line = *line-number*)

The mapping definition file (for category) contains a line with an invalid format.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and correct the mapping definition file (category). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2064-E

An attempt to read the family-label mapping file has failed.

An attempt to read the mapping definition file (for family) resulted in an error.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2065-E

The file size of the family-label mapping file has exceeded the limit (*file-size*).

The size of the mapping definition file (for family) has exceeded the maximum size.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the mapping definition file (for family) and revise it so that the maximum size is not exceeded. Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2066-E

An invalid key has been specified. (line = *line-number*, item key = *key-name*)

An invalid key is specified in the mapping definition file (for family).

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the key indicated by *line-number* and *key-name* in the message, and then correct the mapping definition file (for family). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2067-E

An invalid display name has been specified. (line = *line-number*, item key = *key-name*, display name = *display-name*)

An invalid display name (label) is specified in the mapping definition file (for family).

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the display name indicated by *line-number*, *key-name*, and *display-name* in the message, and then correct the mapping definition file (for family). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2068-E

Keys have been duplicated. (line = *line-number*, key = *key-name*)

The same key is specified more than once in the mapping definition file (for family).

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the key indicated by *line-number* and *key-name* in the message, and then correct the mapping definition file (for family). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2069-E

The format is invalid. (line = *line-number*)

The mapping definition file (for family) contains a line with an invalid format.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the `jegn_spmd_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the line indicated by *line-number* in the message and correct the mapping definition file (family). Then start the service or re-execute the `jegn_spmd_reload` command.

KNAG2070-E

The system environment is invalid. (*location, reason-code*)

The service cannot be executed because the system environment is not valid.

S:

Terminates the service startup processing.

O:

Execute installation and setup again.

KNAG2071-E

An attempt to open the message file has failed.

An attempt to open the message file failed.

S:

Terminates command processing.

O:

In Windows:

Use the data collection tool to collect data and then contact the system administrator.

In UNIX:

Possible causes are listed below. Check the environment.

- The user might not have read permissions for the files under `/opt/jpleg4nnmi/lib/nls`. Grant read permissions.
- The number of open files might have reached the maximum permitted in the system. Check and revise (if necessary) the kernel parameter.
- A temporary memory shortage might have occurred. Re-execute the command. Also terminate any unneeded process.
- The directory or file might have been deleted. Re-install it.

If the problem cannot be resolved, use the data collection tool to collect data and then contact the system administrator.

KNAG2072-E

The number of extended attribute mapping definitions has exceeded the limit (*maximum-value*). (*line = line-number, number of definitions = definitions-count*)

The number of extended attribute mapping definitions has exceeded the maximum.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.

- When the `jegn_spm�_reload` command is executing: The system resumes processing using the unupdated information.

O:

Check the indicated line in the message and correct the NNMi incident forwarding filter definition file. Then start the service or re-execute the `jegn_spm�_reload` command.

KNAG2074-E

The loading of the CIA Mapping file failed.

An attempt to read the custom attribute mapping definition file resulted in an error.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the reload command is executing: The system resumes processing using the reload information.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2075-E

Exceeded the limit (*file-size*). of the CIA Mapping file size.

The custom attribute mapping definition file has exceeded the maximum size limit.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the reload command is executing: The system resumes processing using the reload information.

O:

- When the JP1/IM - EG for NNMi service is running: Check the custom attribute mapping definition file and revise it so that it does not exceed the maximum size limit. Then start the service.
- When the reload command is executing: Check the custom attribute mapping definition file and revise it so that it does not exceed the maximum size limit. Then execute the reload command again.

KNAG2076-E

Duplicated NNMi incident name cannot be specified. (line number: *line-number*)

An invalid key is specified in the custom attribute mapping definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the reload command is executing: The system resumes processing using the reload information.

O:

- When the JP1/IM - EG for NNMi service is running: Check the line indicated by the line number in the message and edit the custom attribute mapping definition file. Then start the service.
- When the reload command is executing: Check the line indicated by the line number in the message and edit the custom attribute mapping definition file. Then execute the reload command again.

KNAG2077-E

An invalid key is specified. (line number: *line-number*, key name: *key-name*)

The same key is specified more than once in the custom attribute mapping definition file.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the reload command is executing: The system resumes processing using the reload information.

O:

- When the JP1/IM - EG for NNMi service is running: Check the key indicated by the line number and key name in the message, and edit the custom attribute mapping definition file. Then start the service.
- When the reload command is executing: Check the key indicated by the line number and key name in the message, and edit the custom attribute mapping definition file. Then execute the reload command again.

KNAG2078-E

An invalid format line. (line number: *line-number*)

The custom attribute mapping definition file contains a line with an invalid format.

S:

- When the JP1/IM - EG for NNMi service is running: The system stops the JP1/IM - EG for NNMi service.
- When the reload command is executing: The system resumes processing using the reload information.

O:

- When the JP1/IM - EG for NNMi service is running: Check the line indicated by the line number in the message and edit the custom attribute mapping definition file. Then start the service.
- When the reload command is executing: Check the line indicated by the line number in the message and edit the custom attribute mapping definition file. Then execute the reload command again.

KNAG2900-E

There is not enough memory. (*maintenance-information*)

A memory shortage has occurred.

S:

Stops the JP1/IM - EG for NNMi service.

O:

Use the data collection tool to collect data and then contact the system administrator.

KNAG2901-E

A system error occurred. (*maintenance-information*)

S:

Stops the JP1/IM - EG for NNMi service.

O:
Use the data collection tool to collect data and then contact the system administrator.

9.3.4 Messages related to process management (KAVB3501 to KAVB3999)

Notes:

- In addition to the messages listed here, other messages with message IDs (such as internal error messages) might also be displayed.
- Messages related to process management might also be output by other programs, such as JP1/Base and JP1/IM - Manager (if installed). For details about messages output by programs other than JP1/IM - EG for NNMi, see the appropriate documentation for the specific products.

KAVB3501-E

An attempt to open the message file has failed.

An attempt to open the message file failed.

S:
Terminates process management.

O:
In Windows:
Use the data collection tool to collect data and then contact the system administrator.

In UNIX:
Possible causes are listed below. Check the environment.

- The user might not have read permissions for the files under `/opt/jpleg4nnmi/lib/nls`. Grant read permissions.
- The number of open files might have reached the maximum permitted in the system. Check and revise (if necessary) the kernel parameter.
- A temporary memory shortage might have occurred. Re-execute the command. Also terminate any unneeded process.
- The directory or file might have been deleted. Re-install it.

If the problem cannot be resolved, use the data collection tool to collect data and then contact the system administrator.

KAVB3502-E

An attempt to read the message file has failed.

An attempt to read the message file has failed.

S:
Does not output messages.

O:
Check if JP1/Base was set up successfully.

KAVB3503-E

An attempt to read the message file has failed.

An attempt to read the message file has failed.

S:

Does not output messages.

O:

Check if there is a message file (`jegnspm.cat`) under the `/opt/jp1eg4nnmi/lib/nls` directory and whether the reference permissions are appropriate.

KAVB3504-E

An error occurred in internal processing to output a message.

An error occurred during internal processing for message output.

S:

Does not output messages.

O:

Check for a shortage of system resources.

KAVB3516-E

An attempt to start the process management has failed. (`errno = request-code`)

An attempt to start process management failed.

S:

Terminates process management.

O:

Check if the product has been installed correctly.

KAVB3552-E

component-name name-of-managed-process has timed out.

The request resulted in a timeout. *component-name* indicates `JP1_EGN`. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

O:

In the case of the reload request, check integrated trace logs to see if there are any log entries for errors in definition files. If you find an error, correct the error in the relevant definition file and then execute the `jegn_spm_reload` command.

If no error on definition files is found, increase the timeout value and then re-execute the command.

Otherwise, wait a while and then re-execute the request.

If the same event occurs after re-execution, collect the required data using the data collection tool and contact the system administrator.

KAVB3553-E

SIGKILL was sent to *name-of-managed-process* of *component-name*, but termination could not be detected.

After sending SIGKILL, the system was unable to determine whether termination occurred. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Terminates process management.

O:

Make sure that the indicated process is not running. If this process is running, terminate it manually.

KAVB3554-I

A *component-name* reload request has finished.

A reload request has been completed. *component-name* is JP1_EGN.

S:

Resumes processing.

KAVB3564-I

jegn_spmd: *component-name* will now start all inactive processes.

All managed processes that are currently inactive will be started. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3574-I

jegn_spmd_reload: A reload request will now be sent to all running processes of *component-name*.

The system will send a reload request to all managed processes that are active. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3577-I

jegn_spmd_stop: A stop request will now be sent to all processes of *component-name*.

The system will send a stop request to all managed processes. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3578-I

component-name has ended.

Process management is being terminated. *component-name* indicates JP1_EGN.

S:

Terminates process management.

KAVB3586-I

component-name has terminated.

Process management has terminated. *component-name* indicates JP1_EGN.

S:

Terminates process management.

KAVB3597-I

`jegn_spmc_stop -kill`: A forced stop (kill) will be performed on all processes of *component-name*.

All managed processes are being terminated forcibly. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3599-E

`main_loop`: An invalid request was received for Service Control Manager. (event ID = *request-type*)

An invalid request was received.

S:

Resumes processing.

O:

Use the data collection tool to collect data and then contact the system administrator.

KAVB3602-I

component-name received a startup report from *name-of-managed-process*.

A startup completion notification has been received. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3603-I

All processes of *component-name* are running.

All managed processes have started. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3604-I

component-name startup has finished.

Service startup processing has been completed. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3605-I

component-name completed to send the start up request to the *name-of-managed-process*.

Startup processing for the indicated managed process, which terminated abnormally, has been completed. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3608-I

component-name received a reload-completed notification from *name-of-managed-process*.

A reload completion notification was received from the indicated managed process. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3609-I

A *component-name* reload request has finished.

Reload processing has been completed for all managed processes. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3610-I

component-name received an termination notification from *name-of-managed-process*.

A termination notification was received from the indicated managed process. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3612-I

A stop request will now be sent to all processes of *component-name*.

A termination request is being sent to all managed processes. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3613-W

A *component-name* timeout occurred in *name-of-managed-process*. Processing continues.

Startup processing for the indicated managed process resulted in a timeout. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

O:

Wait a while. If the service does not start because startup processing for the managed process still isn't completed, use the `jegn_spm�_stop -kill` command to restart the service.

KAVB3614-E

Process management will now stop because an invalid *component-name* status occurred.

Process management is being terminated because of an invalid status. *component-name* indicates JP1_EGN.

S:

Terminates command processing.

O:

Use the data collection tool to collect data and then contact the system administrator.

KAVB3616-I

Restart of the *component-name name-of-managed-process* has finished.

Restart has been completed for the indicated managed process, which had terminated abnormally. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3620-E

The user does not have permission to execute the command *execution-command-name*.

The user who attempted to execute the command does not have Administrator permissions.

S:

Does not execute the command.

O:

Have a user with Administrator permissions execute the command.

KAVB3621-E

A fork system call failed during initialization: *component-name*

A `fork` system call for background execution failed during process management startup processing. *component-name* indicates JP1_EGN.

S:

Terminates command processing.

O:

Make sure that there is sufficient system memory. Also check that the OS is running normally.

KAVB3623-E

The `setsid` function failed. (*description-of-error*)

A `setsid` system call failed.

S:

Terminates command processing.

O:

Make sure that there is sufficient system memory. Also check that the OS is running normally.

KAVB3624-E

An attempt to create a process management table has failed.

An attempt to create a process management table failed.

S:

Terminates the process management command.

O:

Make sure that there is sufficient system memory and check that the product has been installed correctly. Make sure that the settings are correct in the extended startup process definition file (`jegn_service_0700.conf`). Also make sure that processes managed by process management have terminated normally.

Delete the extended startup process definition file and then start process management.

KAVB3625-E

An internal error occurred. Execution Command names differ. *execution-command-name*

The execution command names do not match.

S:

Terminates command processing.

O:

Check the command name indicated as *execution-command-name*. If you have changed the command name (*execution-command-name*), the command will no longer function.

KAVB3626-E

An attempt to create a lock file has failed. *lock-file-path-description-of-error*

An attempt to create a lock file has failed.

S:

Terminates the process management command.

O:

Check that the `conf` directory exists and that you have read and write permissions. In the case of operation in a cluster system, make sure that the defined `conf` directory exists and that the read and write permissions have been granted.

KAVB3627-I

component-name is already running.

An attempt was made to start the same service more than once concurrently. *component-name* indicates JP1_EGN.

S:

Terminates the process management command.

KAVB3631-E

`build_proc_table` : The return value NULL was returned to the `getfield` function. *setting*

The extended startup process definition file (`jeng_service_0700.conf`) contains an invalid entry.

S:

Terminates command processing.

O:

Make sure that the entries in the extended startup process definition file are correct.

KAVB3642-E

An internal error occurred. Component names differ. *component-name*

The component names do not match. *component-name* indicates JP1_EGN.

S:

Terminates command processing.

O:

Use the data collection tool to collect data and then contact the system administrator.

KAVB3643-E

An attempt to open the environment definition file *file-name* has failed.

An attempt to open the environment definition file failed.

S:

Terminates command processing.

O:

Check that the product has been installed correctly.

KAVB3644-E

An attempt to expand the environment variables has failed.

An attempt to load environment variables from `jegn_spm�_env.conf` failed.

S:

Terminates command processing.

O:

Make sure that the system has sufficient memory.

KAVB3645-I

The logical hostname for process management is *logical-host-name*.

Process management is starting on the logical host.

S:

Resumes processing.

KAVB3646-I

The *option-name* option is specified.

Process management is starting with an option in effect.

S:

Resumes processing.

KAVB3647-E

The expiration of the time limit. JP1/IM-EG for NNMi

The evaluation version has expired.

S:

Cancels processing.

KAVB3649-E

The environment variable of JP1_HOSTNAME is empty.

Specification of the JP1_HOSTNAME environment variable is invalid.

S:

Terminates the process management command.

O:

Either specify the correct logical host name in the JP1_HOSTNAME environment variable or delete the JP1_HOSTNAME environment variable.

KAVB3651-I

Startup processing for *component-name* has started.

Process management is starting a managed process. *component-name* indicates JP1_EGN.

S:

Process management starts the managed process.

KAVB3652-E

A timeout occurred during the wait for a response. (timeout period = *timeout-value* seconds)

A timeout occurred while the system was waiting for a response.

S:

Terminates the process management command.

O:

Change the timeout value and then re-execute the command.

KAVB3653-E

An attempt to send a request to the process management has failed.

Communication with process management from a process management command has failed.

S:

Terminates the process management command.

O:

Make sure that the `/var/opt/jpleg4nnmi/tmp` directory exists.

KAVB3654-E

An attempt to receive a response from the process management has failed.

Data reception processing from process management to a process management command has failed.

S:

Terminates the process management command.

O:

Restart process management and then re-execute the command.

KAVB3655-E

Invalid data was received from the process management.

A process management command received invalid data from process management.

S:
Terminates the process management command.

O:
Invalid data might have been received temporarily. Restart process management and then re-execute the command.

KAVB3656-I

The startup command terminated normally.

The process management startup command terminated normally.

S:
Terminates the process management command.

KAVB3657-E

The startup command terminated abnormally

The startup command terminated abnormally.

S:
Terminates the process management command.

O:
Use the `jegn_spm�_status` command to check the status and then re-execute the command.

KAVB3658-E

The startup command terminated abnormally due to an inconsistent state.

A command is executed while process management was performing other processing.

S:
Terminates the process management command.

O:
Wait a while, use the `jegn_spm�_status` command to check the status, and then re-execute the command.

KAVB3659-I

There were no processes that could run.

There is no process that can be started.

S:
Terminates the process management command.

KAVB3660-E

Invalid data was received.

The process management command received invalid data from process management.

S:
Terminates the process management command.

O:
Invalid data might have been received temporarily. Restart process management and then re-execute the command.

KAVB3661-E

An unexpected result code was received. (return code = *return-code*)

The process management command received an invalid result code from process management.

S:
Terminates the process management command.

O:
Use the `jegn_spm�_status` command to check the status, and then re-execute the command.

KAVB3662-I

The process management is not running.

Process management is not running.

S:
Terminates the process management command.

O:

- When the `jegn_start` command was executed
Either setup has not been executed or a definition might be invalid in the NNMi incident forwarding filter definition file.
Check the integrated trace log, take appropriate action according to the displayed messages, and then re-execute the command.

KAVB3663-E

Execute the command from the administrator console.

This command must be executed at the administrator console.

S:
Terminates command processing.

O:
Re-execute the command at the administrator console.

KAVB3672-I

A forced termination (kill) of *component-name* has started.

Forced termination of process management has begun. *component-name* indicates JP1_EGN.

S:

Terminates the process management command.

KAVB3674-I

Termination processing of *component-name* has started.

Termination processing of process management has begun. *component-name* indicates JP1_EGN.

S:

Terminates the process management command.

KAVB3675-I

The stop command terminated normally.

The process management termination command terminated normally.

S:

Terminates the process management command.

KAVB3676-E

The stop command terminated abnormally.

The process management termination command terminated abnormally.

S:

Terminates the process management command.

O:

Wait a while, use the `jegn_spm�_status` command to check the status, and then re-execute the command.

KAVB3677-E

The stop command terminated abnormally due to an inconsistent state.

The command was executed while process management was performing other processing.

S:

Terminates the process management command.

O:

Wait a while and then re-execute the command.

KAVB3678-I

There were no processes that could terminate.

There is no process that can be terminated.

S:

Terminates the process management command.

KAVB3680-I

Reload processing for *component-name* has started.

Reload processing of processes managed by process management has started. *component-name* indicates JP1_EGN.

S:

Terminates the process management command.

KAVB3681-I

The reload command terminated normally.

Process management's reload command terminated normally.

S:

Terminates the process management command.

KAVB3682-E

The reload command terminated abnormally.

Process management's reload command terminated abnormally.

S:

Terminates the process management command.

O:

Check if any of the managed processes has resulted in a reloading error.

KAVB3683-E

The reload command terminated abnormally due to an inconsistent state.

The command was executed while process management was performing other processing.

S:

Terminates the process management command.

O:

Wait a while and then re-execute the command.

KAVB3684-E

There were no processes that could be reloaded.

There is no process that can be reloaded.

S:
Terminates the process management command.

O:
Make sure that a managed process is running.

KAVB3685-E

A timeout occurred in *process-name*.

Reload processing for the indicated process resulted in a timeout.

S:
Terminates the process management command.

O:
Check if any of the managed processes has resulted in a reloading error.

KAVB3690-I

Processing to report the status of *component-name* has started.

Process management's status report processing has started. *component-name* indicates JP1_EGN.

S:
Terminates the process management command.

KAVB3691-I

All the processes have started.

All managed processes are running.

S:
Terminates the process management command.

KAVB3692-I

Some of the processes have started.

Some managed processes are running.

S:
Terminates the process management command.

KAVB3693-I

All of the processes have stopped.

All managed processes are stopped.

S:
Terminates the process management command.

KAVB3694-I

Part of the process is now restarting.

Part of process management is running.

S:

Terminates process management's status notification command.

KAVB3705-I

name-of-managed-process is now starting. (process ID = *process-ID*)

The indicated managed process is being started. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3732-I

component-name detected the termination of *name-of-managed-process*. (process ID = *process-ID*)

Termination of the indicated managed process was detected. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3736-I

All processes of *component-name* have stopped.

All managed processes have terminated. *component-name* indicates JP1_EGN.

S:

Terminates command processing.

KAVB3737-E

The *component-name name-of-managed-process* terminated abnormally

Abnormal termination of the indicated managed process was detected. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

O:

Check the integrated trace log output by the managed process that terminated abnormally and eliminate the cause of the error. Use the `jegn_spm�_status` command to check the status, and then restart. If no message has been output by the managed process, use the data collection tool to collect data and then contact the system administrator.

KAVB3743-I

component-name has terminated.

Process management has terminated. *component-name* indicates JP1_EGN.

S:

Terminates command processing.

KAVB3744-I

component-name startup has finished.

Service startup processing has been completed. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3745-I

The *component-name* startup request has finished.

The startup request has been processed to completion. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3752-E

An attempt to start *name-of-managed-process* has finished. (return code = *return-code*, detail code = *request-code*)

Startup processing for the indicated managed process has failed. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

O:

Use the data collection tool to collect data and then contact the system administrator.

KAVB3760-I

The changes to *file-name* were not applied.

The changes to the settings in the extended startup process definition file (*jegn_service_0700.conf*) were not applied.

S:

Resumes processing.

O:

Change the settings and then re-execute the command.

KAVB3761-E

In the file *file-name*, the restart-or-not value is invalid. (restart-or-not = *setting*)

The setting in the extended startup process definition file (`jegn_service_0700.conf`) for whether restart is to be permitted is not valid.

S:

Resumes processing.

O:

Change the setting and then re-execute the command.

KAVB3762-I

Set 0 or 1 for the restart-or-not value.

You must specify either 0 or 1 in the extended startup process definition file (`jegn_service_0700.conf`) as the setting for whether restart is to be permitted.

S:

Resumes processing.

O:

Specify either 0 or 1 for the restart setting.

KAVB3763-E

In the file *file-name*, the number-of-restarts value is invalid. (restart num. = *setting*)

The specification in the extended startup process definition file (`jegn_service_0700.conf`) for the restart count is not valid.

S:

Resumes processing.

O:

Change the setting and then re-execute the command.

KAVB3764-I

Set 0 to 99 for the number-of-restarts value.

You must specify a value in the range from 0 to 99 in the extended startup process definition file (`jegn_service_0700.conf`) as the setting for the restart count.

S:

Resumes processing.

O:

Specify a value in the range from 0 to 99 for the restart count.

KAVB3765-E

In the file *file-name*, the restart interval value is invalid. (restart interval = *setting*)

The specification in the extended startup process definition file (`jegn_service_0700.conf`) for the retry interval is not valid.

S:

Resumes processing.

O:

Change the setting and then re-execute the command.

KAVB3766-I

Set 0 to 3600 for the restart interval value.

You must specify a value in the range from 0 to 3,600 in the extended startup process definition file (`jegn_service_0700.conf`) as the setting for the retry interval.

S:

Resumes processing.

O:

Specify a value in the range from 0 to 3,600 for the retry interval.

KAVB3767-E

In the file *file-name*, the restart-count reset time is invalid. (restart-count reset time = *setting*)

The specification in the extended startup process definition file (`jegn_service_0700.conf`) for the restart-count reset time is not valid.

S:

Resumes processing.

O:

Change the setting and then re-execute the command.

KAVB3768-I

Set 3600 to 2147483647 for the restart-count reset time.

You must specify a value in the range from 3,600 to 2,147,483,647 in the extended startup process definition file (`jegn_service_0700.conf`) as the setting for the restart-count reset time.

S:

Resumes processing.

O:

Specify a value in the range from 3,600 to 2,147,483,647 for the restart-count reset time.

KAVB3769-I

In *file-name*, check the entries: process-name|path|startup-option|restart-or-not|number-of-restarts|restart-interval|restart-count-reset-time|

Check the indicated entries in the extended startup process definition file (`jegn_service_0700.conf`).

S:

Resumes processing.

O:

Check the entries in the extended startup process definition file.

KAVB3777-I

component-name: The stopped *name-of-managed-process* will be restarted. (restart count = *restart-count*)

The indicated managed process, which was terminated, is being restarted. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Restarts the indicated managed process.

KAVB3778-I

component-name: A startup request was sent to the process *name-of-managed-process*.

A start request was sent to the indicated managed process. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3779-I

component-name: An attempt to send a startup request to the process *name-of-managed-process* failed.

An attempt to send a startup request to the indicated managed process has failed. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

KAVB3786-E

To process *child-process-ID-of-managed-process*, the system sent the signal *signal-name*

The indicated signal was sent to the indicated child process of a managed process. *child-process-ID-of-managed-process* indicates the process ID of a process generated by the active managed process.

S:

Resumes processing.

KAVB3788-E

component-name: The number of restarts of *name-of-managed-process* exceeded the specified restart count.

The number of restart attempts for the indicated managed process has exceeded the specified maximum. *component-name* indicates JP1_EGN. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management.

S:

Resumes processing.

O:

Check the integrated trace log output by the managed process that terminated abnormally and eliminate the cause of the error. Use the `jegn_spmc_status` command to check the status, and then restart. If no message has been output by the managed process, use the data collection tool to collect data and then contact the system administrator.

KAVB3802-W

The process manager will not be monitored because an attempt to initialize the health check function failed.

Process management will not be monitored because initialization of the health check function failed.

S:

Resumes processing.

O:

To use the health check function to monitor process management, restart process management.

KAVB3840-E

The product information could not be acquired because there was not enough memory. (Detailed information : *function-name, return-value*)

An attempt to acquire product information failed because of insufficient resources.

S:

Cancels processing.

O:

Check for a shortage of system resources. After the resource shortage is resolved, re-execute the command. If the error cannot be resolved, use the data collection tool to collect data and then contact the system administrator.

KAVB3841-E

The product information could not be acquired because the environment is invalid. (Detail information : *function-name, return-value*)

An attempt to acquire product information failed because of an invalid environment.

S:

Cancels processing.

O:

Check for a system failure. Uninstall the product, reinstall it, and then re-execute the command.

KAVB3846-I

component-name completed the reload request.

Reload processing has been completed. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3855-I

The process *name-of-managed-process* will be terminated by SIGKILL. (process ID = *process-ID*)

SIGKILL has been sent to the indicated managed process. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3862-E

component-name: No processes could be started.

The system was unable to start any of the managed processes. *component-name* indicates JP1_EGN.

S:

Terminates command processing.

O:

Make sure that there is sufficient system memory and check if the product has been installed correctly.

KAVB3863-E

component-name: No processes can be reloaded.

None of the managed processes was ready to be reloaded. *component-name* indicates JP1_EGN.

S:

Resumes processing.

O:

Wait a while and then re-execute the command.

KAVB3870-E

The conf directory path cannot be obtained from the common definition.

An attempt to acquire the `conf` directory path from the common definition failed.

S:

Terminates the process management command.

O:

When operating in a cluster system:

Make sure that the correct logical host name is specified in the argument of the process management command. Also make sure that the correct logical host name is set in the JP1_HOSTNAME environment variable.

When not operating in a cluster system:

Make sure that the JP1_HOSTNAME environment variable is not used during startup. If the JP1_HOSTNAME environment variable is not set, perform a repair installation.

KAVB3871-E

The conf directory path cannot be obtained by using the specified logical hostname.

The attempt to acquire the `conf` directory path from the common definition using the specified logical host name has failed.

S:

Terminates the process management command.

O:

This operation assumes you are operating in a cluster system. Make sure that the specified logical host name is correct or that setup has been completed successfully.

KAVB3872-E

The log directory path cannot be obtained from the common definition information.

An attempt to acquire the `log` directory path from a common definition has failed.

S:

Terminates the process management command.

O:

If you are operating in a cluster system, make sure that the specified logical host name is correct or that setup has been completed successfully. If you are not operating in a cluster system, perform a repair installation.

KAVB3873-E

The log directory path cannot be obtained by using the specified logical hostname.

An attempt to acquire the `log` directory path from a common definition using the specified logical host name has failed.

S:

Terminates the process management command.

O:

This operation assumes you are operating in a cluster system. Make sure that the specified logical host name is correct or that setup has been completed successfully.

KAVB3874-E

HNTRLib could not be initialized.

Initialization of HNTRLib2 has failed. No log information will be output.

S:

Resumes processing.

O:

If process management was running, terminate it and then restart it.

KAVB3875-E

HNTRLib could not be initialized.

An attempt to initialize HNTRLib2 has failed. No log information will be output.

S:

Resumes processing.

O:

If process management was running, terminate it and then restart it.

KAVB3899-E

The work directory path cannot be acquired from the common definition information. (return code = *return-code*)

An attempt to acquire the `work` directory path from a common definition has failed.

S:

Terminates the process management command.

O:

If you are operating in a cluster system, make sure that the specified logical host name is correct or that setup has been completed successfully. If you are not operating in a cluster system, perform a repair installation.

KAVB3905-I

A stop request was sent to the process *name-of-managed-process*. (process ID = *process-ID*)

A termination request has been issued to the indicated managed process. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3908-I

A reload request was sent to the process *name-of-managed-process*. (process ID = *process-ID*)

A reload request has been issued to the indicated managed process. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3910-I

SIGTERM will terminate the process *name-of-managed-process*. (process ID = *process-ID*)

SIGTERM has been sent to the indicated managed process. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3911-E

The process management daemon is busy.

Some other command processing is underway.

S:

Terminates the process management command.

O:

Wait a while and then re-execute the command. If this message was displayed when the `jegn_spm�_reload` command was executed during startup, termination, or reload processing, wait until the other processing is completed, and then re-execute the command.

KAVB3912-I

The process is running.

S:

Terminates the process management command.

KAVB3913-I

The process is not running.

S:

Terminates the process management command.

KAVB3914-E

An attempt to open the lock file under the `conf` directory has failed.

An attempt to open the lock file in the `conf` directory has failed.

S:

Terminates the process management command.

O:

Check that there is a `conf` directory and that you have write permissions.

If you are operating in a cluster system, check that the defined `conf` directory exists and that you have write permissions.

KAVB3935-E

`create_pre_process_entry`: Memory allocation failed. (*request-code*)

Creation of a startup preprocessing management table has failed. Startup preprocessing is not being performed.

S:

Resumes processing.

O:

Check if a memory shortage occurred.

KAVB3960-I

Startup preprocessing is being performed.

Process management is engaged in startup preprocessing.

S:

Terminates process management's status notification command.

KAVB3961-E

The request could not be accepted because startup preprocessing is being performed.

Process management was unable to accept a command request because it was engaged in startup preprocessing.

S:

Terminates the process management command.

O:

Wait a while and then re-execute the command.

KAVB3981-I

`jegn_spm�_stop -job`: A request to stop job restrictions will be sent to all processes of *component-name*.

A job restriction stop request is being sent to all managed processes. *component-name* indicates JP1_EGN.

S:

Resumes processing.

KAVB3984-I

A request to stop job restrictions has been sent to the process *name-of-managed-process*. (process ID = *process-ID*)

A job restriction stop request has been sent to the indicated managed process. *name-of-managed-process* indicates the name of a process that constitutes a component managed by process management. *process-ID* indicates the process ID of the active managed process.

S:

Resumes processing.

KAVB3986-I

Processing to stop *component-name* job restrictions has started.

Process management's job restriction stop processing has started. *component-name* indicates JP1_EGN.

S:

Terminates the process management command.

10

Troubleshooting

This chapter describes how to handle problems that occur in JP1/IM - EG for NNMi.

10.1 Troubleshooting procedure

The following is the procedure for handling problems in JP1/IM - EG for NNMi:

1. Check the event

Check the event at the time of an error. If a message has been displayed, check its contents. If you are able to identify the cause of the error, correct it according to the error handling procedure.

2. Collect data

If the error cannot be resolved in step 1, or in the event of an internal error or a communication error, you must collect the data needed to determine the cause of the error. See *10.3 Data to be collected in the event of an error* and collect the required data.

3. Investigate the problem

Investigate the problem on the basis of the collected data and then isolate the problem or the extent of the problem.

10.2 Types of log information

JP1/IM - EG for NNMi outputs three types of log information while it is operating:

- Integrated trace log
- Trace log for issued JP1 events
- Trace logs for each process

This section describes these three types of log information.

10.2.1 Integrated trace log

The integrated trace log consists of the trace information output by the individual programs. It is output to a single file by the Hitachi Network Objectplaza Trace Library (HNTRLib2).

The default output destination for the integrated trace log is as follows:

In Windows (32-bit):

```
system-drive:\Program Files(x86)\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log
```

In Windows (64-bit):

```
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 any text editor to view the integrated trace log information. The following shows an output example of integrated trace log information.

Figure 10–1: Output example of integrated trace log information

The diagram illustrates the structure of an integrated trace log entry. It shows a sample log line with various fields and their corresponding labels. Red arrows point from the labels to the specific fields in the log line.

```

**** Microsoft WindowsNT5.2 (Build:3790) Service Pack 1
TZ=(local)-9:00          2009/08/02 16:04:23.343
  yyyy/mm/dd hh:mm:ss.sss          pid      tid      message-id
message (LANG=0x0411)
0062 2009/08/01 10:20:45.765   jegneg4nnmi   00001214 00000B4C KNAG2000-I
The JP1/IM - EG for NNMi service has started. (Logical hostname:HOST2)
  
```

Labels and their corresponding fields:

- Time zone:** Points to the time zone information in the first line.
- OS information:** Points to the OS version information in the first line.
- Start time of Hitachi Network Objectplaza Trace Library (HNTRLib2):** Points to the timestamp in the second line.
- Host name:** Points to the host name in the second line.
- Number:** Points to the message number (0062).
- Date:** Points to the date (2009/08/01).
- Time:** Points to the time (10:20:45.765).
- Application name:** Points to the application name (jegneg4nnmi).
- pid:** Points to the process ID (00001214).
- tid:** Points to the thread ID (00000B4C).
- Message ID:** Points to the message ID (KNAG2000-I).
- Message text:** Points to the message text (The JP1/IM - EG for NNMi service has started. (Logical hostname:HOST2)).

The tables below list and describe the header information and output items that are output to the integrated trace log.

Table 10–1: Header information in the integrated trace log

Header information	Description
OS information	Information about the OS on which the Hitachi Network Objectplaza Trace Library (HNTRLib2) is running
Host name	Name of the host at which the Hitachi Network Objectplaza Trace Library (HNTRLib2) is running

Header information	Description
Time zone	In Windows: Time zone of the OS In UNIX: Value of the TZ environment variable for the integrated trace process. If the TZ environment variable has not been set, Unknown is displayed.
Start time of Hitachi Network Objectplaza Trace Library (HNTRLib2)	Time the Hitachi Network Objectplaza Trace Library (HNTRLib2) started

Table 10–2: Output items in the integrated trace log

Output item	Description
Number	Trace record number (4 digits) This number is assigned to each process that outputs log information.
Date	Trace acquisition date: <i>yyyy/mm/dd</i> (year/month/date)
Time	Trace acquisition time (local time): <i>hh:mm:ss.sss</i> (hour:minute:second.millisecond)
Application name	Name that identifies the application (application ID name). JP1/IM - EG for NNMi outputs the following application names: <ul style="list-style-type: none"> JP1/IM - EG for NNMi service jegneg4nnmi Process management JEGN_SPMD
pid	Process ID (assigned by the OS)
tid	Thread ID (used for identifying threads)
Message ID	Message ID (see the explanation of the output format of messages) This is a message ID used by this product.
Message text	Message text that is output to the integrated trace log This is a message text output by this product.

Note:

The time of a log entry in the integrated trace log reflects the format for the time zone of the process that outputs the log.

Therefore, if a user changes the TZ environment variable and then starts a service or executes a command, the time might be output in a different format than that used for the time zone set in the OS.

10.2.2 Trace log for issued JP1 events

The trace log for issued JP1 events is used to output the conversion results when NNMi incidents are converted into JP1 events. You can use this log to obtain the results of filtering by the filter conditional statements in the NNMi incident forwarding filter definition file and to obtain the JP1 event issuance status.

The default output destinations for trace logs for issued JP1 events are as follows:

In Windows:

- Physical host: *EG-for-NNMi-path*\log\jegnevent{1|2|3|4}.log

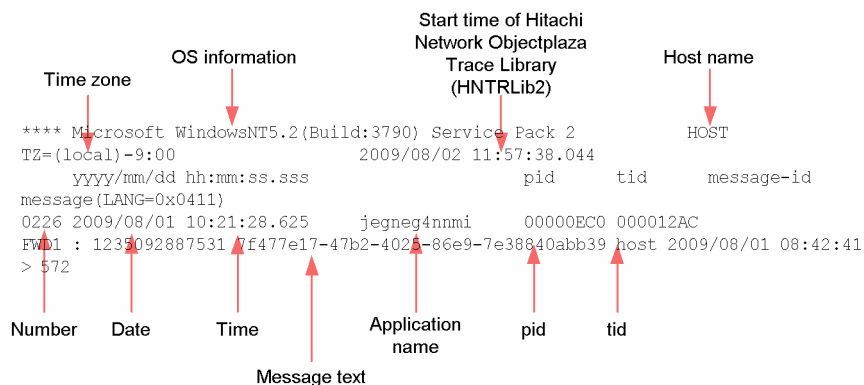
- Logical host: *shared-folder*\JP1EG4NNMI\log\jegnevent{1|2|3|4}.log

In UNIX:

- Physical host: /var/opt/jp1eg4nnmi/log/jegnevent{1|2|3|4}.log
- Logical host: *shared-directory*/jp1eg4nnmi/log/jegnevent{1|2|3|4}.log

You can use any text editor to view the trace logs for issued JP1 events. The following shows an output example of trace information for issued JP1 events.

Figure 10–2: Output example of trace log information for issued JP1 events



The tables below list and describe the header information and output items that are output to the trace logs for issued JP1 events.

Table 10–3: Header information in the trace log for issued JP1 events

Header information	Description
OS information	Information about the OS on which the trace function of JP1/IM - EG for NNMI is running
Host name	Name of the host at which the trace function of JP1/IM - EG for NNMI is running
Time zone	In Windows: Time zone of the OS In UNIX: Value of the TZ environment variable for the trace process. If the TZ environment variable has not been set, Unknown is displayed.
Trace function start time	Time the trace function of JP1/IM - EG for NNMI started

Table 10–4: Output items in the trace log for issued JP1 events

Output item	Description
Number	Trace record number (4 digits) This number is assigned to each process that outputs log information.
Date	Trace acquisition date: <i>yyyy/mm/dd</i> (year/month/date)
Time	Trace acquisition time (local time): <i>hh:mm:ss.sss</i> (hour:minute:second.millisecond)
Application name	Name that identifies the application (application ID name) JP1/IM - EG for NNMI outputs the following application names: <ul style="list-style-type: none"> • JP1/IM - EG for NNMI service jegneg4nnmi • Process management

Output item	Description
Application name	JEGN_SPMD
pid	Process ID (assigned by the OS)
tid	Thread ID (used for identifying threads)
Message text	Message text that is output to the trace log for issued JP1 events This is a message text output by this product.

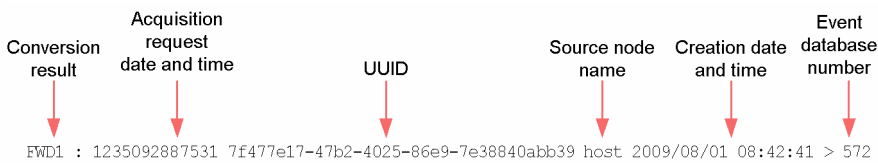
Format of message text

The following shows the format of the message texts that are output to the trace log for issued JP1 events:
*conversion-result*Δ*Δacquisition-request-date-and-time*Δ*UUID*Δ*source-node-name*Δ*creation-date-and-time*Δ*>*Δ*event-database-number*

Δ indicates one or more consecutive spaces or tabs.

The following shows an output example of a message text.

Figure 10–3: Output example of a message text in the trace log for issued JP1 events



The following table describes the items in the message text.

Table 10–5: Items in the message text in the trace log for issued JP1 events

Item	Description
Conversion result	Result of converting an NNMi incident into a JP1 event: <i>FWDn</i> Indicates that the NNMi incident was converted into a JP1 event because filter conditional statement <i>n</i> specified in the forwarding condition block were satisfied. <i>EXC</i> Indicates that the NNMi incident was not converted into a JP1 event because none of the filter conditional statements specified in the forwarding condition block was satisfied.
Acquisition request date and time	Date and time an NNMi incident acquisition request was issued to NNMi This value is expressed as the elapsed time in milliseconds since 1970-01-01 at 00:00:00 (world standard time).
UUID	UUID of the NNMi incident
Source node name	Source node name of the NNMi incident
Creation date and time	NNMi incident creation date and time (local time: <i>yyyy/mm/dd hh:mm:ss</i> (year/month/date hour:minute:second))
Event database number	Serial number of the JP1 event that was issued by converting the NNMi incident This item is output only when the conversion result is <i>FWDn</i> .

Note:

The time of a log entry in the trace log for issued JP1 events reflects the format for the time zone of the process that outputs the log.

Therefore, if a user changes the TZ environment variable and then starts a service or executes a command, the time might be output in a different format than that used for the time zone set in the OS.

10.2.3 Trace logs for each process

The trace logs for each process consist of log information that is output by each function of JP1/IM - EG for NNMi. The log information is output to a different log file for each function. Note that the contents of these trace logs are not disclosed because they contain product information.

10.3 Data to be collected in the event of an error

This section describes the data that needs to be collected when an error has occurred.

JP1/IM - EG for NNMi provides the data collection tool (`jegn_log` command) that collects the needed data in the batch mode. For details about the `jegn_log` command, see *jegn_log.bat (Windows only)* or *jegn_log.sh (UNIX only)* in 7. *Commands*.

The following describes the data that needs to be collected in Windows and UNIX.

10.3.1 Data to be collected (in Windows)

This subsection describes the data to be collected in Windows when an error has occurred.

The data collection tool (`jegn_log.bat` command) classifies the target folders and files for data collection into primary data and secondary data categories and then stores the collected data directly under the specified *data storage folder*.

The following tables show the organization of folders for the data that is stored directly under the data storage folder and their contents.

Table 10–6: Organization and contents of data folders (physical host)

Folder name	Type	Data that is stored
<code>data-storage-folder\jp1_default\eg4nnmi_1st\oslog</code>	Primary data	OS log information
<code>data-storage-folder\jp1_default\eg4nnmi_1st\spool</code>		Integrated trace log
<code>data-storage-folder\jp1_default\eg4nnmi_1st\eg4nnmi</code>		Information about JP1/IM - EG for NNMi
<code>data-storage-folder\jp1_default\eg4nnmi_1st\base</code>		Information about JP1/Base
<code>data-storage-folder\jp1_default\eg4nnmi_1st\ucpsb</code>		Information about Web server
<code>data-storage-folder\jp1_default\eg4nnmi_2nd\oslog</code>	Secondary data	OS log information
<code>data-storage-folder\jp1_default\eg4nnmi_2nd\base</code>		Information about JP1/Base

Table 10–7: Organization and contents of data folders (logical host)

Folder name	Type	Data that is stored
<code>data-storage-folder\logical-host-name\eg4nnmi_1st\oslog</code>	Primary data	OS log information
<code>data-storage-folder\logical-host-name\eg4nnmi_1st\eg4nnmi</code>		Information about JP1/IM - EG for NNMi
<code>data-storage-folder\logical-host-name\eg4nnmi_1st\base</code>		Information about JP1/Base
<code>data-storage-folder\logical-host-name\eg4nnmi_1st\ucpsb</code>		Information about Web server
<code>data-storage-folder\logical-host-name\eg4nnmi_2nd\oslog</code>	Secondary data	OS log information
<code>data-storage-folder\logical-host-name\eg4nnmi_2nd\base</code>		Information about JP1/Base

For details about the `jegn_log.bat` command, see *jegn_log.bat (Windows only)* in 7. *Commands*.

Cautions to be taken when using the data collection tool

- If you execute the data collection tool, the system information on the machine may not have been collected when execution of the data collection tool is completed. This is because the process that internally collects the OS information has not been completed, even though execution of the data collection tool has been completed. After ensuring that execution of `msinfo32.exe` has been completed from the **Processes** tab or the **Details** tab, by starting the Task Manager, perform operations such as compressing the collected data by using a compression tool, or moving or deleting the collected data.
- If there is a Windows event in the Windows event log in which the message format provided by the event log-issuing product and the number of padded characters do not match, an application error might occur during execution of the data collection tool. This is not a problem because the data is collected even in such cases.

When this problem occurs, a dialog box is displayed, and execution of the data collection tool might stop (the tool restarts when you respond to the dialog box). If you want to disable the display of the dialog box, execute the following procedure:

1. Click the **Start** menu and enter `gpedit.msc` in **Search for Program and File** or **Run**.
2. **Local group policy data editor** appears. Select **Local computer policy**, **Computer composition**, **Management template**, **Windows component**, and then **Windows error report** in the tree on the left-hand side.
3. In **Settings** on the right-hand side, select **Effective** in **Do not display the user interface in which a severe error occurred**, and click the **OK** button.

(1) OS log information

This subsection describes the OS log information that needs to be collected when an error has occurred. You can use the data collection tool (`jegn_log.bat` command) to collect the OS log information. The tables below list and describe the OS log information that can be collected by the data collection tool.

In the tables, the *File name* column shows the name of the file at the storage location after data has been collected by the data collection tool.

Table 10–8: OS log information (primary data for the physical host)

Type of information	Data that is collected	File name
Data collection date and time	<ul style="list-style-type: none"> • Execution result of <code>date /t</code> • Execution result of <code>time /t</code> 	<code>date.log</code>
Log files for Hitachi Integrated Installer	Files under <i>Windows-installation-folder</i> \Temp\HCDINST\	Copies of the files at the left
Host name settings set in the computer	<i>system-root-folder</i> \system32\drivers\etc\hosts	hosts
Service port settings set in the computer	<i>system-root-folder</i> \system32\drivers\etc\services	services
NIC installation status	Execution result of <code>ipconfig /all</code>	<code>ipconfig.log</code>
List of started services	Execution result of <code>net start</code>	<code>netstart.log</code>
Network statistical information	Execution result of <code>netstat -nao</code>	<code>netstat.log</code>
Environment variables for the computer	Execution result of <code>set</code>	<code>set.log</code>
System information for the computer	Execution result of <code>msinfo32 /report:filename</code>	<code>msinfo32.log</code>

Type of information	Data that is collected	File name
Registry information	Result of collection by the <code>reg</code> command of the contents of the HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI registry	hitachi_reg.txt
ON/OFF information for the media sense function	Result of collection by the <code>reg</code> command of the contents of the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisabledDHCPMediaSense registry	DisableDHCPMediaSense_reg.txt
JP1/Base access permission information (installation folder)	Execution result of <code>cacls Base-path</code>	cacls_jplbase.log
JP1/Base access permission information (log folder)	Execution result of <code>cacls Base-path\log</code>	cacls_jplbase_log.log
JP1/Base access permission information (command execution log folder)	Execution result of <code>cacls Base-path\log\COMMAND</code>	cacls_jplbase_log_COMMAND.log
JP1/Base access permission information (event database folder)	Execution result of <code>cacls Base-path\sys</code>	cacls_jplbase_sys.log
	Execution result of <code>cacls Base-path\sys\event</code>	cacls_jplbase_sys_event.log
	Execution result of <code>cacls Base-path\sys\event\servers</code>	cacls_jplbase_sys_event_servers.log
	Execution result of <code>cacls Base-path\sys\event\servers\default</code>	cacls_jplbase_sys_event_servers_default.log
JP1/IM - EG for NNMi access permission information (installation folder)	Execution result of <code>cacls EG-for-NNMi-path</code>	cacls_jpleg4nnmi.log
JP1/IM - EG for NNMi access permission information (log folder)	Execution result of <code>cacls EG-for-NNMi-path\log</code>	cacls_jpleg4nnmi_log.log
List of JP1/Base files	Execution result of <code>dir Base-path /s</code>	dir_jplbase.log
List of JP1/IM - EG for NNMi files	Execution result of <code>dir EG-for-NNMi-path /s</code>	dir_jpleg4nnmi.log
Host name for resolving the network address	Execution result of <code>jbsgethostbyname</code>	<ul style="list-style-type: none"> • jbsgethostbyname.log (standard output) • jbsgethostbyname_err.log (standard error)
Health check	Execution result of <code>jbshcstatus - debug -a</code>	<ul style="list-style-type: none"> • jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error)
Event service's process activity status	Execution result of <code>jevstat</code>	<ul style="list-style-type: none"> • jevstat.log (standard output) • jevstat_err.log (standard error)
Process activity status (JP1/Base)	Execution result of <code>jbs_spmd_status</code>	<ul style="list-style-type: none"> • jbs_spmd_status.log (standard output) • jbs_spmd_status_err.log (standard error)

Type of information	Data that is collected	File name
Process activity status (JP1/IM - EG for NNMi)	Execution result of <code>jegn_spm�_status</code>	<ul style="list-style-type: none"> <code>jegn_spm�_status.log</code> (standard output) <code>jegn_spm�_status_err.log</code> (standard error)
jp1hosts2 information registered on the host	Execution result of <code>jbshosts2export</code>	<ul style="list-style-type: none"> <code>jbshosts2export.log</code> (standard output) <code>jbshosts2export_err.log</code> (standard error)
Execution result of the data collection command	Execution result of the <code>jegn_log.bat</code> command	<code>jegn_log_result.log</code>
Library information for product information acquisition and logs	Files under <code><%SystemDrive%>\Program Files (x86)\Hitachi\jp1common\jp1imegn\</code>	Copies of the files at the left
JP1/Base access permission information (ALLUSERSPROFILE folder)	Execution result of <code>cacls <%ALLUSERSPROFILE%>\Hitachi\jp1\jp1_default\JP1Base\log</code>	<code>cacls_programdata_jplbase_log.log</code>
List of JP1/Base files (ALLUSERSPROFILE folder)	Execution result of <code>dir <%ALLUSERSPROFILE%>\Hitachi\jp1\jp1_default\JP1Base /s</code>	<code>dir_programdata_jplbase.log</code>

Table 10–9: OS log information (secondary data for the physical host)

Type of information	Data that is collected	File name
Data collection date and time	<ul style="list-style-type: none"> Execution result of <code>date /t</code> Execution result of <code>time /t</code> 	<code>date.log</code>
Windows event log	<ul style="list-style-type: none"> Application: <code>system-root-folder\system32\config\AppEvent.Evt</code> System: <code>system-root-folder\system32\config\SysEvent.Evt</code> 	<ul style="list-style-type: none"> <code>AppEvent (Backup) .evt</code> <code>AppEvent (Backup) .txt</code> <code>SysEvent (Backup) .evt</code> <code>SysEvent (Backup) .txt</code>
Crash dump [#]	<code>user-specified-folder\user.dmp</code>	<code>user.dmp</code>
Dr. Watson log [#]	<code>user-specified-folder\drwtsn32.log</code>	<code>drwtsn32.log</code>

#

Output of a crash dump must be set in advance. For details about how to specify the output settings, see [2.4.5\(1\) Preparations for collecting data in the event of an error \(Windows only\)](#).

Table 10–10: OS log information (primary data for the logical host)

Type of information	Data that is collected	File name
Data collection date and time	<ul style="list-style-type: none"> Execution result of <code>date /t</code> Execution result of <code>time /t</code> 	<code>date.log</code>
JP1/Base access permission information (shared folder)	Execution result of <code>cacls shared-folder\JP1Base</code>	<code>cacls_jplbase.log</code>
JP1/Base access permission information (log folder)	Execution result of <code>cacls shared-folder\JP1Base\log</code>	<code>cacls_jplbase_log.log</code>
JP1/Base access permission information (command execution log folder)	Execution result of <code>cacls shared-folder\JP1Base\log\COMMAND</code>	<code>cacls_jplbase_log_COMMAND.log</code>

Type of information	Data that is collected	File name
JP1/Base access permission information (event database folder)	Execution result of <code>cacls shared-folder\JP1Base\event</code>	<code>cacls_jp1base_event.log</code>
JP1/IM - EG for NNMI access permission information (shared folder)	Execution result of <code>cacls shared-folder\JP1EG4NNMI</code>	<code>cacls_jpleg4nnmi.log</code>
JP1/IM - EG for NNMI access permission information (log folder)	Execution result of <code>cacls shared-folder\JP1EG4NNMI\log</code>	<code>cacls_jpleg4nnmi_log.log</code>
List of JP1/Base files	Execution result of <code>dir shared-folder\JP1Base /s</code>	<code>dir_logical-host-name_jp1base.log</code>
List of JP1/IM - EG for NNMI files	Execution result of <code>dir shared-folder\JP1EG4NNMI /s</code>	<code>dir_logical-host-name_jpleg4nnmi.log</code>
Host name for resolving the network address	Execution result of <code>jbsgethostbyname logical-host-name</code>	<ul style="list-style-type: none"> <code>jbsgethostbyname.log</code> (standard output) <code>jbsgethostbyname_err.log</code> (standard error)
Event service's process activity status	Execution result of <code>jevstat logical-host-name</code>	<ul style="list-style-type: none"> <code>jevstat.log</code> (standard output) <code>jevstat_err.log</code> (standard error)
Health check	Execution result of <code>jbshcstatus -debug -a -h logical-host-name</code>	<ul style="list-style-type: none"> <code>jbshcstatus.log</code> (standard output) <code>jbshcstatus_err.log</code> (standard error)
Process activity status (JP1/Base)	Execution result of <code>jbs_spmd_status -h logical-host-name</code>	<ul style="list-style-type: none"> <code>jbs_spmd_status.log</code> (standard output) <code>jbs_spmd_status_err.log</code> (standard error)
Process activity status (JP1/IM - EG for NNMI)	Execution result of <code>jegn_spmd_status -h logical-host-name</code>	<ul style="list-style-type: none"> <code>jegn_spmd_status.log</code> (standard output) <code>jegn_spmd_status_err.log</code> (standard error)
jp1hosts2 information registered on the host	Execution result of <code>jbshosts2export -h logical-host-name</code>	<ul style="list-style-type: none"> <code>jbshosts2export.log</code> (standard output) <code>jbshosts2export_err.log</code> (standard error)
JP1/Base access permission information (ALLUSERSPROFILE folder)	Execution result of <code>cacls <%ALLUSERSPROFILE%>\Hitachi\jp1\logical-host-name\JP1Base\log</code>	<code>cacls_programdata_jp1base_log.log</code>
List of JP1/Base files (ALLUSERSPROFILE folder)	Execution result of <code>dir <%ALLUSERSPROFILE%>\Hitachi\jp1\logical-host-name\JP1Base /s</code>	<code>dir_programdata_jp1base.log</code>

Table 10–11: OS log information (secondary data for the logical host)

Type of information	Data that is collected	File name
Data collection date and time	<ul style="list-style-type: none"> Execution result of <code>date /t</code> Execution result of <code>time /t</code> 	<code>date.log</code>

(2) Integrated trace log

You can use the data collection tool (`jegn_log.bat` command) to collect the integrated trace log. The table below shows the integrated trace log that can be collected by the data collection tool.

In the table, the *File name* column shows the name of the file at the storage location after data has been collected by the data collection tool.

Table 10–12: Integrated trace log (primary data for the physical host)

Type of information	Data that is collected	File name
Integrated trace log	<i>system-drive</i> :ProgramFiles(x86)\Hitachi\HNTRLib2\spool	The following file by default: hntr2[1 2 3 4].log

(3) Information about JP1/IM - EG for NNMi

This subsection describes the information about JP1/IM - EG for NNMi that needs to be collected when an error has occurred. You can use the data collection tool (`jegn_log.bat` command) to collect the information about JP1/IM - EG for NNMi. The tables below list and describe the information about JP1/IM - EG for NNMi that can be collected by the data collection tool.

In the tables, the *File name* column shows the name of the file at the storage location after data has been collected by the data collection tool.

Table 10–13: Information about JP1/IM - EG for NNMi (primary data for the physical host)

Type of information	Data that is collected	File name	
Patch application history	<i>EG-for-NNMi-path</i> \PATCHLOG.TXT	Patchlog_jp1eg4nnmi.txt	
Model name and version information	<i>EG-for-NNMi-path</i> \Version.txt	Version.txt	
License type and expiration date	<i>EG-for-NNMi-path</i> \ProductInfo.txt	ProductInfo.txt	
Configuration and definition files	Files under <i>EG-for-NNMi-path</i> \conf\	Copies of the files at the left	
Log files	Operating log information for JP1/IM - EG for NNMi	Files under <i>EG-for-NNMi-path</i> \log\	Copies of the files at the left
	Communication log information for JP1/IM - EG for NNMi	Files under <i>EG-for-NNMi-path</i> \lib\uCPSB\CC\client\logs\	Copies of the files at the left
Forwarding filter definition files	Files under <i>EG-for-NNMi-path</i> \dat\	Copies of the files at the left	

Table 10–14: Information about JP1/IM - EG for NNMi (primary data for the logical host)

Type of information	Data that is collected	File name
Configuration and definition files	Files under <i>shared-folder</i> \JP1EG4NNMI\conf\	Copies of the files at the left
Log files	Files under <i>shared-folder</i> \JP1EG4NNMI\log\	Copies of the files at the left

Type of information	Data that is collected	File name
Forwarding filter definition files	Files under <i>shared-folder</i> \JP1EG4NNMI\dat\	Copies of the files at the left

(4) Information about JP1/Base

This subsection describes the information about JP1/Base that needs to be collected when an error has occurred.

Collect JP1/Base information using the JP1/Base data collection tool (*jbs_log.bat* command). For details about how to use the JP1/Base data collection tool, see the *JP1/Base User's Guide*.

You can use the data collection tool (*jegn_log.bat* command) to collect the information about JP1/Base.

The tables below list and describe the information about JP1/Base that can be collected by the data collection tool.

In the tables, the *File name* column shows the name of the file at the storage location after data has been collected by the data collection tool.

Table 10–15: Information about JP1/Base (primary data for the physical host)

Type of information	Data that is collected	File name
Patch information	<i>Base-path</i> \PatchLog.txt	Patchlog_jp1base.txt
Model name and version information	<i>Base-path</i> \Version.txt	Version.txt
License type and expiration date	<i>Base-path</i> \ProductInfo.txt	ProductInfo.txt
Configuration and definition files	Files under <i>Base-path</i> \conf\	Copies of the files at the left
Common definition information	Files under <i>Base-path</i> \default\	Copies of the files at the left
Log files	Files under <i>Base-path</i> \log\	All files under the folder at the left except COMMAND
Plug-in service configuration files	Files under <i>Base-path</i> \plugin\conf\	Copies of the files at the left
Log and temporary files	Files under <i>Base-path</i> \sys\tmp\event\	Copies of the files at the left
Log files (ALLUSERSPROFILE folder)	Files under <%ALLUSERSPROFILE%>\Hitachi\jp1\jp1_default\JP1Base\log\	Copies of the files at the left

Table 10–16: Information about JP1/Base (secondary data for the physical host)

Type of information	Data that is collected	File name
Command execution log files	Files under <i>Base-path</i> \log\COMMAND\	Copies of the files at the left
Event database	Files under <i>Base-path</i> \sys\event\servers\default\	Copies of the files at the left

Table 10–17: Information about JP1/Base (primary data for the logical host)

Type of information	Data that is collected	File name
Configuration and definition files	Files under <i>shared-folder</i> \JP1Base\conf\	Copies of the files at the left
Log files	Files under <i>shared-folder</i> \JP1Base\log\	All files under the folder at the left except COMMAND

Type of information	Data that is collected	File name
Event server settings	<i>shared-folder</i> \JP1Base\event	All files under the folder at the left except <i>IMEvent*. *</i>
Log files (ALLUSERSPROFILE folder)	Files under <%ALLUSERSPROFILE%>\Hitachi\jp1\ <i>logical-host-name</i> \JP1Base\log\	Copies of the files at the left

Table 10–18: Information about JP1/Base (secondary data for the logical host)

Type of information	Data that is collected	File name
Command execution log files	Files under <i>shared-folder</i> \JP1Base\log\COMMAND\	Copies of the files at the left
Event database	<i>shared-folder</i> \JP1Base\event	<i>IMEvent*. *</i>

(5) Information about the operation

You need the following information about the operation at the time the error occurred:

- Details of the operation (at the time of the error and before and after the error occurred)
- Time the error occurred
- Machine configuration (OS version, host name, JP1/IM - EG for NNMi system configuration)
- Repeatability

10.3.2 Data to be collected (in UNIX)

This subsection describes the data to be collected in UNIX when an error has occurred.

The data collection tool (*jegn_log.sh* command) classifies the target directories and files for data collection into primary data and secondary data categories, archives the data directly under the specified *data storage directory*, and then creates compressed files.

The following table lists the compressed files that are stored in the data storage folder.

Table 10–19: Compressed file containing collected data

Compressed file	Description
<i>data-storage-directory</i> /jp1_default_jpleg4nnmi_1st.tar.gz	Stores primary data for the physical host
<i>data-storage-directory</i> /jp1_default_jpleg4nnmi_2nd.tar.gz	Stores secondary data for the physical host
<i>data-storage-directory</i> / <i>logical-host-name</i> _jpleg4nnmi_1st.tar.gz	Stores primary data for the logical host
<i>data-storage-directory</i> / <i>logical-host-name</i> _jpleg4nnmi_2nd.tar.gz	Stores secondary data for the logical host

For details about the *jegn_log.sh* command, see *jegn_log.sh (UNIX only)* in 7. *Commands*.

(1) OS log information

This subsection describes the OS log information that needs to be collected when an error has occurred. You can use the data collection tool (`jegn_log.sh` command) to collect the OS log information. The tables below list and describe the OS log information that can be collected by the data collection tool.

Table 10–20: OS log information (primary data for the physical host)

Type of information	Data that is collected	Storage location [#]
Information about the installed Hitachi products	<code>/etc/.hitachi/pplistd/pplistd</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/pplistd</code>
Hitachi PP Installer installation log file	<code>/etc/.hitachi/.install.log*</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/.install.log*</code>
Uninstallation log file for Hitachi PP Installer	<code>/etc/.hitachi/.uninstall.log*</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/.uninstall.log*</code>
Common definition information	Files under <code>/opt/jpl/hcclibcnf/</code>	<code>./opt/jpl/hcclibcnf/</code> (contains copies of the files indicated at left)
JP1/Base installation log files	<code>/tmp/HITACHI_JP1_INST_LOG/jplbase_inst{1 2 3 4 5}.log</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/HITACHI_JP1_INST_LOG/jplbase_inst{1 2 3 4 5}.log</code>
JP1/IM - EG for NNMi installation log files	<code>/tmp/HITACHI_JP1_INST_LOG/jpleg_inst{1 2 3 4 5}.log</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/HITACHI_JP1_INST_LOG/jpleg_inst{1 2 3 4 5}.log</code>
JP1/IM - Manager installation log files	<code>/tmp/HITACHI_JP1_INST_LOG/jplimm_inst{1 2 3 4 5}.log</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/HITACHI_JP1_INST_LOG/jplimm_inst{1 2 3 4 5}.log</code>
List of files	<ul style="list-style-type: none"> • Execution result of <code>ls -lRa /opt/jpleg4nnmi</code> • Execution result of <code>ls -lRa /etc/opt/jpleg4nnmi</code> • Execution result of <code>ls -lRa /var/opt/jpleg4nnmi</code> • Execution result of <code>ls -lRa /opt/jplbase</code> • Execution result of <code>ls -lRa /etc/opt/jplbase</code> • Execution result of <code>ls -lRa /var/opt/jplbase</code> • Execution result of <code>ls -lRa /tmp/HITACHI_JP1_INST_LOG</code> • Execution result of <code>ls -lRa /etc/.hitachi</code> • Execution result of <code>ls -lRa /etc/.hlic</code> 	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/inst_dir_lRa.log</code>
	<ul style="list-style-type: none"> • Execution result of <code>ls -lRLa /opt/jpleg4nnmi</code> • Execution result of <code>ls -lRLa /etc/opt/jpleg4nnmi</code> 	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/inst_dir.log</code>

Type of information	Data that is collected	Storage location#
List of files	<ul style="list-style-type: none"> • Execution result of <code>ls -lRla /var/opt/jpleg4nnmi</code> • Execution result of <code>ls -lRla /opt/jplbase</code> • Execution result of <code>ls -lRla /etc/opt/jplbase</code> • Execution result of <code>ls -lRla /var/opt/jplbase</code> • Execution result of <code>ls -lRla /tmp/HITACHI_JP1_INST_LOG</code> • Execution result of <code>ls -lRla /etc/.hitachi</code> • Execution result of <code>ls -lRla /etc/.hlic</code> 	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/inst_dir.log
Data collection date and time	Execution result of date	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/date.log
Disk information	Execution result of <code>df -T -k</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/df.log
btrfs file system information	When btrfs is installed: Execution result of <code>btrfs filesystem show -all-device</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/btrfs.log
Process activity information from the automatic startup service (systemd)	When systemd is installed: <ul style="list-style-type: none"> • Execution result of <code>systemctl --all</code> • Execution result of <code>systemctl list-unit-files</code> • Execution result of <code>systemctl status jpl_base</code> • Execution result of <code>systemctl status jpl_eg4nnmi</code> 	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/systemctl.log
Environment variables for the computer	Execution result of <code>env</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/env.log
Host name settings set in the computer	<code>/etc/hosts</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/hosts
Shared memory status in process-to-process communication	Execution result of <code>ipcs -ma</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ipcs.log
Host name for resolving the network address	Execution result of <code>jbsgethostbyname</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ <ul style="list-style-type: none"> • <code>jbsgethostbyname.log</code> (standard output) • <code>jbsgethostbyname_err.log</code> (standard error)
Health check	Execution result of <code>jbshcstatus -debug -a</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ <ul style="list-style-type: none"> • <code>jbshcstatus.log</code> (standard output) • <code>jbshcstatus_err.log</code> (standard error)
Event service's process activity status	Execution result of <code>jevstat</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ <ul style="list-style-type: none"> • <code>jevstat.log</code> (standard output) • <code>jevstat_err.log</code> (standard error)

Type of information	Data that is collected	Storage location#
Process activity status (JP1/Base)	Execution result of <code>jbs_spmd_status</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ • <code>jbs_spmd_status.log</code> (standard output) • <code>jbs_spmd_status_err.log</code> (standard error)
Process activity status (JP1/IM - EG for NNMi)	Execution result of <code>jegn_spmd_status</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ • <code>jegn_spmd_status.log</code> (standard output) • <code>jegn_spmd_status_err.log</code> (standard error)
jp1hosts2 information registered on the host	Execution result of <code>jbshosts2export</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ • <code>jbshosts2export.log</code> (standard output) • <code>jbshosts2export_err.log</code> (standard error)
Execution result of the data collection command	Execution result of the <code>jegn_log.sh</code> command	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/jegn_log_result.log
Obtaining IP addresses	Execution result of <code>ifconfig -a</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ifconfig.log
	Execution result of <code>ip addr show</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ip_addr_show.log
NIC installation status	Execution result of <code>netstat -ia</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/netstat_ia.log
	Execution result of <code>ip -s link</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ip_s_link.log
Network statistical information	Execution result of <code>netstat -nap</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/netstat_na.log
	Execution result of <code>ss -nap</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ss_na.log
List of users set in the computer	<code>/etc/passwd</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/passwd
List of processes	Execution result of <code>ps -elfa</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ps.log
Service port settings set in the computer	<code>/etc/services</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/services
Memory information	<code>cat /proc/meminfo</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/swapinfo.log
System diagnostic information	Execution result of <code>dmesg</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/sys_info.log

Type of information	Data that is collected	Storage location [#]
syslog	/var/log/messages	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/syslog.log
OS version information	Execution result of <code>uname -a</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/uname_a.log
Kernel parameter information	<ul style="list-style-type: none"> • Execution result of <code>sysctl -a</code> • Execution result of <code>ulimit -a</code> 	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/ <ul style="list-style-type: none"> • <code>sysctl.log</code> • <code>ulimit.log</code>
Page size information	Execution result of <code>dmesg</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/pagesize.log
OS patch application status	Execution result of <code>rpm-qa</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/rpm.log
Process startup information used by init daemon	/etc/inittab	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/inittab
Disk mount information	/etc/fstab	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/fstab
Distribution information	In Linux 7, Linux 8, or Linux 9: Files under /etc/os-release Files under /etc/redhat-release In Oracle Linux 7, Oracle Linux 8, or Oracle Linux 9: Files under /etc/os-release In SUSE Linux 12: Files under /etc/os-release Files under /etc/SuSE-release In SUSE Linux 15: Files under /etc/os-release	./var/opt/jpleg4nnmi/log/_jpl_default/oslog (contains copies of the files indicated at left)
Product information log (JP1/IM - EG for NNMI)	Trace logs and error logs that are output at installation <ul style="list-style-type: none"> • <code>hliccmd{n}.log</code> • <code>hlicliberr{n}.log</code> • <code>hliclibmgrerr{n}.log</code> • <code>hliclibtrc{n}.log</code> • <code>hliclibmgrtrc{n}.log</code> 	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/hliclog (contains copies of the files indicated at left)

#

This is the storage location after a compressed file (`jpl_default_jpleg4nnmi_1st.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–21: OS log information (secondary data for the physical host)

Type of information	Data that is collected	Storage location [#]
Data collection date and time	Execution result of <code>date</code>	./var/opt/jpleg4nnmi/log/_jpl_default/oslog/date.log

#

This is the storage location after a compressed file (`jpl_default_jpleg4nnmi_2nd.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–22: OS log information (primary data for the logical host)

Type of information	Data that is collected	Storage location [#]
Data collection date and time	Execution result of date	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/date.log
Host name for resolving the network address	Execution result of jbsgethostbyname <i>logical-host-name</i>	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/ • jbsgethostbyname.log (standard output) • jbsgethostbyname_err.log (standard error)
Event service's process activity status	Execution result of jevstat <i>logical-host-name</i>	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/ • jevstat.log (standard output) • jevstat_err.log (standard error)
Health check	Execution result of jbshcstatus -debug -a -h <i>logical-host-name</i>	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/ • jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error)
Process activity status (JP1/Base)	Execution result of jbs_spmd_status - h <i>logical-host-name</i>	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/ • jbs_spmd_status.log (standard output) • jbs_spmd_status_err.log (standard error)
Process activity status (JP1/IM - EG for NNMi)	Execution result of jegn_spmd_status - h <i>logical-host-name</i>	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/ • jegn_spmd_status.log (standard output) • jegn_spmd_status_err.log (standard error)
jp1hosts2 information registered on the host	Execution result of jbshosts2export - h <i>logical-host-name</i>	./var/opt/jpleg4nnmi/log/ _logical-host-name/oslog/ • jbshosts2export.log (standard output) • jbshosts2export_err.log (standard error)
List of files	<ul style="list-style-type: none"> • Execution result of <code>ls -lRa <i>shared-directory</i>/jp1base</code> • Execution result of <code>ls -lRa <i>shared-directory</i>/jpleg4nnmi</code> • Execution result of <code>ls -lRa <i>shared-directory</i>/event</code> 	./var/opt/jpleg4nnmi/log/ _logical-host-name/ oslog/share_dir_lRa.log
	<ul style="list-style-type: none"> • Execution result of <code>ls -lRLa <i>shared-directory</i>/jp1base</code> • Execution result of <code>ls -lRLa <i>shared-directory</i>/jpleg4nnmi</code> • Execution result of <code>ls -lRLa <i>shared-directory</i>/event</code> 	./var/opt/jpleg4nnmi/log/ _logical-host-name/ oslog/share_dir.log

#

This is the storage location after a compressed file (*logical-host-name_jpleg4nnmi_1st.tar.gz*) that was created by the data collection tool has been decompressed.

Table 10–23: OS log information (secondary data for the logical host)

Type of information	Data that is collected	Storage location#
Data collection date and time	Execution result of date	<code>./var/opt/jpleg4nnmi/log/_logical-host-name/oslog/date.log</code>

#

This is the storage location after a compressed file (*logical-host-name_jpleg4nnmi_2nd.tar.gz*) that was created by the data collection tool has been decompressed.

(2) Integrated trace log

You can use the data collection tool (`jegn_log.sh` command) to collect the integrated trace log. The table below shows the integrated trace log that can be collected by the data collection tool.

Table 10–24: Integrated trace log (primary data for the physical host)

Type of information	Data that is collected	Storage location#
Integrated trace log	Files under <code>/var/opt/hitachi/HNTRLib2/spool/</code>	<code>./var/opt/hitachi/HNTRLib2/spool/</code> (contains copies of the files indicated at left)

#

This is the storage location after a compressed file (`jp1_default_jpleg4nnmi_1st.tar.gz`) that was created by the data collection tool has been decompressed.

(3) Information about JP1/IM - EG for NNMi

This subsection describes the information about JP1/IM - EG for NNMi that needs to be collected when an error has occurred. You can use the data collection tool (`jegn_log.sh` command) to collect the information about JP1/IM - EG for NNMi. The tables below list and describe the information about JP1/IM - EG for NNMi that can be collected by the data collection tool.

Table 10–25: Information about JP1/IM - EG for NNMi (primary data for the physical host)

Type of information	Data that is collected	Storage location#
Patch application history	<code>/opt/jpleg4nnmi/patch_history</code>	<code>./opt/jpleg4nnmi/patch_history</code>
Patch log information	<code>/opt/jpleg4nnmi/update.log</code>	<code>./opt/jpleg4nnmi/update.log</code>
Configuration and definition files	Files under <code>/etc/opt/jpleg4nnmi/conf</code>	<code>./etc/opt/jpleg4nnmi/conf/</code> (contains copies of the files indicated at left)
Log files	Operating log information for JP1/IM - EG for NNMi	Files under <code>/var/opt/jpleg4nnmi/log</code> (contains copies of the files indicated at left)
	Communication log information for JP1/IM - EG for NNMi	Files under <code>/opt/jpleg4nnmi/lib/uCPSB/CC/client/logs</code> (contains copies of the files indicated at left)

Type of information	Data that is collected	Storage location#
Core analysis information (result of analysis by seraph)	Analysis result of the core file under <code>/var/opt/jpleg4nnmi/log</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/oslog/core_module-name.log</code>
Forwarding filter definition files	Files under <code>/var/opt/jpleg4nnmi/dat</code>	<code>./var/opt/jpleg4nnmi/dat/</code> (contains copies of the files indicated at left)
Automated startup and stop scripts	Files under <code>/etc/opt/jpleg4nnmi</code>	<code>./etc/opt/jpleg4nnmi/</code> (contains copies of the files indicated at left)

#

This is the storage location after a compressed file (`jpl_default_jpleg4nnmi_1st.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–26: Information about JP1/IM - EG for NNMi (secondary data for the physical host)

Type of information	Data that is collected	Storage location#
Core analysis information (result of the car command)	car file of the core file under <code>/var/opt/jpleg4nnmi/log</code>	<code>./var/opt/jpleg4nnmi/log/_jpl_default/core/core_module-name_car.tar.gz</code>

#

This is the storage location after a compressed file (`jpl_default_jpleg4nnmi_2nd.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–27: Information about JP1/IM - EG for NNMi (primary data for the logical host)

Type of information	Data that is collected	Storage location#
Configuration and definition files	Files under <code>shared-directory/jpleg4nnmi/conf</code>	<code>shared-directory/jpleg4nnmi/conf/</code> (contains copies of the files indicated at left)
Log files	Files under <code>shared-directory/jpleg4nnmi/log</code>	<code>shared-directory/jpleg4nnmi/log/</code> (contains copies of the files indicated at left)
Core analysis information (result of analysis by seraph)	Analysis result of the core file under <code>shared-directory/jpleg4nnmi/log</code>	<code>./var/opt/jpleg4nnmi/log/_shared-directory/oslog/core_module-name.log</code>
Forwarding filter definition files	Files under <code>shared-directory/jpleg4nnmi/dat</code>	<code>shared-directory/jpleg4nnmi/dat/</code> (contains copies of the files indicated at left)

#

This is the storage location after a compressed file (`logical-host-name_jpleg4nnmi_1st.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–28: Information about JP1/IM - EG for NNMi (secondary data for the logical host)

Type of information	Data that is collected	Storage location#
Core analysis information (result of the car command)	car file of the core file under <code>shared-directory/jpleg4nnmi/log</code>	<code>./var/opt/jpleg4nnmi/log/_shared-directory/core/core_module-name_car.tar.gz</code>

#

This is the storage location after a compressed file (`logical-host-name_jpleg4nnmi_2nd.tar.gz`) that was created by the data collection tool has been decompressed.

(4) Information about JP1/Base

This subsection describes the information about JP1/Base that needs to be collected when an error has occurred. You can use the data collection tool (`jegn_log.sh` command) to collect the information about JP1/Base. If you do not collect this information, execute the `jegn_log.sh` command with the `-n`, `-p`, or `-r` option specified.

The tables below list and describe the information about JP1/Base that can be collected by the data collection tool.

Table 10–29: Information about JP1/Base (primary data for the physical host)

Type of information	Data that is collected	Storage location [#]
Automated startup and stop scripts	Files under <code>/etc/opt/jplbase/</code>	<code>./etc/opt/jplbase/</code> (contains copies of the files indicated at left)
Configuration and definition files	Files under <code>/etc/opt/jplbase/conf/</code>	<code>./etc/opt/jplbase/conf/</code> (contains copies of the files indicated at left)
Common definition information	Files under <code>/etc/opt/jplbase/default/</code>	<code>./etc/opt/jplbase/default/</code> (contains copies of the files indicated at left)
Plug-in service configuration files	Files under <code>/opt/jplbase/plugin/conf/</code>	<code>./opt/jplbase/plugin/conf/</code> (contains copies of the files indicated at left)
Patch application history	<code>/opt/jplbase/PatchInfo</code>	<code>./opt/jplbase/PatchInfo</code>
Patch log information	<code>/opt/jplbase/PatchLog</code>	<code>./opt/jplbase/PatchLog</code>
Log files	<code>/var/opt/jplbase/log</code>	<code>./var/opt/jplbase/log/</code> (contains copies of the files indicated at left except the <code>COMMAND</code> and core files)
Log and temporary files	Files under <code>/var/opt/jplbase/sys/tmp/</code>	<code>./var/opt/jplbase/sys/tmp/</code> (contains copies of the files indicated at left)

#

This is the storage location after a compressed file (`jpl_default_jpleg4nnmi_1st.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–30: Information about JP1/Base (secondary data for the physical host)

Type of information	Data that is collected	Storage location [#]
SES configuration files	<ul style="list-style-type: none"> • <code>/tmp/.JP1_SES*</code> • <code>/usr/tmp/jpl_ses</code> • <code>/usr/lib/jpl_ses/log</code> • <code>/usr/lib/jpl_ses/sys</code> • <code>/usr/bin/jpl_ses/jp*</code> • <code>/var/opt/jpl_ses</code> 	<ul style="list-style-type: none"> • <code>./tmp/.JP1_SES*</code> • <code>./usr/tmp/jpl_ses</code> • <code>./usr/lib/jpl_ses/log</code> • <code>./usr/lib/jpl_ses/sys</code> • <code>./usr/bin/jpl_ses/jp*</code> • <code>./var/opt/jpl_ses</code>
Command execution log files	Files under <code>/var/opt/jplbase/log/COMMAND/</code>	<code>./var/opt/jplbase/log/COMMAND/</code> (contains copies of the files indicated at left)
Event database	Files under <code>/var/opt/jplbase/sys/event/servers/default/</code>	<code>./var/opt/jplbase/sys/event/servers/default/</code> (contains copies of the files indicated at left)

#

This is the storage location after a compressed file (`jpl_default_jpleg4nnmi_2nd.tar.gz`) that was created by the data collection tool has been decompressed.

Table 10–31: Information about JP1/Base (primary data for the logical host)

Type of information	Data that is collected	Storage location [#]
Configuration and definition files	Files under <i>shared-directory</i> / jplbase/conf/	<i>.shared-directory</i> /jplbase/conf/ (contains copies of the files indicated at left)
Log files	<i>shared-directory</i> /jplbase/log	<i>.shared-directory</i> /jplbase/log/ (contains copies of the files indicated at left except the COMMAND and core files)
Event server settings	<i>shared-directory</i> /event	All files under the <i>.shared-directory</i> / event/ (contains copies of the files indicated at left except IMEvent*)

#

This is the storage location after a compressed file (*logical-host-name*_jplieg4nnmi_1st.tar.gz) that was created by the data collection tool has been decompressed.

Table 10–32: Information about JP1/Base (secondary data for the logical host)

Type of information	Data that is collected	Storage location [#]
Command execution log files	Files under <i>shared-directory</i> / jplbase/log/COMMAND/	<i>.shared-directory</i> /jplbase/log/ COMMAND/ (contains copies of the files indicated at left)
Event database	<i>shared-directory</i> /event	<i>.shared-directory</i> / event/IMEvent*.*

#

This is the storage location after a compressed file (*logical-host-name*_jplieg4nnmi_2nd.tar.gz) that was created by the data collection tool has been decompressed.

(5) Information about the operation

You need the following information about the operation at the time the error occurred:

- Details of the operation (at the time of the error and before and after the error occurred)
- Time the error occurred
- Machine configuration (OS version, host name, JP1/IM - EG for NNMi system configuration)
- Repeatability

Appendixes

A. Lists of Files and Directories

This appendix describes the files and directories that are used in JP1/IM - EG for NNMI.

A.1 Files and folders (in Windows)

The following table lists the folders that are used in JP1/IM - EG for NNMI (Windows version).

Table A–1: List of folders for JP1/IM - EG for NNMI (Windows version)

Folder name	Description	
<i>EG-for-NNMi-path</i>	\bin	Command storage folder
	\lib	Library storage folder
	\conf ^{#1}	Definition file storage folder
	\log ^{#1}	Log storage folder
	\dat ^{#1}	dat file storage folder
	\tmp	Temporary file storage folder
	\tools	Tool storage folder
<i>system-drive</i> : \Program Files (x86) \Hitachi \jplcommon \#2	Product information storage folder	

#1
In the case of a logical host, the *conf*, *log*, and *dat* folders are stored under *shared-folder* \JP1EG4NNMI.

#2
The location represented by *system-drive*: \Program Files is determined at the time of installation by an OS environment variable, and might differ depending on the environment.

Of the files stored in the folders listed above, those that can be referenced and edited by the user are listed in the following table.

Table A–2: List of files that can be referenced and edited by the user (Windows version)

Folder name	File name	Description	Ref	Edit
\conf	imevtgw_nnmi_cia_map.conf	Custom attribute mapping definition file ^{#2}	Y	Y
	imevtgw_nnmi_forward_filter.conf	NNMI incident forwarding filter definition file	Y	Y
	imevtgw_nnmi_forward_filter.conf.sample	Sample file of the NNMI incident forwarding filter definition file	Y	Y ^{#1}
	imevtgw_nnmi_label_mapping_category_en.conf	Mapping definition file (for category)	Y	Y
	imevtgw_nnmi_label_mapping_category_en.conf.sample	Sample file of the mapping definition file (for category)	Y	Y ^{#1}
	imevtgw_nnmi_label_mapping_family_en.conf	Mapping definition file (for family)	Y	Y
	imevtgw_nnmi_label_mapping_family_en.conf.sample	Sample file of the mapping definition file (for family)	Y	Y ^{#1}

Folder name	File name	Description	Ref	Edit
\conf	jegn_service_0700.conf	Extended startup process definition file	Y	P
	jegn_service_0700.conf.model	Model file for the extended startup process definition file	Y	p#1
	jegn_param_v7.conf	JP1/IM - EG for NNMi parameter definition file	Y	N
	jegn_param_v7.conf.model	Model file for the JP1/IM - EG for NNMi parameter definition file	Y	N
	jegn_env.conf	Environment variables file	Y	N
	jegn_env.conf.model	Model file for the environment variables file	Y	N
\log	jegnevent{1 2 3 4}.log	Trace log for issued JP1 events	Y	N
\tools	jegn_log.bat	Data collection tool	Y	N

Legend:

Ref: Referencing

Edit: Editing

Y: Supported

P: Partially editable

N: Not supported

#1

Use a copy of the file.

#2

If custom attribute mapping is not set, this file does not exist.

A.2 Files and directories (in UNIX)

The following table lists the directories that are used in JP1/IM - EG for NNMi (UNIX version).

Table A–3: List of directories for JP1/IM - EG for NNMi (UNIX version)

Directory name	Description
/opt/jpleg4nnmi/bin	Command storage directory
/opt/jpleg4nnmi/lib	Library storage directory
/opt/jpleg4nnmi/tools	Tool storage directory
/etc/opt/jpleg4nnmi	Script file storage directory
/etc/opt/jpleg4nnmi/conf#	Definition file storage directory
/var/opt/jpleg4nnmi/log#	Log storage directory
/var/opt/jpleg4nnmi/dat#	dat file storage directory
/var/opt/jpleg4nnmi/tmp	Temporary file storage directory

#

In the case of a logical host, the conf, log, and dat folders are stored under *shared-directory/jpleg4nnmi*.

Of the files stored in the directories listed above, those that can be referenced and edited by the user are listed in the following table.

Table A–4: List of files that can be referenced and edited by the user (UNIX version)

Directory name	File name	Description	Referencing	Editing
/etc/opt/ jpleg4nnmi	jegn_start	Script for automatically starting JP1/IM - EG for NNMi	Y	P#3
	jegn_start.model	Model file for the script for automatically starting JP1/IM - EG for NNMi	Y	N#1
	jegn_stop	Script for automatically terminating JP1/IM - EG for NNMi	Y	P#3
	jegn_stop.model	Model file for the script for automatically terminating JP1/IM - EG for NNMi	Y	N#1
	jegn_start.cluster	Script for starting JP1/IM - EG for NNMi on the physical host	Y	N
	jegn_stop.cluster	Script for terminating JP1/IM - EG for NNMi on the physical host	Y	N
	jegn_killall.cluster	Script for forcibly terminating processes of JP1/IM - EG for NNMi when operating in a cluster system	Y	N
/etc/opt/ jpleg4nnmi/conf	imevtgw_nnmi_cia_map.conf	Custom attribute mapping definition file#2	Y	Y
	imevtgw_nnmi_forward_filter.conf	NNMi incident forwarding filter definition file	Y	Y
	imevtgw_nnmi_forward_filter.conf.sample	Sample file of the NNMi incident forwarding filter definition file	Y	Y#1
	imevtgw_nnmi_label_mapping_category_en.conf	Mapping definition file (for category)	Y	Y
	imevtgw_nnmi_label_mapping_category_en.conf.sample	Sample file of the mapping definition file (for category)	Y	Y#1
	imevtgw_nnmi_label_mapping_family_en.conf	Mapping definition file (for family)	Y	Y
	imevtgw_nnmi_label_mapping_family_en.conf.sample	Sample file of the mapping definition file (for family)	Y	Y#1
	jegn_service_0700.conf	Extended startup process definition file	Y	P
	jegn_service_0700.conf.model	Model file for the extended startup process definition file	Y	P#1
	jegn_param_v7.conf	JP1/IM - EG for NNMi parameter definition file	Y	Y
	jegn_param_v7.conf.model	Model file for the JP1/IM - EG for NNMi parameter definition file	Y	Y#1

Directory name	File name	Description	Referencing	Editing
/etc/opt/ jpleg4nnmi/conf	jegn_env.conf	Environment variables file	Y	P
	jegn_env.conf.model	Model file for the environment variables file	Y	p#1
/var/opt/ jpleg4nnmi/log	jegnevent{1 2 3 4}.log	Trace log for issued JP1 events	Y	N
/opt/ jpleg4nnmi/tools	jegn_log.sh	Data collection tool	Y	N

Legend:

Y: Supported

P: Partially editable

N: Not supported

#1

Use a copy of the file.

#2

If custom attribute mapping is not set, this file does not exist.

#3

Only the lines containing the LANG environment variable can be changed.

B. Lists of Processes

This appendix describes the processes of JP1/IM - EG for NNMi.

B.1 List of processes (in Windows)

The table below lists the names of the processes that are displayed on the **Processes** page in Windows Task Manager. In the table, the parentheses enclose the number of instances of the process that can execute concurrently.

Table B–1: Processes of JP1/IM - EG for NNMi (Windows)

Name of parent process	Function	Name of child process	Function
jegn_spmd.exe (1)	Process management of JP1/IM - EG for NNMi	jegneg4nnmi.exe (1)	Main service of JP1/IM - EG for NNMi (Process management display name: jegneg4nnmi)
jegn_service.exe (1)	Windows service control of JP1/IM - EG for NNMi	--	--

Legend:

--: None

If you are operating in a cluster system, the above processes are executed for each of the physical and logical hosts.

B.2 List of processes (in UNIX)

The table below lists the names of the processes that are displayed when the `ps` command is used. In the table, the parentheses enclose the number of instances of the process that can execute concurrently.

Table B–2: Processes of JP1/IM - EG for NNMi (UNIX)

Name of parent process	Function	Name of child process	Function
jegn_spmd (1)#	Process management of JP1/IM - EG for NNMi	jegneg4nnmi (1)	Main service of JP1/IM - EG for NNMi (Process management display name: jegneg4nnmi)

#

The number of concurrent executions of the process may be increased temporarily.

If you are operating in a cluster system, the above processes are executed for each of the physical and logical hosts.

C. List of Limit Values

The following table lists the limit values for JP1/IM - EG for NNMi.

Table C–1: List of limit values

Item	Limit value
Maximum size of the NNMi incident forwarding filter definition file	10 MB
Maximum number of forwarding condition blocks that can be specified in the NNMi incident forwarding filter definition file	100
Maximum size of the mapping definition file (for category)	10 MB
Maximum size of the mapping definition file (for family)	10 MB

D. Performance and Estimation

For details about the memory requirements and the required disk capacity for JP1/IM - EG for NNMi, see the Release Notes.

E. Regular Expressions

The REGEX operator enables you to use regular expressions in filtering conditional statements in the NNMi incident forwarding filter definition file. This appendix describes the regular expressions that can be used in the filtering conditional statements.

E.1 Syntax for regular expressions

JP1/IM - EG for NNMi supports the use of regular expressions. The conventions described below must be observed when you use regular expressions.

Note:

If you use regular expressions, we recommend that you use only the ones presented here, because specification of other regular expressions depends on the computer and OS.

(1) Normal characters

Normal characters are those that are evaluated for an exact match when they are specified in a search string. The only characters that are not treated as normal characters are the control codes and special characters.

(2) Special characters

The following are the special characters: ^ \$. * + ? | () { } [] \. The following table explains the special characters.

Table E–1: Special characters in regular expressions

Special character	Description
^	Indicates a beginning specification match (leading-characters match). This is a special character only when it is used at the beginning of a regular expression to denote beginning characters. When this character is used at any other location, it is treated as a normal character.
\$	Indicates an ending specification match (trailing-characters match). This is a special character only when it is used at the end of a regular expression to denote ending characters. When this character is used at any other location, it is treated as a normal character.
.	Indicates any one character.
*	Indicates that the immediately preceding character can be included any number of times or no times.
+	Indicates that the immediately preceding character is included at least once.
?	Indicates that the immediately preceding character is included one time or not at all.
	Indicates the OR condition between the regular expressions specified before and after the vertical bar. This character is used together with the special characters (and) .
()	Indicates grouping of the enclosed regular expressions. These characters are used mainly in conjunction with the character.
{ }	Indicates that the immediately preceding character is to be included as many times as the value specified within the curly brackets.
[]	Indicates that the value includes any of the characters enclosed in the square brackets. If the first character enclosed in the square brackets is the ^, the value includes any character other than the characters enclosed in the square brackets.

Special character	Description
\	Escape character. When \ is specified immediately before a special character, that special character does not perform its function as a special character and instead is treated as a normal character. Note that \n is handled as the linefeed character and \t is handled as the tab character.

E.2 How to specify regular expressions

The following table describes how to specify regular expressions.

Table E–2: How to specify regular expressions

Specification method	Description
<i>character-string</i>	Match a line that contains the specified character string.
<i>^character-string</i>	Match a line that begins with the specified character string.
<i>character-string\$</i>	Match a line that ends with the specified character string.
<i>^character-string\$</i>	Combines ^ and \$ to match a line that consists only of the specified character string.
<i>^\$</i>	Combines ^ and \$ to match a null line.
<i>.</i> (period)	Match any one character.
<i>character*</i>	Match a character string in which the character immediately preceding * is included any number of times or no times.
<i>.*</i>	Combines . (period) and * to match any character string.
<i>character+</i>	Match a character string in which the character immediately preceding + is included at least once.
<i>character?</i>	Match a character string in which the character immediately preceding ? is included once or not at all.
<i>regular-expression regular-expression</i>	Match either of the regular expressions separated by the character.
<i>(regular-expressions)</i>	Groups regular expressions. This method is used mainly in conjunction with the character.
<i>character{n}</i>	Match a character string in which the character immediately preceding {n} is included n times.
<i>character{n, }</i>	Match a character string in which the character immediately preceding {n, } is included at least n times.
<i>character{n, m}</i>	Match a character string in which the character immediately preceding {n, m} is included at least n times but no more than m times.
<i>[character-string]</i>	Match any of the characters in the character string specified in [].
<i>[^character-string]</i>	Match any character that is not one of the characters in the character string specified in [].
<i>[character–character]</i>	Match any character that is within the specified range of character codes (when sorted in ascending order).
<i>[^character–character]</i>	Match any character that is not within the specified range of character codes (when sorted in ascending order).
<i>\special-character</i>	Handle the specified special character as a normal character.

E.3 Hints on using regular expressions

- The control codes (such as linefeed and tab) might be handled differently depending on the product and OS. If you use regular expressions to specify conditions for messages, specify the part that does not include control codes.
- If you make frequent use of the regular expression `. *` for matching all characters, the search processing might take a long time. If you use `. *` for long messages, use it only at the necessary locations.
- The `|` special character represents the OR condition. Note the following about using this OR condition in regular expressions:

The `|` special character for the OR condition has a low priority in a regular expression, which means that you must specify explicitly the range of the OR condition. If you do not specify the range, the OR condition might not work or might malfunction. Specify the range of an OR condition by enclosing the range in parentheses `()`.

The following example selects those NNMI incidents whose source node includes `gyoumu` or `host`:

```
SRC_NODE_NAME REGEX ^.* (gyoumu|host) .*$
```

- Any space that is specified before or after the `|` special character is treated as a character. If you do not intend to include spaces, do not specify them in conjunction with the `|` special character.

E.4 Examples of regular expressions

The following table shows examples of regular expressions.

Table E-3: Examples of regular expressions

Specification method	Function	Character string specified as the regular expression	Pattern that matches or does not match the regular expression	Result
<i>character-string</i>	Matches a line that contains the specified character string.	spring	spring has come.	Y
			winter-summer-autumn- spring	Y
			----- spring -----	Y
<i>^character-string</i>	Matches a line that begins with the specified character string.	^spring	spring has come.	Y
			winter-summer-autumn-spring	N
			-----spring-----	N
<i>character-string\$</i>	Matches a line that ends with the specified character string.	spring\$	spring has come.	N
			winter-summer-autumn- spring	Y
			-----spring-----	N
<i>^character-string\$</i>	Matches a line that contains only the specified character string.	^spring\$	spring has come.	N
			winter-summer-autumn-spring	N
			spring	Y
			spring	N
<i>^\$</i>	Matches a null line.	^\$		Y
			spring	N
<i>. (period)</i>	Matches any one character.	in.e	winter has come.	Y
			mother of in vention	Y

Specification method	Function	Character string specified as the regular expression	Pattern that matches or does not match the regular expression	Result
. (period)	Matches any one character.	in.e	life is in everything	Y
			eight nine ten	N
			increasing population	N
		s..ing	picnic in spring	Y
			skiing in winter	Y
<i>character*</i>	Matches a character string in which the character immediately preceding * is included any number of times or no times.	ro*m	terminal	Y
			cd- rom	Y
			living room	Y
		h.*n	This is a pen.	Y
			That is an apple.	Y
<i>regular-expression regular-expression</i>	Matches either the left-hand regular expression or the right-hand regular expression.	[0-9]+ apple	That is an apple .	Y
			spring in 2009	Y
<i>(regular-expressions)</i>	Groups regular expressions. This method is used mainly when the is used.	i(n.e ng)	winter has come.	Y
			interesting book	Y
[<i>character-string</i>]	Matches any of the characters in the character string specified in [].	[pr]	spring has come.	Y
			today is monday.	N
[<i>character-character</i>]	Matches any of the characters within the specified range of character codes (when sorted in ascending order).	[a-i]	spring has come.	Y
[<i>^character-character</i>]	Matches any characters not within the specified range of character codes (when sorted in ascending order).	[^a-i]	spring has come.	Y
\ <i>special-character</i>	Treats the specified special character as a normal character.	o\.h	<stdio. h >	Y
			another man	N

Legend:

Bold type: Character that provides the match with the specified regular expression

Y: There is a match

N: There is no match

F. Definition Files

The following table lists and describes the definition files for JP1/IM - EG for NNMi.

Table F–1: List of definition files

Definition file name	Description
Custom attribute mapping definition file (<code>imevtgw_nnmi_cia_map.conf</code>)	<p>Defines which sequence custom attributes are mapped in when JP1/IM-EG for NNMi handles the custom attributes of NNMi incidents.</p> <p>There is no custom attribute mapping definition file at the time of installation. If necessary, create a new custom attribute mapping definition file.</p> <p>For details, see 4.3 Creating a custom attribute mapping definition file.</p>
NNMi incident forwarding filter definition file (<code>imevtgw_nnmi_forward_filter.conf</code>)	<p>Defines conditions for converting NNMi incidents acquired from NNMi into JP1 events.</p> <p>There is no NNMi incident forwarding filter definition file at the time of installation. If necessary, copy the sample file, rename it, and then edit the sample definitions in the file.</p> <p>For details, see 4.1 Creating an NNMi incident forwarding filter definition file.</p>
Mapping definition file (for category) (<code>imevtgw_nnmi_label_mapping_category.conf</code>)	<p>Defines the label names for Category, which is an attribute of NNMi incidents.</p> <p>There is no NNMi incident forwarding filter definition file at the time of installation. If necessary, copy the sample file, rename it, and then edit the sample definitions in the file.</p> <p>For details, see 4.2 Creating a mapping definition file.</p>
Mapping definition file (for family) (<code>imevtgw_nnmi_label_mapping_family.conf</code>)	<p>Defines the label names for Family, which is an attribute of NNMi incidents.</p> <p>There is no NNMi incident forwarding filter definition file at the time of installation. If necessary, copy the sample file, rename it, and then edit the sample definitions in the file.</p> <p>For details, see 4.2 Creating a mapping definition file.</p>
Extended startup process definition file (<code>jegn_service_0700.conf</code>)	<p>Defines information about the processes of the functions that constitute JP1/IM - EG for NNMi.</p> <p>JP1/IM - EG for NNMi provides a model extended startup process definition file in which the required definitions have already been set. To make a change in these settings, copy the model file and edit only the <i>whether-restartable</i> parameter as appropriate for your operation.</p> <p>For details, see F.1 Extended startup process definition file (<code>jegn_service_0700.conf</code>).</p>
JP1/IM - EG for NNMi parameter definition file (<code>jegn_param_V7.conf</code>)	<p>Defines whether JP1 events are to be issued when processes of JP1/IM - EG for NNMi result in an error and during automatic recovery from abnormal termination.</p> <p>JP1/IM - EG for NNMi provides a model JP1/IM - EG for NNMi parameter definition file in which the required definitions have already been set. To make changes in these settings, copy the model file and then edit the copy.</p> <p>For details, see F.2 JP1/IM - EG for NNMi parameter definition file (<code>jegn_param_V7.conf</code>).</p>
Environment variables file (<code>jegn_env.conf</code>)	A file that sets environment variables of product JP1/IM - EG for NNMi.

Storage location:

In Windows:

- Physical host: `EG-for-NNMi-path\conf`
- Logical host: `shared-folder\JP1EG4NNMI\conf`

In UNIX:

- Physical host: `/etc/opt/jpleg4nnmi/conf`
- Logical host: `shared-directory/jpleg4nnmi/conf`

F.1 Extended startup process definition file (`jegn_service_0700.conf`)

Format

```
process-name|path|start-options|whether-restartable|restart-count|retry-interval|restart-count-reset-time
```

Files

`jegn_service_0700.conf` (extended startup process definition file)

`jegn_service_0700.conf.model` (model file for the extended startup process definition file)

Description

The extended startup process definition file defines information about the processes of the functions that constitute JP1/IM - EG for NNMi.

JP1/IM - EG for NNMi uses the process management function to control restart in the event of abnormal termination of a process. The process management function controls the processes according to definitions in the extended startup process definition file.

JP1/IM - EG for NNMi provides a model extended startup process definition file in which the required definitions have already been set. To make a change in these settings, copy the model file and edit only the *whether-restartable* parameter as appropriate for your operation. Normally, there is no need to change any of the other parameter settings because appropriate values have already been set as the defaults for each process.

Do not specify any unneeded characters, such as spaces. Edit only the value of the *whether-restartable* parameter.

In the case of a cluster configuration, if the extended startup process definition file is not found in the `conf` folder at the logical host when a process of process management is started at the logical host, the extended startup process definition file at the physical host is copied.

When the definitions are applied

The settings in this definition file take effect when JP1/IM - EG for NNMi starts or when the `jegn_spm�_reload` command is executed to reload the definitions. For details about the `jegn_spm�_reload` command, see [jegn_spm�_reload](#) in 7. *Commands*.

Information to be specified

process-name

Specifies the name of a process that is to be started and terminated by the process management function of JP1/IM - EG for NNMi.

Do not edit this parameter because the process names of JP1/IM - EG for NNMi have already been specified.

The process names are displayed by the `jegn_spm�_status` command.

path

Specifies the absolute path of the process's executable file.

Do not edit this parameter because the paths of the JP1/IM - EG for NNMi processes have already been specified.

start-options

Specifies start options for the process.

Do not edit this parameter because the start options have already been specified for the applicable processes.

whether-restartable

Specifies whether the process is to be restarted if it terminates abnormally.

To restart the process, specify 0; to not restart the process, specify 1.

The default is 0.

restart-count

Specifies the retry count for process restarts.

The permitted value is from 0 to 99. The default is 3.

If 0 is specified in the *whether-restartable* field, this parameter is ignored even when a value is specified.

retry-interval

Specifies the retry interval in seconds for process restarts.

The permitted value is from 0 to 3600. The default is 3.

If 0 is specified in the *whether-restartable* field, this parameter is ignored even when a value is specified.

restart-count-reset-time

Specifies the amount of time in seconds that must elapse after a restart of the process before the restart count is reset.

The permitted value is from 3600 to 2147483647. The default is 21600.

When the specified time elapses since the process restarted, the restart count is reset. If the process terminates abnormally again thereafter, the restart count begins again with 1. If the process is started by a restart but terminates abnormally again before the specified time has elapsed, the previous restart count is inherited.

If 0 is specified in the *whether-restartable* field, this parameter is ignored even when a value is specified.

Notes

In case of operation using a cluster system

Do not restart JP1 by JP1 process management. Restart JP1 by the cluster software.

F.2 JP1/IM - EG for NNMi parameter definition file (jegn_param_V7.conf)

Format

```
[logical-host-name\JP1EG4NNMi]
"SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT"=dword:value
"SEND_PROCESS_RESTART_EVENT"=dword:value
```

Files

jegn_param_V7.conf (JP1/IM - EG for NNMi parameter definition file)

jegn_param_V7.conf.model (model file for the JP1/IM - EG for NNMi parameter definition file)

Description

The JP1/IM - EG for NNMi parameter definition file defines whether JP1 events are to be issued in the event of an error in a JP1/IM - EG for NNMi process and during automatic recovery from abnormal termination. By issuing JP1 events in the event of a process error and during automatic recovery from abnormal termination, you can manage the error logs of problems that occurred in JP1/IM - EG for NNMi. We recommend that you use this definition file to specify that JP1 events are to be issued.

JP1/IM - EG for NNMi provides a model JP1/IM - EG for NNMi parameter definition file in which the required definitions have already been set. To make changes in these settings, copy the model file and then edit the copy.

The following shows the processes of JP1/IM - EG for NNMi and the JP1 events that can be issued.

Processes of JP1/IM - EG for NNMi

- Process management of JP1/IM - EG for NNMi (jegn_spm))
- Main service of JP1/IM - EG for NNMi (jegneg4nnmi)

JP1 events that can be issued

Event ID	Issuance timing
0x000061F0	When a process terminates abnormally
0x000061F1	When startup of a process results in a timeout
0x000061F2	When a process that terminated abnormally has restarted

For details about the JP1 events, see [8.4.2 Details of JP1 events](#).

When the definitions are applied

The settings in this definition file take effect after JP1/IM - EG for NNMi is restarted by executing the `jbssetcnf` command of JP1/Base with this definition file specified in an argument. For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

Information to be specified

[*logical-host-name*\JP1EG4NNMI]

This is a key name of the environment settings for JP1/IM - EG for NNMi.

Set in *logical-host-name* either JP1_DEFAULT for the physical host or the logical host name for the logical host.

"SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT"=dword:*value*

Specify 1 in *value* in order for JP1 events to be issued at the following times:

- When a process terminates abnormally
The JP1 event whose event ID is 0x000061F0 is issued.
- When no start notification is sent during startup and a timeout occurs
The JP1 event whose event ID is 0x000061F1 is issued.

The default is 0, in which case these JP1 events are not issued.

"SEND_PROCESS_RESTART_EVENT"=dword:*value*

Specify 1 in *value* in order for a JP1 event to be issued at the following time:

- When a process that terminated abnormally is restarted by the process restart function
The JP1 event whose event ID is 0x000061F2 is issued.

The default is 0, in which case this JP1 event is not issued.

G. Version Changes

This appendix describes the changes between versions.

G.1 Changes in version 13-00

- The following OSs were added to the supported OSs:
 - Microsoft(R) Windows Server(R) 2019
 - Microsoft(R) Windows Server(R) 2022
 - Red Hat(R) Enterprise Linux(R) Server 8 (64-bit x86_64)
 - Red Hat(R) Enterprise Linux(R) Server 9 (64-bit x86_64)
 - Oracle Linux(R) Operating System 8
 - Oracle Linux(R) Operating System 9
 - SUSE Linux(R) Enterprise Server 15
- The following OSs were deleted from the supported OSs:
 - Microsoft(R) Windows Server(R) 2012
 - Red Hat(R) Enterprise Linux(R) Server 6 (64-bit x86_64)
 - CentOS 6 (x64)
 - CentOS 7
 - Oracle Linux(R) Operating System 6 (x64)
- A description of the JP1/IM - EG for NNMi service was added.
- The default port number, which is set when a port number (`-port` option) is not specified during a new setup using the `setup` command (`jeqn_setup`), was changed.
- English UTF-8 encoding values were added for the environment variables file (`jeqn_env.conf` file) and environment variable `LANG` in the JP1/Base `jp1bs_param.conf` file.
- A description was added to the procedure for configuring automatic startup and termination settings in UNIX when SELinux is enabled.
- A description regarding data collection preparations for troubleshooting (Windows only) was added.
- The following descriptions were added to backup and restoration procedures:
 - Configuration information management
 - Backup and restoration of common definition information
- Boot process information was removed from OS log information retrievable using data collection tools in UNIX. Additional changes were made to the description of distribution information.

G.2 Changes in version 12-00

(1) Changes in the manual 3021-3-D57(E)

- The following operating system is no longer supported:

- Microsoft(R) Windows Server(R) 2008 R2
- It corresponds to TLSv1.2 by https connection with NNMi. Accordingly, changed the notation of SSL to the notation of TLS.
- The information was increased that can be obtained with data collection tool.

G.3 Changes in version 11-50

(1) Changes in the manual 3021-3-A13-10(E)

None.

H. Reference Material for this Manual

This appendix provides reference material for readers of this manual.

H.1 Related publications

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

Manuals related to JP1

- *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))
- *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems

Manuals related to JP1/IM

- *JP1 Version 13 Integrated Management 3: 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))
- *JP1 Version 12 Integrated Management 2: Getting Started* (3021-3-D50(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager Overview and System Design Guide* (3021-3-D51(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager Configuration Guide* (3021-3-D52(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager Administration Guide* (3021-3-D53(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager GUI Reference* (3021-3-D54(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager Command and Definition File Reference* (3021-3-D55(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager Messages* (3021-3-D56(E))
- *JP1 Version 11 Integrated Management: Getting Started (Integrated Console)* (3021-3-A06(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Overview and System Design Guide* (3021-3-A07(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Configuration Guide* (3021-3-A08(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Administration Guide* (3021-3-A09(E))
- *JP1 Version 11 JP1/Integrated Management - Manager GUI Reference* (3021-3-A10(E))

- *JP1 Version 11 JP1/Integrated Management - Manager Command and Definition File Reference (3021-3-A11(E))*
- *JP1 Version 11 JP1/Integrated Management - Manager Messages (3021-3-A12(E))*

H.2 Conventions: Abbreviations

This manual uses the following abbreviations for the names of Hitachi products and other products:

Abbreviation		Full name or meaning
JP1/IM	JP1/IM - Manager	JP1/Integrated Management - Manager
		JP1/Integrated Management 2 - Manager
		JP1/Integrated Management 3 - Manager
	JP1/IM - View	JP1/Integrated Management - View
		JP1/Integrated Management 2 - View
		JP1/Integrated Management 3 - View
JP1/IM - EG for NNMi		JP1/Integrated Management - Event Gateway for Network Node Manager i
		JP1/Integrated Management 2 - Event Gateway for Network Node Manager i
		JP1/Integrated Management 3 - Event Gateway for Network Node Manager i
Linux	Linux 7	Red Hat(R) Enterprise Linux(R) Server 7
	Linux 8	Red Hat(R) Enterprise Linux(R) Server 8
	Linux 9	Red Hat(R) Enterprise Linux(R) Server 9
	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
	SUSE Linux 12	SUSE Linux(R) Enterprise Server 12
	SUSE Linux 15	SUSE Linux(R) Enterprise Server 15
NNMi	JP1/NNMi	JP1/Network Node Manager i 11-00 or later
	JP1/NNMi Advanced	JP1/Network Node Manager i Advanced 11-00 or later

In this manual, *Linux* is generally referred to as *UNIX*.

H.3 Acronyms

This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
AP	Application Program

Abbreviation	Full name or meaning
API	Application Programming Interface
DB	Database
FTP	File Transfer Protocol
GUI	Graphical User Interface
ID	Identification number
IP	Internet Protocol
MSCS	Microsoft Cluster Service
OS	Operating System
PC	Personal Computer
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
WWW	World Wide Web

H.4 Conventions: KB, MB, GB and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.
- 1 TB (terabyte) is 1,024⁴ bytes.

I. Glossary

A

agent

A program that is managed by another program in the system or a host that is managed by another host in the system. JP1/IM - EG for NNMi is installed on an agent host.

B

basic attribute

A type of information item (attribute) of JP1 events that characterizes all JP1 events.

See *JP1 event*.

C

cluster system

A system in which multiple servers are linked and operated as a single system.

The purpose of a cluster system is to improve availability by enabling application processing to be transferred to another server in the event of a failure in the executing server. Such transfer of processing is called a *failover*.

If a failure occurs on the server that is executing an application (primary node), the standby server (secondary node) inherits the application. This is also called a *node switching system* because it involves switching of the application processing from the primary node to the secondary node.

There is also a type of cluster system that is configured to distribute the workload by running multiple servers in parallel. However, in this manual, *cluster system* refers to the configuration that supports failover in order to prevent interruption of application processing.

common definition information

A database that stores the definition parameters for the JP1 execution environment and that is managed by JP1/Base. This database is located on each server's local disk. It contains the definition parameters for the physical host and the logical host separately.

When JP1 is operated in a cluster system, the logical host definition contained in the common definition information must be the same between the servers of the primary and secondary nodes. Therefore, when setup and environment setup are performed, the parameters are set on the active server and then those settings are copied to the standby server.

conditional statement

A filtering conditional statement that is used to include as conversion targets those NNMi incidents that satisfy a specified condition. The conditional statements are specified in the filter condition block in the NNMi incident forwarding filter definition file.

E

Event Console window

A JP1/IM - View window that displays the JP1 events received by the central console arranged in the order received (by time). This is the first window displayed when you log in to JP1/IM - Central Console.

JP1/IM uses JP1 events to record the events that occur at each host and facilitates centralized management by transferring the important JP1 events to JP1/IM's manager host. By displaying these JP1 events in the Event Console window, you can monitor centrally the significant events that have occurred in the system.

event ID

A JP1 event attribute that identifies the program that issued the JP1 event and that indicates the nature of the event. The event ID is a basic attribute of JP1 events and its attribute name is `B.ID`.

The event ID is expressed in hexadecimal, such as `7FFF8000`.

Unique event IDs are assigned to each JP1-series product. For details about the JP1 events that are issued by each JP1-series product, see the appropriate documentation for each product.

Event IDs that can be used by the user are from `0` to `1FFF` and from `7FFF8000` to `7FFFFFFF`.

The details of JP1 events are indicated by an 8-byte numeric value that consists of the basic code (leading 4 bytes) and an extended code (trailing 4 bytes). Normally, only the 4-byte basic code is used. The extended code is set to `0` except when the user uses the API to set a code. When specification of both basic and extended codes is needed, they are connected by a colon (:), such as `7FFF8000:0`.

event server

A program that provides functions for managing JP1 events in JP1/Base. JP1 events can be collected and distributed while the event server is running.

event service

A function for registering and managing as JP1 events the events that occur in the system.

exclusion condition

A filtering conditional statement that is used to exclude as conversion targets those NNMi incidents that satisfy a specified condition. The exclusion conditions are specified in the filter condition block in the NNMi incident forwarding filter definition file.

extended attribute

A type of information item (attribute) of JP1 events that is specified by the programs that issue events.

See *JP1 event*.

F

failover

A function for ensuring uninterrupted processing by switching JP1 to another normal server in the event of a failure on the server where JP1 is running. Failover can also refer to switching of the servers that run JP1 by an action of a system administrator.

This is also referred to as *node switching*, because failover occurs from the active server to the standby server.

I

incident

A single failure event that has an adverse effect on the quality of IT services and prevents normal system operation.

J

JP1 common definition information

See *common definition information*.

JP1 event

Information used in JP1 to manage events that occur in the system.

JP1 events use the following attributes to record events:

- Basic attributes

All JP1 events have basic attributes.

For example, when attribute names are specified, B . ID (or just ID) is specified for the event ID.

- Extended attributes

A program that issues JP1 events can specify any desired extended attributes. The extended attributes consist of the following common information and program-specific information:

- Common information (extended attribute information whose format is standardized according to the JP1 event)

- Program-specific information (information other than the common information whose format is specific to a program)

For example, when attribute names are specified, E . SEVERITY (or just SEVERITY) is specified for the severity.

The JP1 events are managed by the event service of JP1/Base. Events that occur in the system are recorded in the database as JP1 events.

JP1/Base

The program that provides the event service. JP1/Base can be used to control the service startup sequence and to send and receive JP1 events. JP1/Base is a prerequisite program for JP1/IM - EG for NNMi.

JP1/IM - Manager

A program used to achieve integrated management of systems by providing for centralized monitoring and operation of the entire system.

JP1/IM - View

The program that provides the viewer function (GUI) for enabling integrated management of systems in JP1/IM.

JP1/NNMi

A collective name for integrated network management programs that manage the network configuration, performance, and failures.

JP1/Power Monitor

A program used to start and terminate hosts automatically. JP1/Power Monitor enables the user to start and terminate hosts on the basis of schedules, as well as to start and terminate remote hosts.

JP1/Software Distribution

A collective name for systems that use a network to perform software distribution and client management in the batch mode.

jp1hosts information

The `hosts` information that defines the correspondences between JP1-specific host names and IP addresses.

This information is used to customize JP1 communication operations in an environment that is connected to multiple networks. JP1/Base manages the `jp1hosts` information.

`jp1hosts` information does not support communication using IPv6 addresses. To use IPv6 addresses for communication, you must set `jp1hosts2` information.

See *jp1hosts2 information*.

During JP1 communication, the `jp1hosts` information has precedence over other information, such as `hosts`. This enables JP1-specific correspondences between host names and IP addresses that differ from the settings in the OS to be used for communication.

jp1hosts2 information

The `hosts` information that defines the correspondences between JP1-specific host names and IP addresses.

This information is used to customize JP1 communication operations in an environment that is connected to multiple networks. JP1/Base manages the `jp1hosts2` information.

To use IPv6 addresses for communication, you must set `jp1hosts2` information.

During JP1 communication, the `jp1hosts2` information has precedence over other information, such as `hosts`. This enables JP1-specific correspondences between host names and IP addresses that differ from the settings in the OS to be used for communication.

Note that JP1/IM - EG for NNMi supports IPv4/IPv6 mixed environment (dual-stack environment), however, it does not support an environment with IPv6 only.

L

logical host

A logical server that becomes the JP1 execution environment when JP1 is operating in a cluster system. This is also the unit of failover in the event of a failure.

A logical host has a logical IP address and a shared disk that are inherited during failover. It consists of applications, such as JP1 programs, that are run using the logical IP address and shared disk.

In the event of failover, the logical IP address and shared disk are transferred for continuation of JP1 execution. As a result, although the physical server running JP1 has changed, other hosts can still use the same IP address to access the server as if there had been no change in the operating host.

M

manager

A program whose role is to manage other programs in the system, or a host whose role is to manage other hosts in the system.

The JP1 events issued by JP1/IM - EG for NNMi are managed by the JP1/IM - Manager that is installed on the manager host.

N

NNMi incident

A single error event that is reported when something unintended occurs in a network device managed by JP1/NNMi.

node switching system

See *cluster system*.

P

physical host

The physical server in a cluster system (when JP1 is operating in the cluster system). In addition to the physical host, there are also logical hosts (so that a logical server can fail over without depending on the physical server).

S

severity

One of the attributes of JP1 events that indicates the seriousness of events in the system.

Severity belongs to the common information of the extended attributes of JP1 events. Its attribute name is `E.SEVERITY`.

The severity levels include Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

V

viewer

A program that provides appropriate GUI-based windows for achieving integrated management of JP1/IM systems. Viewer also refers to the host that runs the viewer.

Index

A

- abnormal process termination
 - setting JP1 event issuance in event of 37
 - settings for restarting after 37
- agent 18, 237
- applicable OS 18
- attribute of NNMi incident 56
- automated startup script 34
- automated stop script 34
- automatic startup, setting 33
- automatic termination, setting 33

B

- basic attribute 113, 237

C

- changing
 - host name 85
 - IP address 85
 - port number 85
 - system date and time 85
 - time zone 86
- cluster system 237
 - changing logical host name 85
 - deleting logical host 49
 - environment setup procedure 40
 - installing and setting up active server 42
 - installing and setting up logical host 42
 - installing and setting up standby server 43
 - notes about cluster operation 50
 - operation and environment configuration 39
 - procedure for changing settings 44
 - registering into cluster software 45
- commands 89
 - format of explanations of 90
 - jegn_killall.cluster (UNIX) 92
 - jegn_log.bat (Windows) 93
 - jegn_log.sh (UNIX) 95
 - jegn_setup 98
 - jegn_setup_cluster 103
 - jegn_spm�_reload 104
 - jegn_spm�_status 106
 - jegn_start.cluster (UNIX) 109
 - jegn_start (UNIX) 108

- jegn_stop.cluster (UNIX) 111
- jegn_stop (UNIX) 110
 - lists of 91
 - startup, termination, and setup 91
 - troubleshooting 91
- common definition information 237
- conditional statement 54, 237
- conventions
 - diagrams 6
 - fonts and symbols 7
- conversion procedure 20
- custom attribute mapping definition file
 - creating 68
 - format of 69
 - name and storage location of 68

D

- data collection tool 199
- definition files 228
 - custom attribute mapping definition file 68
 - definition file for executing applications 76
 - definition file for extended event attributes 71
 - definition file for opening monitor windows 75
 - editing 84
 - editing JP1/IM - Manager 71
 - extended startup process definition file 229
 - JP1/IM - EG for NNMi parameter definition file 230
 - mapping definition file 66
 - NNMi incident forwarding filter definition file 52
 - setting 33
- details of event ID
 - 0x00006100 120
 - 0x000061F0 120
 - 0x000061F1 121
 - 0x000061F2 121
- diagram conventions 6
- directories, list of 218

E

- editing
 - definition file 84
 - hosts file 85
 - jp1hosts2 definition file 85
 - jp1hosts definition file 85

- environment variables settings (UNIX only) 31
- error, settings for handling 35
- Event Console window 238
- event ID 238
- event server 238
- event service 238
- exclusion condition 54, 238
- extended attribute 113, 238
 - checking mapping result of 64
 - common information 113
 - mapping 63
 - program-specific information 113
 - total size of 64
- extended startup process definition file 229

F

- failover 238
- files, list of
 - UNIX 218
 - Windows 217
- filter condition block 54
 - example of 60
 - format of 54
- folders, list of 217
- font conventions 7

G

- glossary 237

H

- Hitachi Program Product Installer, using 27
- host name, changing 85
- hosts file, editing 85

I

- incident 239
- installation 23
 - notes in UNIX 29
 - notes in Windows 25
 - procedure in UNIX 26
 - procedure in Windows 24
- internal attribute, displaying 74
- IP address, changing 85

J

- jegn_killall.cluster (UNIX) 92
- jegn_log.bat (Windows) 93
- jegn_log.sh (UNIX) 95
- jegn_setup 98
- jegn_setup_cluster 103
- jegn_spm�_reload 104
- jegn_spm�_status 106
- jegn_start.cluster (UNIX) 109
- jegn_start (UNIX) 108
- jegn_stop.cluster (UNIX) 111
- jegn_stop (UNIX) 110
- JP1/Base 239
- JP1/IM - EG for NNMi 16
 - applicable OS 18
 - overview of operation using 17
 - parameter definition file 230
 - prerequisite program 19
 - starting 78
 - system configuration 18
 - terminating 79
- JP1/IM - EG for NNMi service 21
- JP1/IM - Manager 239
 - editing definition file 71
- JP1/IM - View 239
- JP1/NNMi 240
- JP1/Power Monitor 34, 240
- JP1/Software Distribution 240
 - remote installation in UNIX 26
 - remote installation in Windows 24
- JP1 common definition information 239
- JP1 event 239
- JP1 events 112
 - attributes of 113
 - basic attribute 113
 - converting NNMi incidents into 51
 - details of 120
 - extended attribute 113
 - issued by JP1/IM - EG for NNMi 119
 - list of 120
 - obtained by converting NNMi incidents 114
- jp1hosts2 definition file, editing 85
- jp1hosts2 information 240
- jp1hosts definition file, editing 85
- jp1hosts information 240

L

- language code 31
- limit values, list of 222
- logical host 240
 - deleting 49
 - installing and setting up 42
- log information, types of 194

M

- manager 18, 241
- mapping block 61
 - extended attribute mapping 63
 - message mapping 61
 - severity mapping 62
- mapping definition file
 - creating 66
 - format of 66
 - name and storage location of 66
- memory requirements 223
- message mapping 61
- messages 122
 - command execution 134
 - editing 61
 - format of explanations of 129
 - installation 131
 - KAVB3501 to KAVB3999 166
 - KNAG0001 to KNAG0999 131
 - KNAG1000 to KNAG1999 134
 - KNAG2000 to KNAG2999 149
 - list of 131
 - maximum size of 62
 - output destinations 123
 - output destinations of, related to command execution 123
 - output destinations of, related to installation 123
 - output destinations of, related to process management 125
 - output destinations of, related to services 124
 - output format of 129
 - process management 166
 - services 149

N

- NNMi incident 16, 241
 - attribute of 56
 - attribute value of 58

- conversion procedure 20
- converting, into JP1 event 51
- NNMi incident forwarding filter definition file
 - creating 52
 - defining filter condition block 54
 - defining mapping block 61
 - definition example 64
 - format of 52
 - operand 55
 - operator 55
 - sample file 64
- node switching system 241
- Notes regarding operation 88

O

- operand 55
- operation, overview of 17
- operator 55
- overwrite installation and upgrade installation
 - UNIX 26
 - Windows 24
- overwrite setup 31

P

- performance and estimation 223
- physical host 241
- port number, changing 85
- prerequisite program 19
- primary data
 - UNIX 95
 - Windows 93
- processes, list of 221

R

- regular expression 224
 - example of 226
 - hints on using 226
 - specifying 225
 - syntax for 224
- remote installation
 - UNIX 26
 - Windows 24
- required disk capacity 223

S

- secondary data

UNIX 95

Windows 93

setting

JP1 event issuance in event of abnormal process termination 37

preparation for collecting data in event of error (Windows) 35

restart after abnormal process termination 37

suppressing error reporting to Microsoft 37

setting language code in common definition 32

setting language code in environment variable file 31

settings

backing up 81

changing 84

restoring 83

setup 23, 30

severity 241

mapping 62

starting 78

start sequence definition file 33

startup control 33

symbol conventions 7

syntax conventions 8

system administrator, notes for 130

system configuration 18

system date and time, changing 85

T

terminating 79

time zone, changing 86

TLS protocol versions can be used 31

trace log

for each process 198

for issued JP1 events 195

integrated 194

troubleshooting 192

command 91

data to be collected in UNIX 206

data to be collected in Windows 199

primary data for UNIX 95

primary data for Windows 93

procedure 193

secondary data for UNIX 95

secondary data for Windows 93

types of log information 194

U

uninstallation

procedure in UNIX 27

procedure in Windows 25

V

viewer 18, 242

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
