

**JP1 Version 11**

**JP1/Performance Management User's Guide**

**3021-3-A38-30(E)**

## Notices

### ■ Relevant program products

*JP1/Performance Management - Manager (for Windows Server 2008 R2, Windows Server 2012, Windows Server 2016)*

P-2A2C-AABL JP1/Performance Management - Manager 11-50

List of products and product names:

P-CC2A2C-5ABL JP1/Performance Management - Manager 11-50

P-CC2A2C-5RBL JP1/Performance Management - Web Console 11-50

*JP1/Performance Management - Manager (for CentOS 6 (x64), CentOS 7, Linux 6 (x64), Linux 7, Oracle Linux 6 (x64), Oracle Linux 7, SUSE Linux 12)*

P-812C-AABL JP1/Performance Management - Manager 11-50

List of products and product names:

P-CC812C-5ABL JP1/Performance Management - Manager 11-50

P-CC812C-5RBL JP1/Performance Management - Web Console 11-50

*JP1/Performance Management - Manager (for AIX V6.1, AIX V7.1, AIX V7.2)*

P-1M2C-AABL JP1/Performance Management - Manager 11-50

List of products and product names:

P-CC1M2C-5ABL JP1/Performance Management - Manager 11-50

P-CC1M2C-5RBL JP1/Performance Management - Web Console 11-50

*JP1/Performance Management - Base (for Windows Server 2008 R2, Windows Server 2012, Windows Server 2016)*

P-CC2A2C-AJBL JP1/Performance Management - Base 11-50

*JP1/Performance Management - Base (for HP-UX 11i V3 (IPF))*

P-CC1J2C-AJBL JP1/Performance Management - Base 11-50

*JP1/Performance Management - Base (for CentOS 6 (x64), CentOS 7, Linux 6 (x64), Linux 7, Oracle Linux 6 (x64), Oracle Linux 7, SUSE Linux 12)*

P-CC812C-AJBL JP1/Performance Management - Base 11-50

*JP1/Performance Management - Base (for Solaris 10, Solaris 11)*

P-CC9D2C-AJBL JP1/Performance Management - Base 11-50

*JP1/Performance Management - Base (for AIX V6.1, AIX V7.1, AIX V7.2)*

P-CC1M2C-AJBL JP1/Performance Management - Base 11-50

In addition to the above products, this product is targeted at the PFM - Agent and PFM - RM products of JP1/Performance Management, which require JP1/Performance Management - Base. Also, these products include parts that were developed under licenses received from third parties.

## ■ Trademarks

HITACHI, Cosminexus, HiRDB, JP1, OpenTP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

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

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

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

IBM, AIX 5L are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Intel is a trademark of Intel Corporation in the U.S. and/or other countries.

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

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

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

ODBC is Microsoft's strategic interface for accessing databases.

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

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

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

SAP and R/3 and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

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

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

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

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

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

The following program product contains some parts whose copyrights are reserved by Oracle and/or its affiliates: P-CC9D2C-AJBL

The following program products contain some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-CC9D2C-AJBL.

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

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

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

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

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

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

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

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

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://java.apache.org/>).

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

This product includes software developed by Andy Clark.



JP1/Performance Management - Web Console includes RSA BSAFE(R) software developed by EMC Corporation of the United States.

**HITACHI**  
Inspire the Next

Hitachi, Ltd.



1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)
2. This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))
3. This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))
4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

OpenSSL License

-----

/\* =====

\* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.

\*



\* Redistribution and use in source and binary forms, with or without  
\* modification, are permitted provided that the following conditions  
\* are met:  
\*  
\* 1. Redistributions of source code must retain the above copyright  
\* notice, this list of conditions and the following disclaimer.  
\*  
\* 2. Redistributions in binary form must reproduce the above copyright  
\* notice, this list of conditions and the following disclaimer in  
\* the documentation and/or other materials provided with the  
\* distribution.  
\*  
\* 3. All advertising materials mentioning features or use of this  
\* software must display the following acknowledgment:  
\* "This product includes software developed by the OpenSSL Project  
\* for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"  
\*  
\* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to  
\* endorse or promote products derived from this software without  
\* prior written permission. For written permission, please contact  
\* [openssl-core@openssl.org](mailto:openssl-core@openssl.org).  
\*  
\* 5. Products derived from this software may not be called "OpenSSL"  
\* nor may "OpenSSL" appear in their names without prior written  
\* permission of the OpenSSL Project.  
\*  
\* 6. Redistributions of any form whatsoever must retain the following  
\* acknowledgment:  
\* "This product includes software developed by the OpenSSL Project  
\* for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"  
\*  
\* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY  
\* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
\* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
\* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR  
\* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,  
\* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT  
\* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;  
\* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
\* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,  
\* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)  
\* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED

```

* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given
attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:

```

```

* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the routines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

## ■ 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.

## ■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation	Full name or meaning
Exchange Server	Microsoft(R) Exchange Server
IIS	Microsoft(R) Internet Information Services

Abbreviation		Full name or meaning
Internet Explorer		Windows(R) Internet Explorer(R)
SQL Server		Microsoft(R) SQL Server 2005 Enterprise Edition
		Microsoft(R) SQL Server 2005 Standard Edition
		Microsoft(R) SQL Server 2008 Enterprise
		Microsoft(R) SQL Server 2008 Enterprise R2
		Microsoft(R) SQL Server 2008 Standard
		Microsoft(R) SQL Server 2008 Standard R2
		Microsoft(R) SQL Server 2012 Business Intelligence Edition
		Microsoft(R) SQL Server 2012 Enterprise Edition
		Microsoft(R) SQL Server 2012 Standard Edition
Windows Server 2008	Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2016		Microsoft(R) Windows Server(R) 2016 Datacenter
		Microsoft(R) Windows Server(R) 2016 Standard
WSFC		Microsoft(R) Windows Server(R) Failover Cluster

Windows Server 2008, Windows Server 2012, and Windows Server 2016 are sometimes referred to as *Windows*.

## ■ Issued

Nov. 2017: 3021-3-A38-30(E)

## ■ Copyright

Copyright (C) 2016, 2017, Hitachi, Ltd.

Copyright (C) 2017, Hitachi Solutions, Ltd.

(C)copyright 2000-2009, by Object Refinery Limited and Contributors.

## Summary of amendments

The following table lists changes in this manual (3021-3-A38-30(E)) and product changes related to this manual.

Changes	Location
Added the auto alarm bind function.	<i>2.2.1, 2.2.2, 6.2.1, 6.2.3, 6.4.12, 9.2.6(1), 9.2.7(1), 9.2.11, 11.1.3(1), 11.1.3(2), 11.3.6(1), 11.6.1(8), 17.5.1(2), 17.5.2(2)</i>
A folder having the name of the host can now be automatically created as the folder to which to add agents.	<i>3.2.1(2)</i>
Modified the description regarding the partial backup of performance data with Store version 2.0.	<i>9.3.4</i>
Added a monitoring process that is linked with the IT service management product (JP1/SS).	<i>Chapter 15</i>
Added a troubleshooting guide to be followed when no alarm event is displayed after the port number of the PFM - Manager is changed during operation.	<i>17.2.8(5)</i>
Added a description regarding the materials that must be collected when an issue occurs with Performance Management used in a Docker environment.	<i>17.5.1(8), 17.5.2(6)</i>

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

## Preface

This manual describes methods of operating JP1/Performance Management, how to manage a system when linking with other systems, and troubleshooting.

### ■ Intended readers

This manual is intended for:

- Those who wish to gain an understanding of the operating procedures for JP1/Performance Management in the context of an operation monitoring system
- Those who wish to define conditions for collecting performance data
- Those who wish to define reports and alarms
- Those who wish to monitor a system with reference to collected performance data
- Those who wish to plan strategies for improving the system based on the monitoring results

This manual assumes that the reader is familiar with the system being monitored.

For details on how to collect performance data using JP1/Performance Management - Agent or JP1/Performance Management - Remote Monitor, refer to the manuals for each of these products.

### ■ Organization of this manual

This manual is organized into the following parts. Note that this manual contains information common to all the operating systems that this product supports. If there are differences relating to specific operating systems, we note these differences in the text.

#### *PART 1: Operation*

PART 1 describes how to operate JP1/Performance Management.

#### *PART 2: System Linkage*

PART 2 describes how to configure and operate JP1/Performance Management when you use it in a cluster system or a multiple-monitoring configuration, or link it with other systems.

#### *PART 3: Troubleshooting*

PART 3 describes how to detect errors with JP1/Performance Management and what action you should take when a problem occurs.

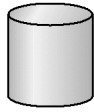
### ■ Conventions: Diagrams

This manual uses the following conventions in diagrams:

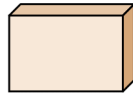
● Server



● Shared disk or local disk



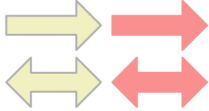
● Program



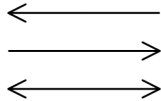
● I/O operation



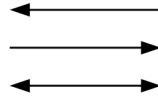
● Data flow



● Control flows



● Other flows



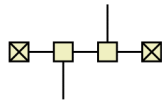
● Processing flow



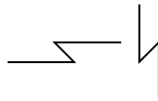
● WAN (Wide Area Network)



● LAN (Local Area Network)



● Communication line



● Window



● Problems



## ■ Conventions: Fonts and symbols

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

Text formatting	Convention
<b>Bold</b>	<p>Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example:</p> <ul style="list-style-type: none"> <li>From the <b>File</b> menu, choose <b>Open</b>.</li> <li>Click the <b>Cancel</b> button.</li> <li>In the <b>Enter name</b> entry box, type your name.</li> </ul>
<i>Italic</i>	<p>Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none"> <li>Write the command as follows: <code>copy source-file target-file</code></li> <li>The following message appears: A file was not found. (file = <i>file-name</i>)</li> </ul> <p>Italic characters are also used for emphasis. For example:</p> <ul style="list-style-type: none"> <li>Do <i>not</i> delete the configuration file.</li> </ul>
Monospace	<p>Monospace characters indicate 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"> <li>At the prompt, enter <code>dir</code>.</li> <li>Use the <code>send</code> command to send mail.</li> <li>The following message is displayed: <code>The password is incorrect.</code></li> </ul>

The following table explains the symbols used in this manual:

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

### Conventions for mathematical expressions

This manual uses the following symbols in mathematical expressions:

Symbol	Meaning
×	Multiplication sign
÷	Division sign

### ■ Conventions: Version numbers

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

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

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



# Contents

Notices	2
Summary of amendments	9
Preface	10

## Part 1: Operation

<b>1</b>	<b>Starting and Stopping Performance Management</b>	<b>26</b>
1.1	Start and stop sequence for the entire Performance Management system	27
1.1.1	Start sequence for the entire Performance Management system	27
1.1.2	Stop sequence for the entire Performance Management system	28
1.2	Starting services	30
1.2.1	Starting services on monitoring managers and monitoring agents	30
1.2.2	Starting services on the monitoring console server	35
1.3	Stopping services	40
1.3.1	Stopping services on monitoring managers and monitoring agents	40
1.3.2	Stopping services on the monitoring console server	43
1.4	Synchronizing the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console	46
1.4.1	Synchronizing starting and stopping	46
1.4.2	Command options when synchronizing service starting and stopping	46
1.5	Logging on to and off from PFM - Web Console	48
1.5.1	Logging on to PFM - Web Console	48
1.5.2	Logging off from PFM - Web Console	48
1.6	Checking the status of services	50
1.6.1	Checking the status of services by using a command	50
1.6.2	Checking the status of services from the web browser	51
1.7	Setting the automatic refresh interval for Web browsers	53
1.8	Notes on starting and stopping Performance Management	54
1.8.1	When starting PFM - Agent or PFM - RM in a large-scale system	54
1.8.2	Starting a PFM - Agent or PFM - RM service during command execution	60
1.8.3	Starting on a Windows machine	60
1.8.4	Monitoring alarm events	61
1.8.5	Executing actions	61
1.8.6	Changing settings when using business groups	62
<b>2</b>	<b>Managing User Accounts and Business Groups</b>	<b>63</b>
2.1	Overview of user accounts and business groups	64
2.1.1	About user authentication modes	64

2.1.2	About user permissions	64
2.1.3	About business groups	64
2.2	User account permissions	66
2.2.1	Functions available to system users	66
2.2.2	Functions available to business group users	71
2.3	Tasks involved in user account setup	76
2.4	Setting the user account authentication mode	78
2.5	Setting up and using Performance Management user accounts	79
2.5.1	Creating a Performance Management user account	79
2.5.2	Editing a Performance Management user account	81
2.6	Setting operating permissions for JP1 users	84
2.7	Setting and using business groups	85
2.7.1	Setting up access control based on business groups	85
2.7.2	Defining business groups in Performance Management	86
2.7.3	Using business groups defined in JP1/IM	89
2.7.4	Using business groups	90
<b>3</b>	<b>Monitoring Agents</b>	<b>95</b>
3.1	Monitoring by using the Agents tree	96
3.1.1	Agent types	97
3.2	Creating and editing an Agents tree in a Web browser	98
3.2.1	Creating an Agents tree	98
3.2.2	Editing the Agents tree	101
3.2.3	Limiting the agents available to users with general user permission	103
3.3	Using commands to create and edit an Agents tree	104
3.3.1	Creating an Agents tree	104
3.3.2	Editing an Agents tree	105
3.4	Monitoring the status of agent operations	106
3.4.1	Checking the status of agents	106
3.4.2	Checking the status of alarms	107
3.4.3	Displaying reports	109
3.4.4	Displaying event history	109
3.4.5	Using summary display to check the operating status	109
3.4.6	Displaying agent properties	116
3.4.7	Editing agent properties	117
3.4.8	Distributing agent properties as a batch	117
<b>4</b>	<b>Managing Operation Monitoring Data</b>	<b>125</b>
4.1	Managing performance data	126
4.1.1	Modifying the recording options for performance data	126
4.1.2	Modifying the retention conditions for performance data (in Store 2.0)	134
4.1.3	Modifying the retention conditions for performance data (in Store 1.0)	141

- 4.1.4 Exporting performance data 149
- 4.1.5 Checking the disk space used for performance data 150
- 4.1.6 Erasing performance data 151
- 4.1.7 Importing backup data (with Store 2.0) 151
- 4.1.8 Converting the data model of backup data (with Store 2.0) 152
- 4.1.9 Displaying information about the Agent Store and Remote Monitor Store services or backup directory (in Store 2.0) 152
- 4.2 Managing event data 154
  - 4.2.1 Changing the maximum number of records for event data 154
  - 4.2.2 Exporting event data 155
  - 4.2.3 Checking the disk space used for event data 155
  - 4.2.4 Erasing event data 156
- 4.3 Notes on working with operation monitoring data in Performance Management 157
  - 4.3.1 Record retention periods in the Store database 157
  - 4.3.2 Size limits that apply to the Store database 157
  - 4.3.3 When the Agent Store or Remote Monitor Store service stops abnormally 158
  - 4.3.4 When the system has insufficient disk capacity 159
  - 4.3.5 Checking the database size and reorganizing the Store database 162
  - 4.3.6 Deleting files and folders that remain in the system after exceeding the retention period 163
  - 4.3.7 Default retention periods for records in Store 2.0 163
  - 4.3.8 Performance data stored after a data model upgrade 164

## **5 Creation of Reports for Operation Analysis 165**

- 5.1 Overview of reports 166
  - 5.1.1 About reports 166
  - 5.1.2 Report types 166
  - 5.1.3 Display formats of reports 167
- 5.2 Overview and procedure for report creation 170
  - 5.2.1 How to create reports 170
  - 5.2.2 Process flow for creating reports 170
- 5.3 Creating reports in the Web browser (Reports tree) 172
  - 5.3.1 Creating a report folder 172
  - 5.3.2 Displaying the New Report window 172
  - 5.3.3 Setting the name and type of a report 172
  - 5.3.4 Setting fields displayed in a report 174
  - 5.3.5 Setting display conditions for fields displayed in a report (filter condition) 175
  - 5.3.6 Setting the display information for a report (refresh interval and display period) 176
  - 5.3.7 Setting the display format (table, list, or graph) of a report 177
  - 5.3.8 Associating a report with another report (drilldown report) 179
  - 5.3.9 Copying a report 180
  - 5.3.10 Editing a report 180
  - 5.3.11 Renaming a folder or report 182

5.3.12	Deleting a folder or report	183
5.3.13	Exporting reports	183
5.3.14	Importing reports	184
5.4	Creating reports in the Web browser (Quick Guide)	185
5.4.1	Creating reports using Quick Guide	185
5.4.2	Searching for fields	185
5.4.3	Default values used for reports created with the Quick Guide	186
5.5	Creating reports by using commands	188
5.5.1	Outputting and customizing report definitions	188
5.5.2	Deleting an unnecessary report	189
5.6	Creating and editing bookmarks in the Web browser	190
5.6.1	Creating bookmarks	190
5.6.2	Adding a bookmark folder	192
5.6.3	Renaming folders and bookmarks	193
5.6.4	Deleting folders, bookmarks, and reports	194
5.6.5	Checking the properties of a bookmark	195
5.6.6	Tiling reports registered in bookmarks	195
5.7	Displaying reports	199
5.7.1	Displaying reports	199
5.7.2	Checking the report properties (definition)	203
5.7.3	Setting the display conditions for a report	203
5.7.4	Displaying a drilldown report	205
5.7.5	Using Autolabel to check data values	207
5.7.6	Changing the color of graph series	209
5.8	Displaying combination reports	212
5.8.1	Preparing to display combination reports	215
5.8.2	Displaying combination reports	216
5.8.3	Checking the properties (definitions) of combination bookmarks	217
5.8.4	Examples of using combination reports in real-world situations	218
5.9	Outputting reports	223
5.9.1	Exporting reports in CSV or HTML format by using a Web browser	223
5.9.2	Exporting reports in CSV or HTML format by using a command	224
5.9.3	CSV format	225
5.9.4	HTML format	226
5.10	Notes on reports	229
5.10.1	Notes on creating reports	229
5.10.2	Notes on displaying reports	229
5.10.3	Notes on combination reports	236
<b>6</b>	<b>Monitoring Operations with Alarms</b>	<b>241</b>
6.1	Overview of alarms	242
6.2	Setting up and operating alarms	243

6.2.1	How to set up and operate alarms	243
6.2.2	Alarm evaluation	244
6.2.3	Flow chart for setting up and operating alarms	250
6.3	Procedures before setting alarms	252
6.3.1	Configuring the email sender	252
6.3.2	Configuring the host to automatically execute commands	252
6.3.3	Configuration for issuing JP1 events	254
6.3.4	Configuration for sending SNMP traps	254
6.3.5	Setting the function for measurement value output at alarm recovery	254
6.4	Setting alarms using the Web browser (Alarms tree)	261
6.4.1	Creating an alarm table	261
6.4.2	Creating an alarm (setting the basic information)	261
6.4.3	Setting a value whose existence is to be monitored	263
6.4.4	Setting the alarm conditions	263
6.4.5	Setting the actions	266
6.4.6	Associating a report with an alarm	270
6.4.7	Copying an alarm table or alarm	271
6.4.8	Editing an alarm	272
6.4.9	Deleting an alarm table or alarm	272
6.4.10	Exporting alarm tables	273
6.4.11	Importing alarm tables	274
6.4.12	Automatically binding alarms to monitoring agents	274
6.5	Setting alarms using the Web browser (Quick Guide)	276
6.5.1	Creating an alarm using Quick Guide	276
6.5.2	The default values of an alarm created by using the Quick Guide	277
6.6	Operating alarms by using the Web browser	279
6.6.1	Changing the association between an alarm table and a monitoring agent	279
6.6.2	Displaying the monitoring agents bound to an alarm table	281
6.6.3	Stopping monitoring with an alarm	282
6.6.4	Starting monitoring with an alarm	282
6.6.5	Checking alarm application status	283
6.6.6	Displaying alarm properties (definitions)	285
6.7	Setting alarms by using commands	287
6.7.1	Creating an alarm definition file	287
6.7.2	Checking the alarm definition file	298
6.7.3	Modifying an alarm definition	298
6.7.4	Copying an alarm table	300
6.7.5	Deleting an alarm table	301
6.7.6	Deleting an alarm	302
6.8	Operating alarms by using commands	304
6.8.1	Associating an alarm table with a monitoring agent	304

- 6.8.2 Unbinding an alarm table bound to a monitoring agent 306
- 6.8.3 Checking the connection between an alarm table and a monitoring agent 309
- 6.8.4 Stopping monitoring with an alarm 310
- 6.8.5 Starting monitoring with an alarm 311
- 6.8.6 Checking the properties of an alarm table 312
- 6.9 Notes on alarms 315
- 6.9.1 Notes on creating alarms 315
- 6.9.2 Notes on the relationship between alarm damping and the issuing of alarm events 316
- 6.9.3 Notes on evaluating alarms 325
- 6.9.4 Notes about alarm application status 327

## **7 Displaying Events 329**

- 7.1 Displaying the latest events 330
- 7.1.1 Displaying the latest events information 330
- 7.1.2 Displaying a report associated with an alarm 331
- 7.1.3 Displaying alarm properties 331
- 7.1.4 Setting the display conditions for the Event Monitor window 332
- 7.2 Displaying the event history 333
- 7.2.1 Displaying the event history 333
- 7.3 Outputting the event history 336
- 7.3.1 Outputting the event history in CSV format 336
- 7.3.2 Outputting the event history in HTML format 336

## **8 Suspending and Resuming Monitoring 337**

- 8.1 Overview of the monitoring suspension function 338
- 8.1.1 Prerequisites for the monitoring suspension function 338
- 8.1.2 Alarms while monitoring is suspended 339
- 8.1.3 Health check while monitoring is suspended 339
- 8.1.4 Operating information while monitoring is suspended 340
- 8.1.5 Monitoring suspension function and system linkage 340
- 8.2 Range of suspending or resuming monitoring 342
- 8.2.1 Range of monitoring suspended or resumed by the host 342
- 8.2.2 Range of monitoring suspended or resumed by the agent 343
- 8.3 Setting the monitoring suspension function 345
- 8.3.1 Monitoring suspension function option 345
- 8.3.2 Automatic synchronization options of the settings information for the monitoring suspension function (for multiple-monitoring) 345
- 8.3.3 Suspending monitoring from a Web browser 346
- 8.3.4 Resuming monitoring from a Web browser 347

## **9 Backing Up and Restoring Data 348**

- 9.1 Overview of backing up and restoring data 349

9.1.1	Information that needs to be backed up	349
9.1.2	Notes on backup and restoration in a cluster system	351
9.2	Backing up and restoring definition information	352
9.2.1	Methods of backing up and restoring definition information	352
9.2.2	Using a command to back up and restore definition information (other than PFM - Web Console)	354
9.2.3	Using a command for backup and file copying for restoration (PFM - Web Console)	357
9.2.4	Backing up and restoring definition information by copying files (other than PFM - Web Console)	366
9.2.5	Backing up and restoring definition information by copying files (PFM - Web Console)	368
9.2.6	Files to be backed up (in Windows)	369
9.2.7	Files to be backed up (in UNIX)	376
9.2.8	Backing up and restoring a report definition	383
9.2.9	Backing up and restoring an alarm definition	383
9.2.10	Backing up and restoring a business group definition	383
9.2.11	Backing up and restoring specific definition information (auto alarm bind definition information)	384
9.2.12	Backing up and restoring a bookmark definition	385
9.2.13	Backing up and restoring a process monitoring definition template	390
9.3	Backing up and restoring operation monitoring data	392
9.3.1	Backup methods	392
9.3.2	Backing up and restoring the event data	392
9.3.3	Backing up and restoring the performance data	394
9.3.4	Partially backing up performance data (Store 2.0)	397
9.4	Migrating Performance Management data to another system	402
9.4.1	Data that can be migrated	402
9.4.2	Migrating data from one Performance Management system to another	402

## Part 2: System Linkage

### 10 Cluster System Configuration and Operation 404

10.1	Overview and design of cluster systems	405
10.1.1	Overview of cluster systems	405
10.1.2	Designing a cluster configuration	407
10.1.3	Planning the network configuration	412
10.1.4	Planning the data configuration	413
10.1.5	Planning operation in a cluster system	414
10.1.6	Planning the failover method	414
10.2	Configuration in a cluster system (in Windows)	415
10.2.1	Before installation and setup	415
10.2.2	Installing and setting up PFM - Manager	417
10.2.3	Installing and setting up PFM - Web Console	429
10.2.4	Installing an upgrade for PFM - Agent or PFM - RM	434
10.2.5	Unsetup and uninstallation of PFM - Manager	435
10.2.6	Unsetup and uninstallation of PFM - Web Console	441

10.3	Changing the cluster system configuration (in Windows)	443
10.3.1	Adding PFM - Agent or PFM - RM	443
10.3.2	Deleting PFM - Agent or PFM - RM	447
10.3.3	Changing logical host names after starting operation	449
10.3.4	Changing the logical host environment after starting operation	463
10.4	Configuration in a cluster system (in UNIX)	465
10.4.1	Before installation and setup	465
10.4.2	Installing and setting up PFM - Manager	466
10.4.3	Installing and setting up PFM - Web Console	478
10.4.4	Installing an upgrade for PFM - Agent or PFM - RM	483
10.4.5	Unsetup and uninstallation of PFM - Manager	483
10.4.6	Unsetup and uninstallation of PFM - Web Console	489
10.5	Changing the cluster system configuration (in UNIX)	491
10.5.1	Adding PFM - Agent or PFM - RM	491
10.5.2	Deleting PFM - Agent or PFM - RM	495
10.5.3	Changing logical host names after starting operation	497
10.5.4	Changing the logical host environment after starting operation	510
10.6	Operation in a cluster system	513
10.6.1	Starting and stopping Performance Management in a cluster system	513
10.6.2	Managing user accounts in a cluster system	516
10.6.3	Managing agents in an integrated cluster system	516
10.6.4	Collecting and managing operation monitoring data in a cluster system	517
10.6.5	Creating reports in a cluster system	517
10.6.6	Performing realtime operation monitoring by alarms in a cluster system	518
10.6.7	Performing backup and restore in a cluster system	518
10.6.8	Performing the required operation when a failover occurs in a cluster system	519
10.7	Failure recovery in a cluster system	522
10.7.1	Collecting the log information in a cluster system	522
10.8	Notes on cluster systems	523
10.8.1	Detecting failovers	523
10.8.2	Starting and stopping Performance Management	523
10.8.3	Setting Status Server services	523
10.8.4	Executing commands	523
10.8.5	Networks	524
10.8.6	When using JP1 authentication mode	524

## **11 Configuring and Employing Performance Management for Multiple Monitoring 525**

11.1	Overview of multiple monitoring	526
11.1.1	About multiple monitoring	526
11.1.2	Features of multiple monitoring	526
11.1.3	Definition information for multiple monitoring	528



11.2	Before configuring a multiple-monitoring environment	533
11.2.1	System configuration for multiple monitoring	533
11.2.2	Prerequisite product version	535
11.2.3	Prerequisites related to PFM - Manager	535
11.2.4	Prerequisites related to PFM - Web Console	535
11.3	Setting up multiple monitoring	537
11.3.1	Procedure for setting up multiple monitoring	537
11.3.2	Installing and setting up programs	538
11.3.3	Link with other systems in a multiple-monitoring environment	539
11.3.4	Setting PFM - Manager for the connection destination for multiple monitoring	540
11.3.5	Controlling remote actions	541
11.3.6	Setting operation monitoring	542
11.3.7	Checking and changing the action handler for alarms	543
11.3.8	Upgrading PFM - Manager and PFM - Web Console	544
11.4	Unsetting up multiple monitoring	545
11.4.1	Procedure of unsetting up multiple monitoring	545
11.4.2	Releasing links with other systems in a multiple-monitoring environment	546
11.4.3	Deleting the services of the secondary Manager	547
11.4.4	Synchronizing service information with PFM - Web Console	547
11.4.5	Reconfiguring PFM - Manager for connection destination to release multiple monitoring	547
11.4.6	Deleting service information	547
11.5	Duplicating definition information	548
11.5.1	Procedure for duplicating definition information	548
11.5.2	Exporting definition information	549
11.5.3	Importing definition information	551
11.6	Checking duplication of definition information and operation monitoring data	553
11.6.1	Checking duplication of the PFM - Manager definition information	553
11.6.2	Checking duplication of the PFM - Web Console definition information	556
11.6.3	Checking the settings of PFM - Manager to which the monitoring agent connects	557
11.6.4	Checking whether operation monitoring data matches	558
11.7	Switching the primary Manager and the secondary Manager	559
11.7.1	Procedure for switching the primary Manager and the secondary Manager	559
11.7.2	Batch switching the primary Manager and the secondary Manager	560
11.7.3	Switching the primary Manager and the secondary Manager separately	561

## **12 Linking with the Integrated Management Product JP1/IM for Operation Monitoring 562**

12.1	Overview of linking with the integrated management product JP1/IM for operation monitoring	563
12.1.1	Monitoring by using integrated console	564
12.1.2	Monitoring by using integrated scope	564
12.1.3	Linkage of Performance Management and JP1/IM	565
12.2	JP1 events issued from Performance Management to JP1/IM	566

- 12.2.1 JP1 event types 566
- 12.3 Installation and setup when linking with JP1/IM 567
  - 12.3.1 Prerequisites for installation when linking with JP1/IM 567
  - 12.3.2 Setup for linking with JP1/IM (settings for using JP1/IM to monitor events that occurred in Performance Management) 568
  - 12.3.3 Setup for linking with JP1/IM (settings for displaying reports from events in the integrated console) 581
  - 12.3.4 Releasing linkage with JP1/IM 582
- 12.4 Changing the configuration after linking with JP1/IM 583
  - 12.4.1 Changing a host name after linking with JP1/IM 583
  - 12.4.2 Changing an IP address after linking with JP1/IM 583
- 12.5 Operating the linkage with JP1/IM 584
  - 12.5.1 Monitoring alarm events from the JP1/IM integrated console 584
  - 12.5.2 Monitoring from the JP1/IM integrated scope 584
  - 12.5.3 Displaying a Performance Management report from the JP1/IM integrated console 584
  - 12.5.4 Starting PFM - Web Console from the JP1/IM integrated management menu 585
- 12.6 List of attributes of JP1 events issued when linking with JP1/IM 586
  - 12.6.1 When alarm events occur 586
  - 12.6.2 When Performance Management services start 588
  - 12.6.3 When Performance Management services stop 589
  - 12.6.4 When the startup of Performance Management services fails 589
  - 12.6.5 When events for operation occur 590
  - 12.6.6 When agent statuses are changed 591
  - 12.6.7 When the health check status changes 592
  - 12.6.8 When monitoring is suspended with a host specified 593
  - 12.6.9 When monitoring is suspended with an agent specified 594
  - 12.6.10 When monitoring is resumed with a host specified 595
  - 12.6.11 When monitoring is resumed with an agent specified 596

## **13 Performance Monitoring Linked with JP1/Service Level Management (JP1/SLM) 597**

- 13.1 Overview of monitoring linked with JP1/Service Level Management (JP1/SLM) 598
  - 13.1.1 Benefits of linking Performance Management with JP1/SLM 599
- 13.2 Prerequisites for JP1/SLM linkage 600
  - 13.2.1 Programs needed for JP1/SLM linkage 600
  - 13.2.2 Number of linked JP1/SLM instances 600
  - 13.2.3 User authentication mode and business groups for JP1/SLM linkage 601
  - 13.2.4 JP1 user authority for JP1/SLM linkage 601
  - 13.2.5 Recording performance data collected when linked with JP1/SLM 601
  - 13.2.6 Network settings for JP1/SLM linkage 602
  - 13.2.7 Monitoring items for JP1/SLM linkage 603
- 13.3 Building a system linked with JP1/SLM 605
  - 13.3.1 Setup for JP1/SLM linkage 605

- 13.3.2 Releasing linkage with JP1/SLM 606
- 13.3.3 Procedures for releasing linkage with JP1/SLM 607
- 13.4 Changing the configuration after linking with JP1/SLM 610
  - 13.4.1 Changing host names after linking with JP1/SLM 610
  - 13.4.2 Creating or deleting a PFM - Manager logical host after linking with JP1/SLM 611
  - 13.4.3 Applying configuration changes in Performance Management after linking with JP1/SLM 612
- 13.5 Operations when linking with JP1/SLM 613
  - 13.5.1 Starting monitoring from JP1/SLM 613
  - 13.5.2 Stopping monitoring from JP1/SLM 613
  - 13.5.3 Monitoring performance data in JP1/SLM 613
  - 13.5.4 Starting PFM - Web Console from JP1/SLM 613
  - 13.5.5 Synchronizing monitoring settings after backing up and restoring PFM - Manager or JP1/SLM 614

## **14 Monitoring Linked with JP1/AJS3 615**

- 14.1 Overview of monitoring linked with JP1/AJS3 616
  - 14.1.1 Benefits of linking Performance Management with JP1/AJS3 617
- 14.2 Prerequisites for linking with JP1/AJS3 618
- 14.3 Building a system linked with JP1/AJS3 620
  - 14.3.1 Setup for linking with JP1/AJS3 620
  - 14.3.2 Releasing linkage with JP1/AJS3 621
- 14.4 Changing the configuration after linking with JP1/AJS3 622
  - 14.4.1 Changing a host name after linking with JP1/AJS3 622
  - 14.4.2 Changing an IP address after linking with JP1/AJS3 622
- 14.5 Operations when linking with JP1/AJS3 623
  - 14.5.1 Displaying Performance Management reports from the monitor window of JP1/AJS3 - Web Console 623
- 14.6 Notes on linking with JP1/AJS3 624

## **15 Monitoring Linked with the IT Service Management Product (JP1/Service Support) 625**

- 15.1 Overview of monitoring linked with JP1/SS 626
  - 15.1.1 Benefits of linking Performance Management with JP1/SS 626
- 15.2 Prerequisites for linking with JP1/SS 627
- 15.3 Building a system linked with JP1/SS 629
  - 15.3.1 Setup for linking with JP1/SS 629
  - 15.3.2 Releasing linkage with JP1/SS 631
- 15.4 Changing the configuration after linking with JP1/SS 632
  - 15.4.1 Changing a host name after linking with JP1/SS 632
  - 15.4.2 Changing an IP address after linking with JP1/SS 632
- 15.5 Link with JP1/SS in a multiple-monitoring environment 633
- 15.6 Operations when Performance Management linking with JP1/SS 634
  - 15.6.1 Entering information for Item elements 634

- 15.6.2 Viewing Performance Management reports from the JP1/SS interface 634
- 15.7 Notes on linking with JP1/SS 635

## Part 3: Troubleshooting

### 16 Detecting Problems Within Performance Management 636

- 16.1 Overview of detecting problems within Performance Management 637
- 16.2 Using the health check function to check the operating status of monitoring agents and their hosts 640
  - 16.2.1 Configuring the health check function 640
  - 16.2.2 Checking operating statuses 646
  - 16.2.3 Examples of using the health check function 652
  - 16.2.4 Notes on the health check function 655
- 16.3 Using the status management function to check service status 663
  - 16.3.1 Configuring the status management function 664
  - 16.3.2 How to check the service status 665
  - 16.3.3 Status management during cluster system operation 667
  - 16.3.4 When a problem occurs within the status management function 668
- 16.4 Using the PFM service automatic restart functionality to restart PFM services 670
  - 16.4.1 Prerequisites for using the PFM service automatic restart functionality 670
  - 16.4.2 Service startup unit for the PFM service automatic restart functionality 671
  - 16.4.3 Configuring the PFM service automatic restart functionality 671
  - 16.4.4 Using the PFM service automatic restart functionality 674
- 16.5 Detecting problems by linking with the integrated system monitoring product 676
  - 16.5.1 Configuring the output method of the common message log 676
  - 16.5.2 Example of creating a definition file for the JP1/Base log file trapping function 677
  - 16.5.3 Starting the JP1/Base log file trapping function 678

### 17 Error Handling Procedures 679

- 17.1 Error handling procedures 680
- 17.2 Troubleshooting 681
  - 17.2.1 Troubleshooting problems related to setup and service startup 683
  - 17.2.2 Recovery method when the KAVE00493-E message is output and services cannot start 690
  - 17.2.3 Troubleshooting problems related to connecting to agents 696
  - 17.2.4 Troubleshooting problems related to logging on to PFM - Web Console 697
  - 17.2.5 Troubleshooting problems related to executing commands 699
  - 17.2.6 Troubleshooting problems related to agent management 700
  - 17.2.7 Troubleshooting problems related to report definition 702
  - 17.2.8 Troubleshooting problems related to alarm definition 704
  - 17.2.9 Troubleshooting problems related to collecting and managing performance data 707
  - 17.2.10 Troubleshooting problems related to the monitoring suspension function 713
  - 17.2.11 Troubleshooting problems related to linking with other programs 714
  - 17.2.12 Troubleshooting other problems 717

17.3	Troubleshooting for multiple monitoring	718
17.3.1	When the jpctool config mgrimport command is executed, an error is output	718
17.3.2	The host name is not distributed to agents when the jpccconf primmgr notify command is executed	718
17.3.3	The host name is not distributed to the primary Manager when the jpccconf primmgr notify command is executed	719
17.3.4	A connection from PFM - Web Console to PFM - Manager cannot be established	721
17.3.5	No agent is displayed on the secondary Manager	721
17.3.6	Troubleshooting related to events	722
17.3.7	A connection from the time the JP1/IM's Event Console starts monitoring to PFM - Web Console cannot be established	723
17.3.8	PFM-related settings cannot be specified from JP1/SLM	724
17.4	Log information to be output when Performance Management is used	725
17.4.1	Type of log information	725
17.4.2	Details on log information	726
17.5	Data to be collected in the event of trouble	735
17.5.1	Data to be collected in the event of trouble (in Windows)	735
17.5.2	Data to be collected in the event of trouble (in UNIX)	742
17.6	Procedures for collecting data in the event of trouble	749
17.6.1	Collecting data if a problem occurs in Windows (except for PFM - Web Console)	749
17.6.2	Collecting data if a problem occurs in UNIX (except for PFM - Web Console)	752
17.6.3	Collecting data if a problem occurs (in PFM - Web Console)	754
17.7	Restoring the Performance Management system	755
17.7.1	Procedures for recovering from serious failures such as disk failures	755

## Appendixes 758

A	Version Changes	759
A.1	Changes in 11-50	759
A.2	Changes in 11-10	759
A.3	Changes in 11-01	759
A.4	Changes in 11-00	759
A.5	Changes in 10-50	762
A.6	Changes in 10-10	763
A.7	Changes in 10-00	763
A.8	Changes in 09-50	766
A.9	Changes in 09-10	767
A.10	Changes in 09-00	768
B	Reference Material for This Manual	772
C	Glossary	773

## Index 774

# 1

## Starting and Stopping Performance Management

This chapter describes necessary operations of Performance Management, including how to start and stop services of the Performance Management program, how to operate the service information, and how to log on to and off from the Web browser.

# 1.1 Start and stop sequence for the entire Performance Management system

---

This section describes the sequence in which the services of the Performance Management system start and stop, and provides cautionary notes about this sequence.

The sequence for starting and stopping Performance Management in a cluster system is different from a non-cluster system. For details, see sections that describe the setup of each Performance Management program in *10. Cluster System Configuration and Operation*.

## 1.1.1 Start sequence for the entire Performance Management system

The Performance Management system must be started in the order of monitoring manager, monitoring agent, and monitoring console server.

1. Start PFM - Manager by executing the `jpcspm start` command on the monitoring manager.
2. Execute the `jpcspm start` command on each monitoring agent to start PFM - Base and PFM - Agent, or PFM - Base and PFM - RM.
3. Start PFM - Web Console by executing the `jpcwstart` command on the monitoring console server.

The `jpcspm start` command and the `jpcwstart` command start the services for each Performance Management program in sequence. Service dependencies are pre-set in Windows, which means that you do not need to be concerned with the start sequence.

If PFM - Manager or PFM - Base is installed on the same host as PFM - Web Console, their start processes can be linked. For details on how to link start processes, see *1.4 Synchronizing the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console*.

Reference note:

If PFM - Agent or PFM - RM is installed on the same host as PFM - Manager, start the PFM - Manager services first, and then start the PFM - Agent or PFM - RM services.

Notes:

- When you install version 08-00 or later of a Performance Management program, the setting for the status management function is as follows:
    - After a new installation of version 08-00 or later of PFM - Manager or PFM - Base on a host that does not already have a Performance Management program installed:  
Status management function setting: Enabled
    - Other cases<sup>#</sup>:  
Status management function setting: Remains the same
- <sup>#</sup> The following fall under the other cases category:
- Upgrading version 06-70 to 07-10 of PFM - Manager to version 08-00 or later
  - Performing a new installation of version 08-00 or later of PFM - Manager or PFM - Base in an environment where version 06-70 to 07-00 of PFM - Agent is installed

The setting is disabled because Performance Management versions 06-70 to 07-10 do not have the status management function.

For the procedure to change the settings of the status management function, see [16.3.1 Configuring the status management function](#).

- If the Agent Collector or Remote Monitor Collector service fails to start, stop the PFM - Agent or PFM - RM services, and check the common message log to identify the cause of the start failure. Restart the PFM - Agent or PFM - RM services after solving the cause of the Agent Collector or Remote Monitor Collector start failure.
- You can use the health check function with PFM - Manager 08-11 or later. On a host where PFM - Manager version 09-00 or later is installed, the settings of the health check function are as follows:
  - When performing a new installation of PFM - Manager version 09-00 or later in an environment that does not already have PFM - Manager installed:  
Health check function settings: Enabled
  - Other cases<sup>#</sup>:  
Health check function settings: Remains the same

#: The following fall under the other cases category:

- Upgrading version 06-70 to 08-00 of PFM - Manager to version 08-11 or later
- Performing a new installation of version 08-11 or later of PFM - Manager in an environment where version 06-70 to 07-00 of PFM - Agent is installed

Because 06-70 to 08-00 versions of PFM - Manager do not have the health check function, the setting status in this case becomes *invalid*. For details on configuring the health check function, see [16.2.1 Configuring the health check function](#).

## 1.1.2 Stop sequence for the entire Performance Management system

The Performance Management system components must be stopped in the following order the monitoring console server, all monitoring agents, and then the monitoring manager.

1. Stop PFM - Web Console by executing the `jpcwstop` command on the monitoring console server.
2. Execute the `jpcspm stop` command on each monitoring agent to stop PFM - Base and PFM - Agent, or PFM - Base and PFM - RM.
3. Stop PFM - Manager by executing the `jpcspm stop` command on the monitoring manager.

The `jpcspm stop` command and the `jpcwstop` command stop the services for each Performance Management program in sequence. Service dependencies are pre-set in Windows, which means that you do not need to be concerned with the stop sequence.

If PFM - Manager or PFM - Base is installed on the same host as PFM - Web Console, their stops can be linked. For details on how to link stop processes, see [1.4 Synchronizing the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console](#).

Reference note:

If PFM - Manager or PFM - Base is installed on the same host as PFM - Web Console, stop the PFM - Agent or PFM - RM services first, and then stop the PFM - Manager services.



 **Tip**

Take the starting sequence of the entire Performance Management system into consideration when restarting the program automatically. For large-scale systems, PFM - Agent or PFM - RM can be started in stand-alone mode to control the starting sequence of the Performance Management system. For details on the stand-alone mode, see *1.8.1 When starting PFM - Agent or PFM - RM in a large-scale system*.

## 1.2 Starting services

---

This section describes how to start each service of the Performance Management program.

You must have the following OS user permissions to start the services:

- In Windows: Administrators permissions
- In UNIX: root user permissions

### 1.2.1 Starting services on monitoring managers and monitoring agents

#### (1) Manually starting services on monitoring managers and monitoring agents

Use the `jpcspm start` command to manually start services on the monitoring manager or the monitoring agent.

You can use the `jpcspm start` command to start services only on the host to which you have logged on. You cannot start the Performance Management program services on a remote host. When the health check function is enabled, the health check agent starts when PFM - Manager starts.

1. Log on to the host where you want to start services.

Log on to the monitoring manager to start the PFM - Manager services. Log on to the monitoring agent to start the services of PFM-Base and either PFM - Agent or PFM - RM.

2. Execute the `jpcspm start` command.

Specify the service key indicating the service that you want to start, and execute the `jpcspm start` command. Service keys that the `jpcspm start` command can specify are as follows:

- `Manager` or `mgr`: PFM - Manager services on the host
- `AH` or `act`: Action Handler services on the host

For details on the service keys used to start specific PFM - Agent or PFM - RM services on the host, see the appendix describing service naming rules in the manual *JPI/Performance Management Planning and Configuration Guide*. For example, to start all of the PFM - Manager, PFM - Base, PFM - Agent, and PFM - RM services on the local host, specify as follows:

```
jpcspm start -key jplpc
```

Specify the instance name to start, separately instance by instance, a PFM - Agent or PFM - RM that runs in the instance environment.

For example, to start the service that has the instance name `oracleA` in the PFM - Agent for Oracle, specify as follows:

```
jpcspm start -key Oracle -inst oracleA
```

#### (2) Enabling or disabling the automatic service start feature for monitoring managers and monitoring agents (Windows)

With the default installation settings, most services start automatically when the system starts. Note that, however, some services of PFM - Agent for Service Response cannot be set to start automatically. For details, see the chapter that

describes starting and stopping services in the manual *JPI/Performance Management - Agent Option for Service Response*.

If automatic startup processing is affected by high load and times out when the system starts, the Performance Management services might fail to start. In this case, block automatic startup and execute the `jpcspm start` command to start the services.

To disable and enable the automatic start feature:

1. Log on to the monitoring manager or monitoring agent.
2. Choose **Services** in Windows.
3. In the Services dialog box, choose the Performance Management program service and click **Properties** from the pull-down menu.
4. In the service properties dialog box, specify **Startup type**.  
To block automatic startup: **Manual**  
To reset automatic startup: **Automatic**
5. Click the **OK** button.
6. The service properties dialog box closes.
7. For details about Performance Management program services, see the explanation of the correspondence between the Performance Management service name and the Windows service name in the Appendix in the *JPI/Performance Management Planning and Configuration Guide*.

### Important

Performance Management services are usually controlled from a system account. Changing the settings might cause service operation errors.

Do not modify the account settings of a service unless recommended to do so by this manual.

All the PFM - Base, PFM - Manager, and PFM - Web Console services are operated by using a system account.

For details on PFM - Agent or PFM - RM, see the respective PFM - Agent or PFM - RM manual.

## **(3) Enabling or disabling the automatic service start feature for monitoring managers and monitoring agents (UNIX)**

With the default installation settings, services are not set to start automatically when the system starts.

To set services other than PFM - Web Console to start automatically at system startup, store in the installation folder for Performance Management the script file for starting services automatically (`jpc_start`). To disable the automatic service start feature, delete the `jpc_start` file.

Supplemental information:

- By using this script file, you can start services on the physical host only. You cannot start services on the logical host.
- In the default settings of the script file for starting services automatically (`jpc_start`), all the PFM services on the physical host are set to start. Therefore, if an instance is not created in a physical environment that has an agent

that creates an instance, the KAVE06017-W message is output. If you want only specific services to start automatically, edit the following line in the script file:

Before:

```
nohup /opt/jplpc/tools/jpcstart all -nochk 2> /dev/null 1> /dev/null &
```

After:

```
nohup /opt/jplpc/tools/jpcstart act -nochk 2> /dev/null 1> /dev/null
nohup /opt/jplpc/tools/jpcstart <service-key> -nochk 2> /dev/null 1> /dev/
null &
```

Note: Include the first line only if you need to start the Action Handler service. Do not place an ampersand (&) at the end of the first line. In <service-key> in line 2, specify the service key of the service that you want to start automatically.

- For the PFM - Manager service to start automatically, make the following change in the script file for starting services automatically (jpc\_start).

Before:

```
nohup /opt/jplpc/tools/jpcstart all -nochk 2> /dev/null 1> /dev/null &
```

After:

```
nohup /opt/jplpc/tools/jpcstart mgr -nochk 2> /dev/null 1> /dev/null
nohup /opt/jplpc/tools/jpcstart act -nochk 2> /dev/null 1> /dev/null
nohup /opt/jplpc/tools/jpcstart <service-key> -nochk 2> /dev/null 1> /dev/
null &
```

Note: Do not place an ampersand (&) at the end of the first and second lines. In <service-key> in line 3, specify the service key of the service that you want to start automatically.

- To change the temporary file output destination directory, make the following change in the script file for starting services automatically (jpc\_start).

Before:

```
export PATH SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF
```

After:

```
JPC_TMPDIR=temporary-file-output-destination-directory
export PATH SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF JPC_TMPDIR
```

Note: For *temporary-file-output-destination-directory*, specify the path to a directory on the disk that has sufficient free space.

- At startup, Performance Management is subject to the LANG environment variable set in the environment where it operates. In an environment where the LC\_ALL environment variable is set to a different value from the LANG environment variable, either unset the LC\_ALL environment variable or change its value to match the LANG environment variable. Use the following example as a reference for editing the script file for starting services automatically (jpc\_start) to set the LANG environment variable for Performance Management:

Example settings:

```
## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jplpc/bin
SHLIB_PATH=/opt/hitachi/common/lib
LD_LIBRARY_PATH=/opt/hitachi/common/lib
LIBPATH=/opt/hitachi/common/lib
HCCLIBCNF=/opt/jpl/hcclibcnf
LANG=LANG-environment-variable-to-set#1
```

```
export PATH SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF LANG#1
unset LC_ALL#2
```

#1: Line that is to be added to the script file for starting services automatically. For details on the LANG environment variable values you can use with Performance Management, see the chapters on installation and setup in the *JP1/Performance Management Planning and Configuration Guide* and the manuals for PFM - Agent or PFM - RM.

#2: An example of coding that unsets the LC\_ALL environment variable.

### Important

When the automatic service start and stop features are enabled in a CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12 environment and the `jpcspm start` command is used to start services, the services will not stop automatically when the OS shuts down. If you want the services to stop automatically, use the `systemctl` command to restart all Performance Management services. Alternatively, use the `jpcspm stop` command to manually stop the services that were started by the `jpcspm start` command.

The following example uses the `systemctl` command to restart the services:

```
> systemctl stop jpl_pc
> systemctl start jpl_pc
```

To set automatic start of services:

1. Log on to the host that you want to set for the automatic start of services.
2. Execute the following command to move to the `/opt/jplpc` directory:

```
cd /opt/jplpc
```

3. Set the script file for starting services automatically for the Performance Management system.

- Name of the `.model` file of the service automatic start script: `jpc_start.model`
- Name of the script file for starting services automatically: `jpc_start`

Copy the `.model` file of the service automatic start script to the script file for starting services automatically to add execution permission. Execute the command as follows:

```
cp -p jpc_start.model jpc_start
chmod 555 jpc_start
```

4. Register the automatic start script file for AIX (in AIX only).

To execute the automatic service start script file for the Performance Management system specified in step 3, Performance Management provides the automatic start script file for AIX. Register this automatic start script file to the AIX settings file.

- Name of the automatic start script file: `/etc/rc.jpl_pc`
- Name of the settings file: `/etc/inittab`

1. Use the `mkitab` command to register the `/etc/rc.jpl_pc` file to the `/etc/inittab` settings file.

```
mkitab "jplpc:2:wait:/etc/rc.jpl_pc >/dev/console 2>&1"
```

2. Use the `lsitab` command to confirm that the `/etc/rc.jp1_pc` file is registered to the `/etc/inittab` settings file.

```
lsitab jp1pc
jp1pc:2:wait:/etc/rc.jp1_pc >/dev/console 2>&1
```

Registering the file by the `mkitab` command places the file to the bottommost line of the `/etc/inittab` settings file. If a program linked by execution of an action is already registered in the `/etc/inittab` settings file, edit the `/etc/inittab` settings file so that the reference to the automatic start script file appears below it in the file. Also, the line registered in the `/etc/inittab` settings file is not deleted upon uninstallation.

To cancel the registration at uninstallation:

1. Use the `rmitab` command to cancel the registration of the `/etc/rc.jp1_pc` file from the `/etc/inittab` settings file.

```
rmitab jp1pc
```

2. Use the `lsitab` command to confirm that the `/etc/rc.jp1_pc` file is not registered to the `/etc/inittab` settings file.

```
lsitab jp1pc
```

5. Register the Performance Management services into the OS (in CentOS 7, Linux 7, Oracle Linux 7, and SUSE Linux 12 only).

The registration procedure is as follows:

1. Edit the service automatic start script (`/etc/init.d/jp1_pc`).

Before editing:

```
#!/bin/sh
## Copyright (C) 2004, 2016, Hitachi, Ltd.
## Copyright (C) 2016, Hitachi Solutions, Ltd.
## Licensed Material of Hitachi, Ltd.
:
```

After editing:

```
#!/bin/sh
## Copyright (C) 2004, 2016, Hitachi, Ltd.
## Copyright (C) 2016, Hitachi Solutions, Ltd.
## Licensed Material of Hitachi, Ltd.
### BEGIN INIT INFO
# Provides: jp1_pc
# Required-Start: $local_fs $remote_fs $syslog $network
# Required-Stop: $local_fs $remote_fs $syslog $network
# Default-Start: 3 5
# Default-Stop: 0 6
# Description: Start PFM services.
### END INIT INFO
:
```

2. Execute the following command:

```
chkconfig jp1_pc on
```

To disable automatic start of services, perform the procedure below.

## Important

In CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12, also disable the automatic service stop feature when you disable the automatic service start feature. For details, see [1.3.1\(3\) Enabling or disabling the automatic service stop feature for monitoring managers and monitoring agents \(UNIX\)](#).

1. Delete the `jpc_start` file that was stored when the automatic service start feature was set.
2. Execute the following command to delete the Performance Management services that are registered in the OS (in CentOS 7, Linux 7, Oracle Linux 7, and SUSE Linux 12 only):

```
chkconfig jpl_pc off
```

## 1.2.2 Starting services on the monitoring console server

This subsection describes how to start the PFM - Web Console services on the monitoring console server.

Check that the PFM - Manager services that you want to connect PFM - Web Console are operating before starting the PFM - Web Console services.

### (1) Manually starting services on the monitoring console server

The following two methods can be used to start the PFM - Web Console services on the monitoring console server. Note that the instructions for starting services from the Control Panel apply only to Windows systems.

- Starting by using a command
- Starting from the Control Panel (Windows only)

#### (a) Starting services using a command

Use the `jpcwstart` command to start services. With the `jpcwstart` command, you can start the services only on the host to which you have logged on. You cannot start the services of the Performance Management programs on the remote host.

1. Log on to the monitoring console server (the host that has PFM - Web Console installed).
2. Open the Administrator Console.
3. Execute the `jpcwstart` command.  
Execute the command to start the PFM - Web Service and PFM - Web Console services.

#### (b) Starting services from the Control Panel

1. Log on to the monitoring console server (the host that has PFM - Web Console installed).
2. Choose **Services** in Windows.
3. In the Services dialog box, right-click the **PFM - Web Service** service, and from the pulldown menu choose **Start**. The **PFM - Web Console** service also starts. If the **PFM - Web Console** service does not start, right-click the **PFM - Web Console** service, and from the pulldown menu, choose **Start**.

## (2) Enabling or disabling the automatic service start feature for the monitoring console server (Windows)

With the default installation settings, the PFM - Web Console services are set to start automatically when the system starts. For this reason, no operation is necessary after starting the system.

To disable and enable the automatic start feature:

1. Log on to the monitoring console server (the host that has PFM - Web Console installed).
2. Choose **Services** in Windows.
3. In the Services dialog box, select the **PFM - Web Console** service, and from the pulldown menu choose **Properties**.
4. In the Properties dialog box for the PFM - Web Console service, set **Startup type**.  
To cancel the automatic start, select **Manual**.  
To reset the automatic start, select **Automatic**.
5. Click the **OK** button.  
The Properties dialog box of the PFM - Web Console service is closed.
6. Choose the **PFM - Web Service** service, and from the pulldown menu choose **Properties**.
7. In the Properties dialog box for the PFM - Web Service, set **Startup type**.  
To cancel the automatic start, select **Manual**.  
To reset the automatic start, select **Automatic**.
8. Click the **OK** button.

### Important

- Make sure that the startup types of the PFM - Web Console services and the PFM - Web Service services are the same.
- Do not change the settings of the service account. Changing the settings might cause service operation errors.

## (3) Enabling or disabling the automatic service start feature for the monitoring console server (UNIX)

With the default installation settings, services are not set to start automatically when the system starts.

To set start services to start automatically at system startup, store in the installation folder for PFM - Web Console the script file for starting services automatically (`jpcw_start`). To disable the automatic service start feature, delete the `jpcw_start` file.

Note:

At startup, Performance Management is subject to the `LANG` environment variable set in the environment where it operates. Use the following example as a reference for editing the script file for starting services automatically (`jpcw_start`) to set the `LANG` environment variable for Performance Management.

Example settings:

```
LANG=LANG-environment-variable-to-set#  
export LANG#  
nohup /opt/jp1pcwebcon/tools/jpcwstart
```



#: A line to be added to the script file.

For details on the LANG environment variable values you can use with Performance Management, see the chapters on installation and setup in the *JP1/Performance Management Planning and Configuration Guide* and the manuals for PFM - Agent or PFM - RM.

### Important

When the automatic service start and stop features are enabled in a CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12 environment and the `jpcwstart` command is used to start services, the services will not stop automatically when the OS shuts down. If you want the services to stop automatically, use the `systemctl` command to restart all Performance Management services. Alternatively, use the `jpcwstop` command to manually stop the services that were started by the `jpcwstart` command.

The following example uses the `systemctl` command to restart the services:

```
> systemctl stop jpl_webcon
> systemctl start jpl_webcon
```

To set automatic start of services:

1. Log on to the host where you want to start services automatically.
2. Execute the following command to move to the `/opt/jplpcwebcon` directory:

```
cd /opt/jplpcwebcon
```

3. Set the script file for starting services automatically for PFM - Web Console.
  - Name of the `.model` file of the service automatic start script: `jpcw_start.model`
  - Name of the script file for starting services automatically: `jpcw_start`

Copy the `.model` file of the service automatic start script as the script file for starting services automatically, and add execution permission. Execute the commands as follows:

```
cp -p jpcw_start.model jpcw_start
chmod 555 jpcw_start
```

4. Register the automatic start script file for AIX (in AIX only).

To execute the automatic service start script file for PFM - Web Console specified in step 3, PFM - Web Console provides the automatic start script file for AIX. Register this automatic start script file into the AIX settings file.

- Name of the automatic start script file: `/etc/rc.jpl_webcon`
- Name of the settings file: `/etc/inittab`

1. Use the `mkitab` command to register the `/etc/rc.jpl_webcon` file into the `/etc/inittab` settings file.

```
mkitab "jplpcwebcon:2:wait:/etc/rc.jpl_webcon >/dev/console 2>&1"
```

2. Use the `lsitab` command to confirm that the `/etc/rc.jpl_webcon` file is registered in the `/etc/inittab` settings file.

```
lsitab jplpcwebcon
jplpcwebcon:2:wait:/etc/rc.jpl_webcon >/dev/console 2>&1
```

Registering the file with the `mkitab` command places the file as the bottommost line of the `/etc/inittab` settings file. If a program linked by execution of an action is already registered in the `/etc/inittab` settings file, edit the `/etc/inittab` settings file so that the reference to the automatic start script file appears below it in the file.

Also, the line added to the `/etc/inittab` settings file is not deleted upon uninstallation.

To cancel the registration during uninstallation:

1. Use the `rmitab` command to cancel the registration of the `/etc/rc.jp1_webcon` file from the `/etc/inittab` settings file.

```
rmitab jp1pcwebcon
```

2. Use the `lsitab` command to confirm that the `/etc/rc.jp1_webcon` file is not registered in the `/etc/inittab` settings file.

```
lsitab jp1pcwebcon
```

5. Register the Performance Management services into the OS (in CentOS 7, Linux 7, Oracle Linux 7, and SUSE Linux 12 only).

The registration procedure is as follows:

1. Edit the service automatic start script (`/etc/init.d/jp1_webcon`).

Before editing:

```
#!/bin/sh
#
# Title       : jp1_webcon
# Explain    : This is a jp1_webcon file.
# Copyright  : All Rights Reserved. Copyright (C) 2011, Hitachi, Ltd.
# Note       :
# Version    : 09-50
:
```

After editing:

```
#!/bin/sh
#
# Title       : jp1_webcon
# Explain    : This is a jp1_webcon file.
# Copyright  : All Rights Reserved. Copyright (C) 2011, Hitachi, Ltd.
# Note       :
# Version    : 09-50
### BEGIN INIT INFO
# Provides: jp1_webcon
# Required-Start: $local_fs $remote_fs $syslog $network
# Required-Stop: $local_fs $remote_fs $syslog $network
# Default-Start: 3 5
# Default-Stop: 0 6
# Description: Start PFM services.
### END INIT INFO
:
```

2. Execute the following command:

```
chkconfig jp1_webcon on
```

To disable automatic start of services, perform the procedure below.

## Important

In CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12, also disable the automatic service stop feature when you disable the automatic service start feature. For details, see [1.3.2\(3\) Enabling or disabling the automatic service stop feature for the monitoring console server \(UNIX\)](#).

1. Delete the `jpcw_start` file that was stored when the automatic service start feature was set.
2. Execute the following command to delete the Performance Management services that are registered in the OS (in CentOS 7, Linux 7, Oracle Linux 7, and SUSE Linux 12 only):

```
chkconfig jpl_webcon off
```

## 1.3 Stopping services

---

This section describes how to stop Performance Management program services.

You must have the following OS user permissions to stop the services:

- In Windows: Administrators permissions
- In UNIX: Root user permissions

### 1.3.1 Stopping services on monitoring managers and monitoring agents

#### (1) Manually stopping services on monitoring managers and monitoring agents

##### (a) Stopping services by using a command

Use the `jpccspm stop` command to manually stop monitoring manager or the monitoring agent services. With the `jpccspm stop` command, you can stop the services only on the host to which you have logged on. You cannot stop the Performance Management program services on a remote host. When the health check function is enabled, the health check agent stops when PFM - Manager stops.

Use the `jpctool service list` command to check the status of services on the host before stopping services manually.

1. Log on to the host for which you want to stop services.

Log on to the monitoring manager to stop PFM - Manager services. Log on to the monitoring agent to stop the services of PFM-Base and either PFM - Agent or PFM - RM.

2. Execute the `jpctool service list` command.

Execute the `jpctool service list` command to check the status of the services.

For example, specify as follows to check the status of all service operations throughout the entire Performance Management system operating on the local host:

```
jpctool service list -key all
```

For details about the information that you can display by executing the `jpctool service list` command, see [1.6.1 Checking the status of services by using a command](#).

3. Execute the `jpccspm stop` command.

Specify the service key indicating the service you want to stop, and execute the `jpccspm stop` command. Service keys that the `jpccspm stop` command can specify are as follows:

- `jp1pc`: All of the PFM - Manager, PFM - Base, PFM - Agent, and PFM - RM services on the host
- `Manager` or `mgr`: PFM - Manager services on the host
- `AH` or `act`: Action Handler services on the host

For details on the service keys to stop a specific PFM - Agent or PFM - RM service on the host, see the sections that describe the naming rules for services in an appendix of the manual *JPI/Performance Management Planning and Configuration Guide*.

For example, to start all of the PFM - Manager, PFM - Base, PFM - Agent, and PFM - RM services on the local host, specify as follows:

```
jpcspm stop -key jplpc
```

Specify the instance name to stop, separately instance by instance, a PFM - Agent or PFM - RM that runs in the instance environment.

For example, to stop the service that has the instance name `oracleA` in the PFM - Agent for Oracle, specify as follows:

```
jpcspm stop -key Oracle -inst oracleA
```

Reference note:

If you want to stop a specific service of the Performance Management program, first refer to the `Host Name`, `ServiceID`, and `Service Name` that are output by the `jpctool service list` command. From these, you can determine which service indicated below is operating on the local machine and specify an appropriate service key.

- PFM - Manager service
- PFM - Agent or PFM - RM service

## (b) Stopping services from the Web browser

Note:

Administrator user permissions are necessary to stop services from the Web browser.

1. From the monitoring console Web browser, log on to PFM - Web Console.  
Log on to a user account that has administrator user permissions.

2. In the navigation frame of the main window, choose the **Services** tab.

3. In the navigation frame of the Services window, choose the service to be stopped.

The navigation frame displays the following two folders under the root **System**:

### **Machines** folder

This folder contains folders with the same names as the hosts where the Performance Management services are installed. The **Machines** folder manages the PFM - Agent or PFM - RM services for each host.

### **PFM-Manager** folder

This folder manages the PFM - Manager services.

The selected service is marked with a checkmark.

4. In the method frame of the Services window, choose the **Stop service** method.

5. In the confirmation message box that appears, click **OK**.

The selected service stops.

When the service stops successfully, the status message `The service stopped.` appears in the information frame of the Services window.

Note:

You cannot start services from the Web browser. To restart the services that you stopped, execute the `jpcspm start` command on the host that has the relevant services installed.

## (2) Enabling or disabling the automatic service stop feature for monitoring managers and monitoring agents (Windows)

PFM services stop automatically when the system is stopped. However, in this case, the system might be stopped even though PFM services stop abnormally and it might cause file corruption. Therefore, we recommend that you stop PFM services before the system is stopped by using the `jpcspm stop` command.

## (3) Enabling or disabling the automatic service stop feature for monitoring managers and monitoring agents (UNIX)

With the default installation settings, services are not set to stop automatically when the system shuts down.

To set services other than PFM - Web Console to stop automatically at system shutdown, store in the installation folder for the Performance Management system the script file for stopping services automatically (`jpc_stop`). To disable the automatic service stop feature, delete the `jpc_stop` file.

The procedure for enabling the automatic service stop feature is described below.

### Important

- When you enable the automatic service stop feature in CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12, you must also enable the automatic start feature. For details, see [1.2.1\(3\) Enabling or disabling the automatic service start feature for monitoring managers and monitoring agents \(UNIX\)](#).
- When the automatic service start and stop features are enabled in a CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12 environment and the `jpcspm start` command is used to start services, the services will not stop automatically when the OS shuts down. If you want the services to stop automatically, use the `systemctl` command to restart all Performance Management services. Alternatively, use the `jpcspm stop` command to manually stop the services that were started by the `jpcspm start` command.

The following example uses the `systemctl` command to restart the services:

```
> systemctl stop jpl_pc
> systemctl start jpl_pc
```

1. Log on to the host on which the automatic service stop feature is to be enabled.

2. Execute the following command to move to the `/opt/jplpc` directory:

```
cd /opt/jplpc
```

3. Set the script file for stopping services automatically for the Performance Management system.

- Name of the `.model` file of the service automatic stop script: `jpc_stop.model`
- Name of the script file for stopping services automatically: `jpc_stop`

Copy the `.model` file of the service automatic stop script to the script file for stopping services automatically to add execution permission. Execute the command as follows:

```
cp -p jpc_stop.model jpc_stop
chmod 555 jpc_stop
```

4. Specify the automatic stop script file for AIX. (For AIX only)

Register the script file for stopping services automatically for the Performance Management system set in step 3 into the automatic stop script file for AIX.

- Name of the automatic stop script file: `/etc/rc.shutdown`

Add the following lines to the automatic stop script file. You do not need to take the sequence into consideration when stopping services.

```
if [ -x /opt/jplpc/jpc_stop ]; then
    /opt/jplpc/jpc_stop
fi
```

Create a new file if there is no `/etc/rc.shutdown` file. After that, set the attributes of the file as follows:

```
chmod 550 /etc/rc.shutdown
chown root /etc/rc.shutdown
chgrp shutdown /etc/rc.shutdown
```

The added lines and the `/etc/rc.shutdown` file are not deleted upon uninstallation. Delete the added lines, if necessary, when performing uninstallation.

5. To apply the settings, execute the following command to start the Performance Management services other than PFM - Web Console (in CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12 only):

```
systemctl start jpl_pc
```

If you do not execute this command, automatic stop processing will fail for the first service that is run after the settings were specified.

## 1.3.2 Stopping services on the monitoring console server

### (1) Manually stopping services on the monitoring console server

#### (a) Stopping services using a command

Use the `jpcwstop` command to stop services. You can use this command to stop the services only on the host to which you have logged on. You cannot stop the Performance Management program services on the remote host.

To stop services by using a command:

1. Log on to the monitoring console server (the host that has PFM - Web Console installed).
2. Open the Administrator Console.
3. Execute the `jpcwstop` command.

The `jpcwstop` command is stored in the following folder:

- In Windows:  
`PFM-Web-Console-installation-folder\tools\`
- In UNIX:  
`/opt/jplpcwebcon/tools/`

Execute the command to stop the PFM - Web Service and PFM - Web Console services.

## (b) Stopping services from the Control Panel

1. Choose **Services** in Windows.
2. In the Services dialog box, right-click the **PFM - Web Service**, and from the pulldown menu choose **Stop**.
3. Right-click the **PFM - Web Console** service, and from the pulldown menu choose **Stop**.

## (2) Enabling or disabling the automatic stop feature for the monitoring console server (Windows)

No operation is necessary because services stop automatically when the system is stopped.

## (3) Enabling or disabling the automatic service stop feature for the monitoring console server (UNIX)

With the default installation settings, services are not set to stop automatically when the system shuts down.

To stop services automatically at system shutdown, store in the PFM - Web Console installation folder the script file for stopping services automatically (`jpcw_stop`) for PFM - Web Console. To disable the automatic service stop feature, delete the `jpcw_stop` file.

The procedure for enabling the automatic service stop feature is described below.

### Important

- When you enable the automatic service stop feature in CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12, you must also enable the automatic start feature. For details, see [1.2.2\(3\) Enabling or disabling the automatic service start feature for the monitoring console server \(UNIX\)](#).
- When the automatic service start and stop features are enabled in a CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12 environment and the `jpcwstart` command is used to start services, the services will not stop automatically when the OS shuts down. If you want the services to stop automatically, use the `systemctl` command to restart all Performance Management services. Alternatively, use the `jpcwstop` command to manually stop the services that were started by the `jpcwstart` command. The following example uses the `systemctl` command to restart the services:

```
> systemctl stop jpl_webcon  
> systemctl start jpl_webcon
```

1. Log on to the host where you want to stop services automatically.
2. Execute the following command to move to the `/opt/jplpcwebcon` directory:

```
cd /opt/jplpcwebcon
```

3. Set the script file for stopping services automatically for PFM - Web Console.
  - Name of the `.model` file of the service automatic stop script: `jpcw_stop.model`
  - Name of the script file for stopping services automatically: `jpcw_stop`

Copy the `.model` file of the service automatic stop script as the script file for stopping services automatically, and add execution permission. Execute the commands as follows:



```
cp -p jpcw_stop.model jpcw_stop
chmod 555 jpcw_stop
```

4. Register the automatic stop script file for AIX (in AIX only).

Register the script file for stopping services automatically for PFM - Web Console set in step 3 into the automatic stop script file for AIX.

- Name of the automatic stop script file: `/etc/rc.shutdown`

Add the lines shown below to the automatic stop script file. You do not need to take the sequence into consideration when stopping services.

```
if [ -x /opt/jp1pcwebcon/jpcw_stop ]; then
    /opt/jp1pcwebcon/jpcw_stop
fi
```

Create a new file if there is no `/etc/rc.shutdown` file. After that, set the attributes of the file as follows:

```
chmod 550 /etc/rc.shutdown
chown root /etc/rc.shutdown
chgrp shutdown /etc/rc.shutdown
```

The added lines and the `/etc/rc.shutdown` file are not deleted upon uninstallation. Delete the added lines, if necessary, when performing uninstallation.

5. To apply the settings, execute the following command to start the PFM - Web Console service (in CentOS 7, Linux 7, Oracle Linux 7, or SUSE Linux 12 only):

```
systemctl start jp1_webcon
```

If you do not execute this command, automatic stop processing will fail for the first service that is run after the settings were specified.

## 1.4 Synchronizing the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console

If PFM - Manager or PFM - Base is installed on the same host as PFM - Web Console, you can synchronize the starting and stopping of these services. However, the version of each of the services must be 09-00 or later to do this.

### 1.4.1 Synchronizing starting and stopping

If you want to link start and stop processes by using the `jpcspm` command, you must modify the `pfmwebcon_host.conf` file.

1. Use a text editor to open the `pfmwebcon_host.conf` file.

The `pfmwebcon_host.conf` file is located in the following location:

- In Windows:  
`PFM-Web-Console-installation-folder\conf\`
- In UNIX:  
`/opt/jp1pcwebcon/conf/`

2. Edit the `pfmwebcon_host.conf` file and then save it.

The format of the `pfmwebcon_host.conf` file is as follows. Do not enter spaces before or after the equals sign (=).

```
# Operate Host
HOST_NAME=HOSTNAME
```

Table 1–1: Valid values of HOSTNAME

Value	Description
--	Specifies that starting and stopping are not to be synchronized.
localhost	Specifies that starting and stopping are to be synchronized in a non-cluster system environment. Use lower-case characters only.
Logical host name	Specifies that starting and stopping are to be synchronized in a cluster system. Specify the name of the logical host running PFM - Web Console. You cannot specify an IP address. The host name is case sensitive.

#### Legend

--: No value

### 1.4.2 Command options when synchronizing service starting and stopping

To synchronize the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console, use the `jpcspm` command in the same way as with no synchronization. The service keys to be specified for synchronizing the starting and stopping of the services are as follows:

- `all`: All services on the host, including PFM - Web Console.

- `WebConsole` or `wc`: The PFM - Web Console service on the host.

For example, to start all services on the local host, specify the following:

```
jpcspm start -key all
```

For details on starting or stopping services, see [1.2 Starting services](#) and [1.3 Stopping services](#).

## 1.5 Logging on to and off from PFM - Web Console

---

### 1.5.1 Logging on to PFM - Web Console

1. In the Web browser, enter the following URL:

```
http://name-of-host-on-which-PFM-Web-Console-is-installed:20358/  
PFMWebConsole/login.do
```

Change the URL for logging in as appropriate for the environment, as follows:

- When encrypted communication is enabled  
Change `http` to `https`.  
If a host name in FQDN format is specified as a common name in the certificate signing request file, change *name-of-host-on-which-PFM-Web-Console-is-installed* to *name-of-host-on-which-PFM-Web-Console-is-installed+domain-name*.
- If the port number has been changed  
Specify the new port number, not 20358.

Note

If you log on more than once from the same Web browser on the same monitoring console, the previously logged-in session might be invalidated. For details on controlling multiple logins, see the chapter describing the initialization file (`config.xml`) in the manual *JPI/Performance Management Reference*.

2. In the Login window, enter a **User name** and **Password**.

Enter a user name and password.

Reference note:

Use the following user account when logging on for the first time:

**User name:** ADMINISTRATOR

**Password:** None

For security reasons, configure a password for the ADMINISTRATOR account before starting to use Performance Management. See [2. Managing User Accounts and Business Groups](#).

3. Click the **Login** button.

Log on to PFM - Web Console. The main window appears.

Immediately after login, **User Agents** (*logged-on-user-name*) appears in the navigation frame in the root of the Agents tree. In the information frame, the summary that **User Agents** (*logged-on-user-name*) is being selected appears. For details on how to display the summary, see [3.4.5 Using summary display to check the operating status](#).

For details on the main window, see the chapter that describes the main window in the manual *JPI/Performance Management Reference*.

### 1.5.2 Logging off from PFM - Web Console

In the menu bar frame of the main window, click the **Logout** menu to log off from PFM - Web Console. In the displayed confirmation dialog box, click the **OK** button to log off. If you click the **Cancel** button, control is returned to the main window.

Note:

The View Report window, when displayed, might not close in conjunction with the closing of the main window. In the following cases, close each View Report window by using the **Close** button:

- When numerous View Report windows are displayed

Try to have no more than 10 windows displayed for history reports or for realtime reports that do not refresh automatically.

When you display multiple realtime reports that refresh automatically and their refresh processing occurs at the same time, the refresh processing cannot keep up even if 10 windows or less are open. This causes the processing time to exceed the automatic refresh request interval leading to the possible stoppage of automatic refresh.

- When closing the main window while displaying the View Report window and the reports by using automatic refresh (same for displaying the drilldown report)

## 1.6 Checking the status of services

This section describes how to check the status of services.

When PFM - Manager or PFM - Base is installed on the same host as PFM - Web Console, you can use the `jpctool service list` command to check the operating status of all the services at one time.

In other situations, you cannot check information of the PFM - Web Console services by using the `jpctool service list` command. Check the information of the PFM - Web Console services by using the Services dialog box, which is displayed by choosing **Services** in Windows.

### 1.6.1 Checking the status of services by using a command

Use the `jpctool service list` command to check the status of services throughout the entire Performance Management system or to check the service operations on a specific host.

If you edit the `pfmwebcon_host.conf` file beforehand, you can also use this command to check the status of just the PFM - Web Console service that is installed on the host where the `jpctool service list` command is executed. To do so, edit the `pfmwebcon_host.conf` file in the same way as for synchronized starting and stopping of the PFM - Manager or PFM - Base and PFM - Web Console services. For details on how to edit the `pfmwebcon_host.conf` file, see [1.4.1 Synchronizing starting and stopping](#).

1. Log on to the host that has PFM - Manager, PFM - Agent, or PFM - RM installed.
2. Specify the service ID of the service for which you want to display service information, and execute the `jpctool service list` command.

For example, to check the status of all services on the local host, specify as follows:

```
jpctool service list -key all
```

Table 1–2: Information that can be output by the `jpctool service list` command

Output information	Description
Host Name	Name of the host on which services are operating
ServiceID	Service ID
Service Name	Service name
PID	The process ID of the service. <ul style="list-style-type: none"><li>• When the status management function is enabled: The process ID appears only when the Status is Active, Busy, S Active, S Busy, Starting, or Stopping.</li><li>• When the status management function is disabled or your product version does not support the status management function: The process ID appears only when the Status is Active.</li></ul>
Port	The communication port number used by the service. <ul style="list-style-type: none"><li>• When the status management function is enabled: The port number appears only when the Status is Active, Busy, S Active, or S Busy.</li><li>• When the status management function is disabled or your product version does not support the status management function: The port number appears only when the Status is Active.</li></ul>

Output information	Description
Status	<p>The status of the service.</p> <p>When the status management function is enabled:</p> <ul style="list-style-type: none"> <li>• Status display in versions that support the status management function: <ul style="list-style-type: none"> <li>Active: The service is waiting for a request.</li> <li>Inactive: The service is stopped.</li> <li>Starting: The service is starting.</li> <li>Busy: The service is processing a request.</li> <li>S Active: The service is waiting for a request (stand-alone mode).</li> <li>S Busy: The service is processing a request (stand-alone mode).</li> <li>Stopping: The service is stopping.</li> </ul> </li> <li>• Status display in versions that do not support the status management function: <ul style="list-style-type: none"> <li>Active*: The service is running.</li> <li>Incomp*: The service is starting or stopping.</li> <li>Inactive*: Either the system cannot establish a connection to the service or the service is stopped.</li> <li>Comm Err*: The system is able to establish a connection to the service but there is no response.</li> <li>Timeout*: The connection to the service has timed out.</li> <li>Error*: An error other than a connection timeout has occurred. Refer to the common message log for details of the error. For details on PFM - Web Console service errors, see the trace log.</li> </ul> </li> </ul> <p>In the following situations, the above status display applies for services that support the status management function.</p> <ul style="list-style-type: none"> <li>- The Status Server service is stopped.</li> <li>- The Status Server has started but the status management function cannot recognize the status of the service<sup>#</sup>.</li> </ul> <p><sup>#</sup> You will need to restart the service for the status management function to recognize the service status correctly.</p> <p>When the status management function is disabled or your product version does not support the status management function:</p> <ul style="list-style-type: none"> <li>Active: The service is running.</li> <li>Incomp: The service is starting or stopping.</li> <li>Inactive: Either the system cannot communicate with the service or the service is stopped.</li> <li>Comm Err: The system is able to establish a connection to the service but there is no response.</li> <li>Timeout: The connection to the service has timed out.</li> <li>Error: An error other than a connection timeout has occurred. Refer to the common message log for details of the error. For details on PFM - Web Console service errors, see the trace log.</li> </ul>

## 1.6.2 Checking the status of services from the web browser

This subsection describes how to log on to PFM - Web Console from the monitoring console's web browser and how to check the status of services in the Services window.

You must have administrator user permission to check the status of services from the web browser.

To check the status of services in the monitoring console browser:

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Services** tab.
3. In the navigation frame of the Services window, choose the service of which you want to check an operation status.  
The navigation frame displays the following two folders under the root **System**:

**Machines** folder

This folder contains folders with the same names as the hosts where the Performance Management services are installed. The **Machines** folder manages the PFM - Agent or PFM - RM services for each host.

**PFM-Manager** folder

This folder manages the PFM - Manager services.

The selected service is marked with a checkmark.

4. In the method frame of the Services window, choose the **Service status** method.

The information frame of the Services window displays the name and status of the service selected in step 3.



## 1.7 Setting the automatic refresh interval for Web browsers

---

The window of PFM - Web Console that is displayed in the monitoring console Web browser is automatically refreshed every 60 seconds in the default setting. You can specify the automatic refresh interval for each user that logs on.

The specified automatic refresh interval applies to the following windows:

- Displayed Event Monitor window
- Agent status displayed in the Agents window
- Alarm status displayed in the Agents window
- Health check status displayed in the Agents window
- Displayed System Operational Status Summary window

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the menu bar frame, click the Environment Settings menu.
3. In the Environment Settings window, specify a refresh interval.

### **Refresh Interval**

Specify an interval within 10 to 3,600. The unit is seconds.

The default setting is 60 seconds.

4. Click the **OK** button.

## 1.8 Notes on starting and stopping Performance Management

### 1.8.1 When starting PFM - Agent or PFM - RM in a large-scale system

When starting Performance Management, normally you start PFM - Manager first, and then PFM - Base and either PFM - Agent or PFM - RM. In a large-scale system consisting of multiple servers, normally you start the system by controlling the sequence in which services are started among these servers.

You can still collect the performance data by starting PFM - Base and either PFM - Agent or PFM - RM first even when the Master Manager service and the Name Server service of PFM - Manager are not running.

The *stand-alone mode* refers to when PFM - Agent and PFM - Base or PFM - RM and PFM - Base operate separately.

The modes of the system are designated depending on the state of each program as follows:

- Only PFM - Agent, PFM - RM, or PFM - Base is running.  
This is called *stand-alone mode*.
- Initially PFM - Manager is running together with PFM - Agent, PFM -RM, or PFM - Base. Then PFM - Manager is stopped, so that only PFM - Base, PFM - Agent, or PFM - RM is running.  
This is called *non stand-alone mode*.
- PFM - Manager, PFM - Base, and either PFM - Agent or PFM - RM have started in this sequence and are all running.  
This is called *normal mode*.

Note:

PFM - Agent or PFM - RM cannot start by itself when PFM - Agent or PFM - RM is installed on the same host as PFM - Manager.

#### (1) Overview of stand-alone mode

When PFM - Agent, PFM - RM, or PFM - Base starts, they might fail to communicate with PFM - Manager if, for example, the Master Manager or Name Server service of PFM - Manager is not running. If communication with PFM - Manager fails, PFM - Agent, PFM - RM, or PFM - Base starts in stand-alone mode to collect performance data.

The system in stand-alone mode checks the connection to PFM - Manager after startup once every 5 minutes or at random intervals according to the settings in the startup information file (`jpccomm.ini`) on the local host. If PFM - Manager starts after PFM - Agent, PFM - RM, or PFM - Base have already started in stand-alone mode, and PFM - Manager performs a successful connection check with one of those programs, that program switches from stand-alone mode to normal mode connected to PFM - Manager. At this time, you can consult history reports to check the performance data stored in PFM - Agent or PFM - RM during stand-alone mode.

However, there are partial restrictions on the functionality and executable commands of Performance Management when PFM - Agent and PFM - Base or PFM - RM and PFM - Base run in stand-alone mode.

#### (2) Functions available in stand-alone mode

Table 1–3: Functions available in stand-alone mode

Function	Availability	Service name
Starting and stopping services, and checking operation status	Y	<ul style="list-style-type: none"><li>• In PFM-Agent host</li></ul>

Function	Availability	Service name
Starting and stopping services, and checking operation status	Y	Agent Store, Agent Collector, and Action Handler <ul style="list-style-type: none"> <li>In PFM-RM host Remote Monitor Store, Remote Monitor Collector, and Action Handler</li> </ul>
Collecting history data	Y	<ul style="list-style-type: none"> <li>In PFM-Agent host Agent Store and Agent Collector</li> <li>In PFM-RM host Remote Monitor Store and Remote Monitor Collector</li> </ul>
Displaying reports	N	Agent Store and Remote Monitor Store
Issuing alarms that indicate agent start	Y	Agent Collector and Remote Monitor Collector
Monitoring the performance data by alarms	N	Agent Collector and Remote Monitor Collector
Executing actions in response to alarm events	N	Action Handler
Service status management	Y	Status Server

Legend:

Y: Available

N: Not available

### (3) Commands available in stand-alone mode

Table 1–4: Commands available in stand-alone mode

Command	Function	Availability
<code>jpccconf db define</code>	Changing the directory settings of the Agent Store service and the Remote Monitor Store service	Y
<code>jpccconf db display</code>	Displaying information about the Agent Store service, the Remote Monitor Store service, or backup data	Y
<code>jpccconf db vrsset</code>	Changing the version of the Store database	Y
<code>jpccconf hc</code>	Enabling or disabling the health check function	Y
<code>jpccconf stat</code>	Enabling or disabling the status management function	Y
<code>jpccras</code>	Collecting troubleshooting data of PFM - Manager, PFM - Agent, or PFM - RM	Y
<code>jpccspm start</code>	Starting services	Y
<code>jpccspm stop</code>	Stopping services	Y
<code>jpcctool db backup</code>	Creating backup files of the data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y <sup>#</sup>
<code>jpcctool db clear</code>	Deleting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	N
<code>jpcctool db dmconvert</code>	Converting the data model of backup data	Y
<code>jpcctool db dump</code>	Exporting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y <sup>#</sup>

Command	Function	Availability
<code>jpctool db import</code>	Importing backup data	Y
<code>jpctool service delete</code>	Deleting service information of the agents registered in Performance Management	N
<code>jpctool service list</code> (when other host is specified by the <code>-host</code> option)	Displaying the structure and status of the Performance Management program services	N
<code>jpctool service list</code> (when the <code>-host</code> option is not used)	Checking the status of service operations on the local host	Y

**Legend:**

Y: Available

N: Not available

#

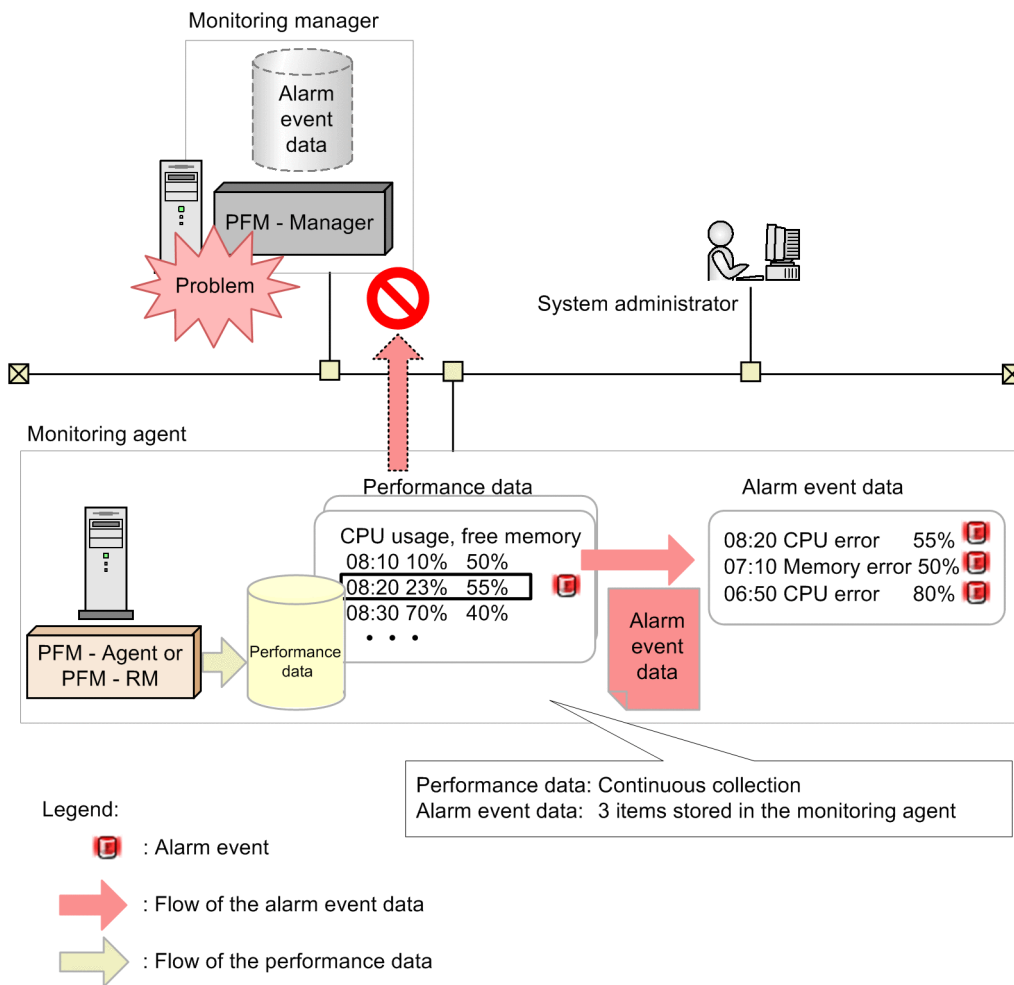
You can execute commands only when specifying the `-alone` option.

## (4) Overview of non stand-alone mode

Initially PFM - Manager runs together with PFM - Agent, PFM - RM or PFM - Base. Then PFM - Manager is stopped, so that only PFM - Base, PFM - Agent or PFM - RM is running. This is called *non stand-alone mode*.

Unlike stand-alone mode, the system does not check the connection to PFM - Manager once every 5 minutes in non stand-alone mode. When PFM - Manager starts, PFM - Agent or PFM - RM operates in normal mode. Performance data accumulated by PFM - Agent or PFM - RM in non-standalone mode can be viewed with historical reports.

Figure 1–1: Overview of non stand-alone mode



Notes:

- Alarm events cannot be reported to PFM - Manager when PFM - Agent or PFM - RM runs in non stand-alone mode. In such cases, the system holds alarm events by each alarm definition, and continues to attempt to report the alarm event until PFM - Manager starts. The oldest alarm event is overwritten when more than three alarm events are retained. All the retained alarm events are deleted when PFM - Agent or PFM - RM stops.

Reference note:

Because the Event Monitor and event history windows handle event data in different ways, the information displayed will differ.

Event history display of three alarm events that occurred in non stand-alone mode

1. PFM - Manager is stopped
2. PFM - Manager starts
3. The three alarms that occurred while PFM - Manager was stopped are sent from PFM - Agent.
4. The events are recorded by the Master Store service of PFM - Manager

Event information can now be displayed for all three events in the event history.

Event monitor display of three alarm events that occurred in non stand-alone mode

The event monitor displays the information stored in the PFM - Web Console cache.

The PFM - Web Console cache is cleared when PFM - Web Console reconnects to the View Server service of PFM - Manager.

When the PFM - Web Console connects to the View Server, its cache is synchronized with that of the View Server service and reconstructed.

In this case, only the most recent event related to the current alarm status of the agent is acquired.

If the alarm status received from the View Server service is normal (green), the event does not appear in the event monitor because the system is considered to be functioning normally.

If the alarm status is Warning (yellow) or Abnormal (red), the system is considered to be in a warning or abnormal state and the alarm event appears in the event monitor.

- The system resets the alarm statuses (alarm table status, which is indicated by the color of the alarm icon) reported to the PFM - Manager when PFM - Manager stops (the color of the alarm icon returns to green (normal)). Subsequently, when PFM - Manager starts, the operation differs depending on whether `Correlator Startup Mode` is enabled or disabled.

When `Correlator Startup Mode` is enabled (recommended)

A check of the information of the alarm status (alarm table status which is indicated by the color of the alarm icon) is performed when PFM - Manager receives an alarm event from PFM - Agent. This operation is for reducing the startup time of the Correlator service and preventing the startup of the Correlator service from failing. Until PFM - Manager receives an alarm event and verifies the agent status, PFM - Manager assumes that the agent status is unchanged since the last time PFM - Manager terminated.

When `Correlator Startup Mode` is disabled

The alarm statuses of all the agents that are registered in (connected to) the PFM - Manager service are checked when PFM - Manager restarts.

The information of alarm statuses (alarm table status, which is indicated by the color of the alarm icon) is checked.

For details about how to set `Correlator Startup Mode`, see the section that explains the setting items of the startup information file (`jpccomm.ini`) in the appendixes of the manual *JPI/Performance Management Reference*.

- An alarm flashing in red in the Web browser display returns to green immediately after PFM - Manager starts, and then returns to flashing red.

## (5) Functions available in non stand-alone mode

Table 1–5: Functions available in non stand-alone mode

Function	Availability	Service name
Starting and stopping services, and checking operation status	Y	<ul style="list-style-type: none"> <li>• In PFM-Agent host Agent Store, Agent Collector, and Action Handler</li> <li>• In PFM-RM host Remote Monitor Store, Remote Monitor Collector, and Action Handler</li> </ul>
Collecting history data	Y	<ul style="list-style-type: none"> <li>• In PFM-Agent host Agent Store and Agent Collector</li> <li>• In PFM-RM host Remote Monitor Store and Remote Monitor Collector</li> </ul>
Displaying reports	N	Agent Store and Remote Monitor Store
Monitoring the performance data by alarms	Y	Agent Collector and Remote Monitor Collector
Executing actions in response to alarm events	N <sup>#</sup>	Action Handler

Function	Availability	Service name
Service status management	Y	Status Server

**Legend:**

Y: Available

N: Not available

#

The system operates differently according to the following conditions:

When "LOCAL" is specified as the Action Handler service

If the host executing the action is running PFM - Base 09-00-09 or later or 10-00 or later

The action is executed even if PFM - Manager is stopped.

If the host executing the action is running PFM - Base 09-00-08 or earlier

- If no action has been executed

No action is executed while PFM - Manager is stopped.

Even when PFM - Manager restarts, any action that was generated while PFM - Manager was stopped is not executed.

- If at least one action has been executed but the Action Handler service that executed the action has not restarted

The action is executed even while PFM - Manager is stopped.

When a value other than "LOCAL" is specified as the Action Handler service

No actions are executed while PFM - Manager is stopped.

After PFM - Manager starts, any actions that were generated while PFM - Manager was stopped are executed.

However, if you specify the Action Handler service on the PFM - Manager host, the actions might not be executed depending on the position of the Action Handler service in the startup sequence.

## (6) Commands available in non stand-alone mode

Table 1–6: Commands available in non stand-alone mode

Command	Function	Availability
jpccconf db define	Changing the directory settings of the Agent Store service or the Remote Monitor Store service	Y
jpccconf db display	Displaying information about the Agent Store service, the Remote Monitor Store service, or backup data	Y
jpccconf db vreset	Changing the version of the Store database	Y
jpccconf hc	Enabling or disabling the health check function	Y
jpccconf stat	Enabling or disabling the status management function	Y
jpccras	Collecting troubleshooting data of PFM - Manager, PFM - Agent, or PFM - RM	Y
jpccspm start	Starting services	Y
jpccspm stop	Stopping services	Y
jpcctool db backup	Creating backup files of the data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y#
jpcctool db clear	Deleting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	N

Command	Function	Availability
<code>jpctool db dmconvert</code>	Converting the data model of backup data	Y
<code>jpctool db dump</code>	Exporting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y#
<code>jpctool db import</code>	Importing backup data	Y
<code>jpctool service delete</code>	Deleting service information of the agents registered in Performance Management	N
<code>jpctool service list</code> (when other host is specified by the <code>-host</code> option)	Displaying the structure and status of the Performance Management program services	N
<code>jpctool service list</code> (when the <code>-host</code> option is not used)	Checking the status of service operations on the local host	Y

Legend:

Y: Available

N: Not available

#

You can execute commands only when specifying the `-alone` option.

## 1.8.2 Starting a PFM - Agent or PFM - RM service during command execution

If you start a PFM - Agent or PFM - RM service while a command is executing (such as `jpctool db dump`), the system starts in stand-alone mode because PFM - Manager takes some time to respond. The system checks for a connection with PFM - Manager for a specific interval (five minutes). If a connection is established, the stand-alone mode ends.

## 1.8.3 Starting on a Windows machine

When you execute the `jpccspm start` command on a Windows machine to start the Performance Management program services, the Performance Management program services might not start if other Windows services start at the same time. If this happens, a KAVE05163-E message is output to the common message log.

When this message is displayed, take the corrective action provided in the message.

If this message is issued frequently, change the retry interval and count at which services are started automatically by the `jpccspm start` command. Changing the retry interval and count avoids service start errors caused by the service control manager.

Directly edit the settings of the `jpccomm.ini` file to change the retry interval and count. The following table describes the section name, label name, and range of setting values that you can edit in the `jpccomm.ini` file.

Section	Label	Value range	Default value	Description
Tools Section	StartService Retry Interval	30 - 600 <sup>#1</sup>	45	Retry interval for service starts (unit: seconds)



Section	Label	Value range	Default value	Description
Tools Section	StartService Retry Count	0 - 120#2	3	Retry count for service start (unit: times)

#1

When the specified value is 29 or lower, or 601 or higher, the system operates as if the specified value is 30, or 600 respectively.

#2

When the specified value is -1 or lower, or 121 or higher, the system operates as if the specified value is 0, or 120 respectively.

The installation folder stores the `jpccomm.ini` file.

To change the retry intervals and counts:

1. Use a text editor or a similar tool to open the `jpccomm.ini` file.
2. Change the retry intervals and counts.

Change values of the following labels:

```
[Tools Section]
StartService Retry Interval=45
StartService Retry Count=3
```

3. Save and then close the `jpccomm.ini` file.

## 1.8.4 Monitoring alarm events

When PFM - Manager stops due to problems or other reasons, PFM - Agent or PFM - RM does not issue alarm events correctly. Start the PFM - Manager for the connection destination.

While PFM - Manager is stopped, PFM - Agent or PFM - RM retains alarm events for each alarm definition. These alarm events are issued after PFM - Manager restarts. The number of retained alarm events is as follows.

- When monitoring state changes for each record instance  
A maximum of three alarm events per alarm definition are retained. If more than three alarm events occur for an instance of a record monitored with a specific alarm definition, the alarm events are overwritten in order from the oldest.
- When not monitoring state changes for each record instance  
A maximum of three alarm events per alarm definition are retained. If more than three alarm events occur for a specific alarm definition, the alarm events are overwritten in order from the oldest.

## 1.8.5 Executing actions

Actions cannot be executed correctly if the PFM - Manager for the connection destination or Action Handler services stop. Start the PFM - Manager for the connection destination and Action Handler services when executing actions.

## 1.8.6 Changing settings when using business groups

If you create business group ordinary users and then disable access control based on business groups, the users you created will no longer be able to log in to the monitoring console. When changing to an environment that does not control access based on business groups, delete the business group ordinary users first.

# 2

## Managing User Accounts and Business Groups

This chapter provides an overview of user management in Performance Management, and describes how to create and edit user accounts and manage business groups.

## 2.1 Overview of user accounts and business groups

---

### 2.1.1 About user authentication modes

You can select the user account management method in Performance Management. One method is to manage user accounts within the operation monitoring system and the other is to perform integrated management of user accounts by using an integrated management system. In this manual, the former is called the *PFM authentication mode*, and the latter is called the *JP1 authentication mode*.

#### PFM authentication mode

Use a *Performance Management user* created in Performance Management to log on to PFM - Web Console. User accounts are managed by PFM - Manager. This is a standard user account management method in the Performance Management system, and is the default setting.

#### JP1 authentication mode

Use a *JP1 user* created in JP1/Base, an authentication server of the integrated management system (JP1/IM), to log on to PFM - Web Console. JP1/Base manages user accounts. You need to install JP1/Base on the host that has PFM - Manager installed to use this mode.

#### Note:

- To use PFM - Manager in a logical host environment to set the JP1 authentication mode, JP1/Base must be running on the same logical host as PFM - Manager.
- To use the JP1 authentication mode, you must set up an authentication server to be used by JP1/Base. However, the JP1/Base authentication server does not need to be running on the same host as PFM - Manager. For details on how to configure the authentication server used by JP1/Base, see the *JP1/Base User's Guide*.
- To use the JP1 authentication mode in an environment using PFM - Manager on a cluster system, JP1/Base must also be used on the cluster system.
- When you set the JP1 authentication mode in PFM - Manager in a multiple-monitoring configuration, you must install JP1/Base on the primary and secondary Manager hosts and set up an authentication server on each host.

### 2.1.2 About user permissions

In Performance Management, you can assign permissions to user accounts that define the operations the user is able to perform. You can assign *administrator user permission*, which gives the user access to all functions of Performance Management including configuring how operating information is collected and changing report and alarm definitions, and *general user permission* which allows the user to view reports and alarms.

For details on the functionality available to users with each user permission, see [2.2 User account permissions](#).

### 2.1.3 About business groups

In Performance Management, you can group monitored hosts by business unit and limit the monitoring agents available to users. A group of monitored hosts created for a business unit is called a *business group*. Users who are assigned a business group are able to reference the monitoring agents within the range defined in the business group.

In this manual, a user who is assigned a business group is called a *business group user*, and a user with access to the entire system is called a *system user*. Only users with general user permission can be assigned a business group. Users

with administrator user permission are already able to configure and reference all monitoring agents. A user with general user permission who is assigned a business group is called a *business group ordinary user*.

In Performance Management, you can use business groups defined by Performance Management, and business groups defined in the integrated management product (JP1/IM).

#### Business groups defined in Performance Management

Business groups are assigned to monitored hosts and user accounts by Performance Management.

Use this approach when you are not linking with JP1/IM, and when you want to manage the business groups used with Performance Management separately from those defined in JP1/IM.

You can use these business groups in PFM authentication mode and in JP1 authentication mode.

#### Business groups defined in JP1/IM

You can use the business groups defined by JP1/IM by importing the business group hierarchy into Performance Management. Use this approach when you are linking Performance Management with JP1/IM and wish to keep the same association in the two products between monitored hosts and the user accounts that are able to access them. This helps you avoid issues that occur due to mismatched business group assignments when performing certain tasks such as displaying Performance Management reports from JP1/IM.

You can use these business groups in JP1 authentication mode.

For details on linking with JP1/IM, see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

## 2.2 User account permissions

The Performance Management functions that are available to a user depend on the permissions assigned to the user account.

### 2.2.1 Functions available to system users

Table 2–1: Available features by user account permission (operations applying to the system in general)

Function	Function detail	Tree or window	Operation applying to the system in general			
			Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Management of the Performance Management program services	Displaying the Services window	Services tree	Y	N	Y	N
	Stopping the Performance Management program services	Services tree	Y	N	Y	N
	Checking the status of the Performance Management program services	Services tree	Y	N	Y	N
Management of the Performance Management user accounts	Displaying the Users window	Users tree	Y	N	N	N
	Creating, copying, and deleting user accounts	Users tree	Y	N	N	N
	Changing the logon password for currently logged-on user accounts	Change Password window	Y	Y	N	N
	Changing the logon password or permission of other user accounts	Users tree	Y	N	N	N
Management of agents	Displaying the Agents window (in User Agents style)	Agents tree	Y	Y	Y	Y
	Displaying the Agents window (in Products style)	Agents tree	Y	C	Y	C
	Creating, copying, and deleting folders	Agents tree	Y	C	Y	C
	Changing folder names	Agents tree	Y	C	Y	C

Function	Function detail	Tree or window	Operation applying to the system in general			
			Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Management of agents	Adding, copying, and deleting agents	Agents tree	Y	C	Y	C
	Displaying agent properties	Agents tree	Y	Y	Y	Y
	Displaying the summary	Agents tree	Y	Y	Y	Y
	Configuring process monitoring	Agents tree	Y	N	Y	N
	Changing agent properties	Services tree	Y	N	Y	N
	Distributing agent properties	Services tree	Y	N	Y	N
	Displaying bound agents	Alarms tree	Y	N	Y	N
Definition and operation of reports	Displaying a report hierarchy	Reports tree	Y	C	Y	C
	Defining reports by using the report wizard	Reports tree	Y	C	Y	C
	Editing report definitions from the View Report window	Reports tree	Y	Y	Y	Y
	Saving report definitions from the View Report window	Reports tree	Y	C	Y	C
	Importing and exporting report definitions	Reports tree	Y	C	Y	C
	Displaying reports about agents	Agents tree/ Bookmarks tree/View Report window	Y	Y	Y	Y
	Displaying reports about alarms	Agents tree	Y	Y	Y	Y
	Editing, copying, and deleting reports	Reports tree	Y	C	Y	C
	Changing report names	Reports tree	Y	C	Y	C
	Displaying report properties	Reports tree	Y	C	Y	C

Function	Function detail	Tree or window	Operation applying to the system in general			
			Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Definition and operation of reports	Changing report display conditions	View Report window	Y	Y	Y	Y
	Printing reports	View Report window	Y	Y	Y	Y
	Outputting report files	Agents tree/ Bookmarks tree	Y	Y	Y	Y
Definition and operation of alarms	Displaying the Alarms window	Alarms tree	Y	N	Y	N
	Defining an alarm by using the alarm wizard	Alarms tree	Y	N	Y	N
	Defining an alarm by using the Quick Guide	Agents tree	Y	N	Y	N
	Binding or unbinding alarm tables in the Agents window	Agents tree	Y	N	Y	N
	Importing and exporting alarm definitions	Alarms tree	Y	N	Y	N
	Displaying the status of agent-related alarms in the Agents tree	Agents tree	Y	Y	Y	Y
	Operating and stopping alarms	Alarms tree	Y	N	Y	N
	Copying and deleting alarm tables	Alarms tree	Y	N	Y	N
	Copying and deleting alarms	Alarms tree	Y	N	Y	N
	Editing alarms	Alarms tree	Y	N	Y	N
	Displaying alarm properties in the Agents window	Agents tree	Y	Y	Y	Y
	Displaying alarm properties in the Event Monitor window	Event Monitor window	Y	Y	Y	Y
	Displaying alarm properties in the Alarms window	Alarms tree	Y	N	Y	N



Function	Function detail	Tree or window	Operation applying to the system in general			
			Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Definition and operation of alarms	Displaying the message area in the navigation frame	Agents tree	Y	N	Y	N
	Displaying the Alarm Application Status window	Agents tree	Y	N	Y	N
	Applying alarm information in the Alarm Application Status window	Agents tree	Y	N	Y	N
Event display	Displaying the Event Monitor window	Event Monitor window	Y	Y	Y	Y
	Changing the event to be displayed	Event Monitor window	Y	Y	Y	Y
	Displaying reports about alarm events	Event Monitor window	Y	Y	Y	Y
	Displaying the Event History window	Agents tree	Y	Y	Y	Y
Monitoring suspension	Displaying the Monitoring Suspension Settings window	Agents tree	Y	Y	Y	Y
	Suspending and resuming monitoring	Agents tree	Y	N	Y	N
Management of the Store database	Changing the recording method of performance data	Services tree	Y	N	Y	N
	Adjusting the retention period of the Store database	Services tree	Y	N	Y	N
	Checking the capacity of the Store database	Services tree	Y	N	Y	N
Management of bookmarks	Displaying the Bookmarks tree	Bookmarks tree	Y	Y	Y	Y
	Creating folders	Bookmarks tree/Agents tree/View Report window/	Y	C	Y	C

Function	Function detail	Tree or window	Operation applying to the system in general			
			Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Management of bookmarks	Creating folders	Bookmark window	Y	C	Y	C
	Deleting folders	Bookmarks tree	Y	C	Y	C
	Changing folder names	Bookmarks tree	Y	C	Y	C
	Deleting bookmarks	Bookmarks tree	Y	C	Y	C
	Displaying bookmark properties	Bookmarks tree	Y	Y	Y	Y
	Changing bookmark names	Bookmarks tree	Y	C	Y	C
	Deleting registered reports	Bookmarks tree	Y	C	Y	C
	Displaying registered reports	Bookmarks tree	Y	Y	Y	Y
	Editing combination reports	Bookmarks tree	Y	C	Y	C
	Tiling display	Bookmarks tree	Y	Y	Y	Y
	Registering bookmarks or combination bookmarks	View Report window/ Bookmark window	Y	C	Y	C
	Registering a baseline	View Report window	Y	C	Y	C
	Updating a baseline	View Report window	Y	C	Y	C
	Display of health check status	Displaying the health check status of each agent from the Agents tree	Agents tree	Y	Y	Y
Displaying the status of lower-level agents as the icon of a higher-level folder in the Agents tree		Agents tree	Y	Y	Y	Y
Changing the priority for displaying the status of lower-level agents as the icon of a higher-level folder		Agents tree	Y	Y	Y	Y

Function	Function detail	Tree or window	Operation applying to the system in general			
			Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Display of health check status	Displaying the health check status of an agent from the Alarm Status window	Agents tree	Y	Y	Y	Y
	Displaying health check events in the Event Monitor or Event History window	Event Monitor window/ Event History window	Y	Y	Y	Y
Display of reports from a related product	Displaying related reports	The window of the related product	Y	Y	Y	Y
Auto alarm bind	Automatically binding an alarm table to monitoring agents	Automatic Bind Settings window	Y	N	Y	N

Legend:

Y: Available

N: Not available

C: In the initialization file (`config.xml`), you can specify whether the function is made available to the user.

## 2.2.2 Functions available to business group users

Table 2–2: Available features by user account permission (operations applying to business groups)

Function	Function detail	Tree or window	Operations applying to business groups	
			Performance Management user	JP1 user
			Business group ordinary user	Ordinary user
Management of Performance Management program services	Displaying the Services window	Services tree	N	N
	Stopping the Performance Management program services	Services tree	N	N
	Checking the status of the Performance Management program services	Services tree	N	N
Management of Performance Management user accounts	Displaying the Users window	Users tree	N	N
	Creating, copying, and deleting user accounts	Users tree	N	N

Function	Function detail	Tree or window	Operations applying to business groups	
			Performance Management user	JP1 user
			Business group ordinary user	Ordinary user
Management of Performance Management user accounts	Changing the logon password for currently logged-on user accounts	Change Password window	Y	N
	Changing the logon password or permission of other user accounts	Users tree	N	N
Management of agents	Displaying the Agents window (in User Agents style)	Agents tree	Y	Y
	Displaying the Agents window (in Products style)#1	Agents tree	C	C
	Creating, copying, and deleting folders	Agents tree	C	C
	Changing folder names	Agents tree	C	C
	Adding, copying, and deleting agents	Agents tree	C	C
	Displaying agent properties	Agents tree	Y	Y
	Displaying the summary	Agents tree	Y	Y
	Configuring process monitoring	Agents tree	N	N
	Changing agent properties	Services tree	N	N
	Distributing agent properties	Services tree	N	N
	Displaying bound agents	Alarms tree	N	N
Definition and operation of reports	Displaying a report hierarchy	Reports tree	N	N
	Defining reports by using the report wizard	Reports tree	N	N
	Editing report definitions from the View Report window	Reports tree	Y	Y
	Saving report definitions from the View Report window	Reports tree	N	N
	Importing and exporting report definitions	Reports tree	N	N
	Displaying reports about agents	Agents tree/Bookmarks tree/View Report window	Y	Y
	Displaying reports about alarms	Agents tree	Y	Y

Function	Function detail	Tree or window	Operations applying to business groups	
			Performance Management user	JP1 user
			Business group ordinary user	Ordinary user
Definition and operation of reports	Editing, copying, and deleting reports	Reports tree	N	N
	Changing report names	Reports tree	N	N
	Displaying report properties	Reports tree	N	N
	Changing report display conditions	View Report window	Y	Y
	Printing reports	View Report window	Y	Y
	Outputting report files	Agents tree/Bookmarks tree	Y	Y
Definition and operation of alarms	Displaying the Alarms window	Alarms tree	N	N
	Defining an alarm by using the alarm wizard	Alarms tree	N	N
	Defining an alarm by using the Quick Guide	Agents tree	N	N
	Binding or unbinding alarm tables in the Agents window	Agents tree	N	N
	Importing and exporting alarm definitions	Alarms tree	N	N
	Displaying the status of agent-related alarms in the Agents tree	Agents tree	Y	Y
	Starting and stopping alarms	Alarms tree	N	N
	Copying and deleting alarm tables	Alarms tree	N	N
	Copying and deleting alarms	Alarms tree	N	N
	Editing alarms	Alarms tree	N	N
	Displaying alarm properties in the Agents window <sup>#2</sup>	Agents tree	Y	Y
	Displaying alarm properties in the Event Monitor window <sup>#2</sup>	Event Monitor window	Y	Y
	Displaying alarm properties in the Alarms window	Alarms tree	N	N
	Displaying the message area in the navigation frame	Agents tree	N	N
Displaying the Alarm Application Status window	Agents tree	N	N	

Function	Function detail	Tree or window	Operations applying to business groups	
			Performance Management user	JP1 user
			Business group ordinary user	Ordinary user
Definition and operation of alarms	Applying alarm information in the Alarm Application Status window	Agents tree	N	N
Event display	Displaying the Event Monitor window <sup>#3</sup>	Event Monitor window	Y	Y
	Changing displayed events	Event Monitor window	Y	Y
	Displaying reports about alarm events	Event Monitor window	Y	Y
	Displaying the Event History window <sup>#3</sup>	Agents tree	Y	Y
Monitoring suspension	Displaying the Monitoring Suspension Settings window	Agents tree	Y	Y
	Suspending and resuming monitoring	Agents tree	N	N
Management of the Store database	Changing the recording method of performance data	Services tree	N	N
	Adjusting the retention period of the Store database	Services tree	N	N
	Checking the capacity of the Store database	Services tree	N	N
Management of bookmarks	Displaying the Bookmarks tree	Bookmarks tree	Y	Y
	Creating folders	Bookmarks tree/Agents tree/Reports window/Bookmark window	N	N
	Deleting folders	Bookmarks tree	N	N
	Changing folder names	Bookmarks tree	N	N
	Deleting bookmarks	Bookmarks tree	N	N
	Displaying bookmark properties	Bookmarks tree	Y	Y
	Changing bookmark names	Bookmarks tree	N	N
	Deleting registered reports	Bookmarks tree	N	N
	Displaying registered reports	Bookmarks tree	Y	Y
	Editing combination reports	Bookmarks tree	N	N
	Tiling display	Bookmarks tree	Y	Y
Registering bookmarks or combination bookmarks	View Report window/Bookmark window	N	N	

Function	Function detail	Tree or window	Operations applying to business groups	
			Performance Management user	JP1 user
			Business group ordinary user	Ordinary user
Management of bookmarks	Registering a baseline	View Report window	N	N
	Updating a baseline	View Report window	N	N
Display of health check status	Displaying the health check status of each agent from the Agents tree	Agents tree	Y	Y
	Displaying the status of lower-level agents as the icon of a higher-level folder in the Agents tree	Agents tree	Y	Y
	Changing the priority for displaying the status of lower-level agents as the icon of a higher-level folder	Agents tree	Y	Y
	Displaying the health check status of an agent from the Alarm Status window	Agents tree	Y	Y
	Displaying health check events in the Event Monitor or Event History window	Event Monitor window/ Event History window	Y	Y
Display of reports from a related product	Displaying related reports	The window of the related product	Y	Y
Auto alarm bind	Automatically binding an alarm table to monitoring agents	Automatic Bind Settings window	N	N

Legend:

Y: Available

N: Not available

C: In the initialization file (`config.xml`), you can specify whether the function is made available to the user.

#1

Only displays the agents in the business groups for which the user has view permission.

#2

The **Action** and **Action Definition** alarm properties are not displayed.

#3

Only displays the events issued by agents in the business groups for which the user has view permission.

## 2.3 Tasks involved in user account setup

This section describes the tasks involved in setting up user accounts for each authentication mode.

Table 2–3: Tasks required to set up user accounts (PFM authentication mode)

Operation target	User permission	Description of task	Overview
Entire system	Management user	<i>2.5.1 Creating a Performance Management user account</i>	Create a user account with <b>Management user</b> selected as the user permission.
	Ordinary user	<i>2.5.1 Creating a Performance Management user account</i>	Create a user account with <b>Ordinary user</b> selected as the user permission.
Business group <sup>#</sup>	Ordinary user	<i>2.7.2 Defining business groups in Performance Management</i>	Create a business group.
		<i>2.5.1 Creating a Performance Management user account</i>	Create a user account as follows: <ul style="list-style-type: none"> <li>• Select <b>Business group ordinary user</b> as the permission</li> <li>• Select the business groups to associate with the user account</li> </ul>

#

Access control based on business groups must be set up before you perform these tasks. For details, see *2.7.1 Setting up access control based on business groups*.

The table below describes the tasks required to set up a user account that uses JP1 authentication mode. You must set the authentication mode in Performance Management before you set up user accounts that use JP1 authentication mode. For details, see *2.4 Setting the user account authentication mode*.

Table 2–4: Tasks required to set up user accounts (JP1 authentication mode)

Operation target	User permission	Description of required tasks	Overview
Entire system	Management user	<i>2.6 Setting operating permissions for JP1 users</i>	Set the JP1 user operating permissions to allow users to have administrator user permission for Performance Management.
	Ordinary user	<i>2.6 Setting operating permissions for JP1 users</i>	Set the JP1 user operating permissions to allow the JP1 user to have ordinary user permission for Performance Management.
Business group (Performance Management) <sup>#1, #2</sup>	Ordinary user	<i>2.7.2 Defining business groups in Performance Management</i>	Create business groups.
		<i>2.6 Setting operating permissions for JP1 users</i>	Set the operating permissions for the JP1 user as follows: <ul style="list-style-type: none"> <li>• Specify the JP1 resource groups to associate with the business group</li> <li>• Select the JP1 permission level to assign ordinary user permission to Performance Management users</li> </ul>
Business group (JP1/IM) <sup>#1, #3</sup>	Ordinary user	<i>2.7.3 Using business groups defined in JP1/IM</i> .	Import the business groups defined in JP1/IM into Performance Management. Also, add a JP1 permission level that gives JP1 users ordinary user permission in Performance Management.



#1

Access control based on business groups must be set up before you perform these tasks. For details, see [2.7.1 Setting up access control based on business groups](#).

#2

A user associated with a business group defined in Performance Management.

#3

A user associated with a business group defined in JP1/IM.

## 2.4 Setting the user account authentication mode

---

Use the `jpcvsvr.ini` file to set the authentication mode of a user account (management method). The default mode is PFM authentication mode. If you will be using the JP1 authentication mode, change the value of `UserServer.authenticationMode` in the `jpcvsvr.ini` file to `JP1`. For details about the `jpcvsvr.ini` file, see the chapter that describes definition files in the manual *JP1/Performance Management Reference*.

Note:

- A message indicating an authentication error appears if, after the authentication mode is set, you logged on to PFM - Web Console by using a user account with a management method that is different from the set mode.

## 2.5 Setting up and using Performance Management user accounts

---

### 2.5.1 Creating a Performance Management user account

If you set the PFM authentication mode, create user accounts by logging on to PFM - Web Console from a web browser.

JP1/Base manages user accounts when you set the JP1 authentication mode. For details on how to manage JP1 users, see the manual *JP1/Base User's Guide*.

Note:

You can create a maximum of 5,000 user accounts.

#### (1) Creating a new Performance Management user account

Reference note: The user account set immediately after installation

The ADMINISTRATOR is set as a default user account immediately after the installation of Performance Management.

The default user account settings are as follows:

- **User name:** ADMINISTRATOR
- **Password:** None. Specify a password before starting operation.
- **Permission:** Management user

1. Log on to PFM - Web Console from the Web browser of the monitoring console.

Log on with a user account that has the administrator user permissions (for example, the default user account ADMINISTRATOR).

2. In the navigation frame of the Main window, choose the **Users** tab.

3. In the method frame of the Users window, select the **New User** method.

4. In the New User window, specify the account information for the Performance Management user account.

Items to be specified are as follows:

##### User Name

Specify 1-16 characters. Characters that can be used include alphabetical characters (upper-case and lower-case), numeric characters, and symbols (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space). The system does not distinguish between upper- and lower-case characters.

If you enter spaces before or after the entered strings, the system deletes the spaces.

##### Password and Confirm password

Specify 1-16 characters. Characters that can be used include alphabetical characters (upper-case and lower-case), numeric characters, and symbols (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space). The system distinguishes between upper- and lower-case characters.

If you enter spaces before or after the entered strings, the system deletes the spaces.

Note:


Hitachi recommends that the password for Performance Management be six or more characters and include both alphanumeric characters and symbols. A confirmation message is displayed when an unsuitable password is entered such as one made up of only alphabetic characters or numeric characters, or one containing five characters or fewer. A message is also displayed when a password that is the same as the user name is entered.

### Selection of authority and Assignment of business groups

Select the user permission for the user account you are creating.

- **Management user:** Permission to manage the entire system.
- **Ordinary user:** Permission to reference the entire system.
- **Business group ordinary user:** Permission to reference the monitoring agents in the business groups displayed in **Assigned business groups**.

### All business groups

This area displays a list of business groups defined in the system. To assign a business group to the user account, select the business group in the list and click the  button. The business groups you assign appear in the **Assigned business groups** list.

### Assigned business groups

This area displays the business groups assigned to the user account you are creating.

5. Click the **OK** button.

The created user account is added to the Performance Management user level in the navigation frame.

## (2) Copying and customizing an existing user account

You can create a user account that has duplicate settings by copying an existing user account and saving it with a different user name.



### Tip

When you copy an existing user account to create a new user account, the procedure also copies information defined in the source user account such as information about the Agents tree for monitoring.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.

Log on with a user account that has the administrator user permissions (for example, the default user account ADMINISTRATOR).

2. In the navigation frame of the Main window, choose the **Users** tab.

3. In the navigation frame of the Users window, select a source user account.

The selected user is marked with a checkmark.

4. Choose the **Copy** method in the method frame.

5. In the Copy window, enter the settings for the new Performance Management user account you are creating.

Each item is populated with information of the source user account. If necessary, make changes for the following items:

### User Name

Specify 1-16 characters. Characters that can be used include alphabetical characters (upper-case and lower-case), numeric characters, and symbols (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space).

The system does not distinguish between upper- and lower-case characters.

If you enter spaces before or after the entered strings, the system deletes the spaces.

## Password and Confirm password

Specify 1-16 characters. Characters that can be used include alphabetical characters (upper-case and lower-case), numeric characters, and symbols (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space). The system distinguishes between upper- and lower-case characters.

If you enter spaces before or after the entered strings, the system deletes the spaces.

Note:

Hitachi recommends that the password for Performance Management be six or more characters and include both alphanumeric characters and symbols. A confirmation message is displayed when an unsuitable password is entered such as one made up of only alphabetic characters or numeric characters, or one containing five characters or fewer. A message is also displayed when a password that is the same as the user name is entered.

## Selection of authority and Assignment of business groups


Select the user permission for the user account you are creating.

- **Management user:** Permission to manage the entire system.

- **Ordinary user:** Permission to reference the entire system.

- **Business group ordinary user:** Permission to reference the monitoring agents in the business groups displayed in **Assigned business groups**.

## All business groups

This area displays a list of business groups defined in the system. To assign a business group to the user account, select the business group in the list and click the  button. The business groups you assign appear in the **Assigned business groups** list.

## Assigned business groups

This area displays the business groups assigned to the user account you are creating.

6. Click the **OK** button.

A newly created user account is added in the Performance Management Users tree.

## 2.5.2 Editing a Performance Management user account

### (1) Changing the password

#### (a) When changing the password for a currently logged-on user account

1. In the menu bar frame of the Main window, choose the **Change Password** menu.

2. In the Change Password window, enter the password information.

#### Current password

Enter the current password.

#### New password and Confirm new password

Enter the new password you wish to specify.

Specify 1-16 characters. Characters that can be used include alphabetical characters (upper-case and lower-case), numeric characters, and symbols (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space).

The system distinguishes between upper- and lower-case characters. If you enter spaces before or after the entered strings, the system deletes the spaces.

Note:

Hitachi recommends that the password for Performance Management be six or more characters and include both alphanumeric characters and symbols. A confirmation message is displayed when an unsuitable password is entered such as one made up of only alphabetic characters or numeric characters, or one containing five characters or fewer. A message is also displayed when a password that is the same as the user name is entered.

3. Click the **OK** button.

The changed password for the currently logged-on user account takes effect.

## **(b) When changing the password for the user account of another user**

To change the password for the user account of another user:

1. Log on to PFM - Web Console from the Web browser of the monitoring console.

Log on with a user account that has the administrator user permissions (for example, the default user account ADMINISTRATOR).

2. In the navigation frame of the Main window, choose the **Users** tab.

3. In the navigation frame of the Users window, select the user account whose password you want to change.

The selected user is marked with a checkmark.

4. Select the **Edit** method in the method frame.

5. In the Edit window, change the password for the user account you selected in step 3.

Specify 1-16 characters. Characters that can be used include alphabetical characters (upper-case and lower-case), numeric characters, and symbols (! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ space). The system distinguishes between upper- and lower-case characters.

If you enter spaces before or after the entered strings, the system deletes the spaces.

Note:

Hitachi recommends that the password for Performance Management be six or more characters and include both alphanumeric characters and symbols. A confirmation message is displayed when an unsuitable password is entered such as one made up of only alphabetic characters or numeric characters, or one containing five characters or fewer. A message is also displayed when a password that is the same as the user name is entered.

6. Click the **OK** button.

The changed password for the selected user account takes effect.

## **(2) Changing the permissions and business group assignments of a Performance Management user account**

1. Log on to PFM - Web Console from the Web browser of the monitoring console.


Log on with a user account that has the administrator user permissions (for example, the default user account ADMINISTRATOR).

2. In the navigation frame of the Main window, choose the **Users** tab.

3. In the navigation frame of the Users window, select the user account whose permissions you want to change.

The selected user is marked with a checkmark.

4. Select the **Edit** method in the method frame.

5. In the Edit window, change the permissions for the user account you selected in step 3.
6. If you selected **Business group ordinary user** in step 5, select the business groups to assign to the user account.  
Select the business groups you want to assign in the **All business groups** area, and click the  button. The business groups you selected appear in the **Assigned business groups** area.
7. Click the **OK** button.  
The changed permissions of the selected user account takes effect.

### (3) Deleting a Performance Management user account

#### Note:

You can delete the default user account (the ADMINISTRATOR user account that does not require a password) if you create another user account.

If you delete the default user account, you cannot re-create the ADMINISTRATOR user account that does not require a password.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
Log on with a user account that has the administrator user permissions (for example, the default user account ADMINISTRATOR).
2. In the navigation frame of the Main window, choose the **Users** tab.
3. In the navigation frame of the Users window, select a user account to be deleted.  
The selected user is marked with a checkmark.
4. Choose the **Delete** method in the method frame.
5. Click the **OK** button in the confirmation dialog box.  
The selected user account is deleted from the navigation frame.

## 2.6 Setting operating permissions for JP1 users

---

If you use JP1 authentication mode, you must set the operating permissions for JP1 users in the authentication server JP1/Base. Assign the operating permissions described in the following table according to the Performance Management permissions you want to assign to the JP1 user.

Table 2–5: Operating permissions for JP1 users

Performance Management permission	JP1 user operating permissions	
	JP1 resource group	JP1 permission level
Management user	JP1_PFM	JP1_PFM_Admin
Ordinary user (business group not assigned)	JP1_PFM	JP1_PFM_Operator
Ordinary user (with business group defined in Performance Management assigned)	Chosen group <sup>#</sup>	JP1_PFM_Operator
Ordinary user (with business group defined in JP1/IM assigned)	See 2.7.3(4) <i>Setting operating permissions for JP1 users</i> .	

#

Specify the JP1 resource group to be associated with the business groups you define in Performance Management. Specify the name as it appears under the JP1 Resource Group Name label in the business group definition file.

For details on how to set the operating permissions of JP1 users, see the *JP1/Base User's Guide*.



## 2.7 Setting and using business groups

---

Before you can use business groups, you need to enable the function that controls access using business groups. You can then set up business groups by defining them in Performance Management, or use the business groups defined in JP1/IM.

### 2.7.1 Setting up access control based on business groups

Set up access control based on business groups on the PFM - Manager host.

#### Important

To control access using business groups, the versions of PFM - Manager and PFM - Web Console must be 10-00 or later. After you enable this function, connections can no longer be established from versions of PFM - Web Console earlier than 10-00.

You can enable or disable access control based on business groups by editing the `jpccomm.ini` file directly. The `jpccomm.ini` file is stored in the following location:

On physical hosts

In Windows:

*installation-folder\*

In UNIX:

*/opt/jp1pc/*

On logical hosts

In Windows:

*environment-directory\jp1pc\*

In UNIX:

*environment-directory/jp1pc/*

#### Important

If you disable access control based on business groups after creating business group ordinary users, those users are no longer able to log on to the monitoring console. Delete business group ordinary users before you disable access control based on business groups.

To enable or disable access control based on business groups:

1. Stop all PFM - Manager services by using the `jpccpm stop` command.

In a cluster system, stop the services from the cluster software.

2. Open the `jpccomm.ini` file on the PFM - Manager host in a text editor or similar.

3. Enable or disable access control based on business groups.

In the `Common Section` section of the `jpccomm.ini` file, change the value of the following label:

To enable the function:

```
Business Group Monitor Mode=1
```

To disable the function:

```
Business Group Monitor Mode=0
```

4. Save the `jpccomm.ini` file and close the text editor.
5. Use the `jpccspm start` command to start the PFM - Manager services.  
In a cluster system, start the services from the cluster software.

## 2.7.2 Defining business groups in Performance Management

You can define business groups in Performance Management by creating, validating, and then importing a business group definition file.

### (1) Creating a business group definition file

The following describes how to create a business group definition file, and enter business group definitions in the file.

#### (a) Outputting a template file for the business group definition file

Before you create a business group definition file, output the template file that includes all of the labels that need to be defined in the business group definition file.

In this example, the template file is output with the file name `/tmp/businessgroup01.cfg`.

1. Log on to the host where PFM - Manager is installed.
2. Output the template file.

To output the template file, use the `jpccconf bgdef export` command. Execute the command with the `-template` option, as follows:

```
jpccconf bgdef export -f /tmp/businessgroup01.cfg -template
```

The output is shown below.

```
#Business Group Definition File Version=0001
#Business Group Definition File Code=

#[Business Group Data]
#Business Group Name=
#JP1 Resource Group Name=
#Host Name=
```

Each line in the template file begins with a hash mark (#). This indicates that the line is a comment line.

For details on the `jpccconf bgdef export` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

#### (b) Creating a business group definition file

Create a business group definition file by editing the output template file `/tmp/businessgroup01.cfg` as follows:

1. Open the `/tmp/businessgroup01.cfg` file in a text editor or similar.

2. Define the header part of the business group definition file.

Define the file header. In the header, define the syntax version of the business group definition file and the character code to use to create the file. These values are defined in the following part of the file header:

```
#Business Group Definition File Version=0001
#Business Group Definition File Code=
:
```

Delete the hash marks (#) at the beginning of these lines and edit the lines as follows:

```
Business Group Definition File Version=0001
Business Group Definition File Code=Shift_JIS
:
```

- **Business Group Definition File Version label**

This is the syntax version of the business group definition file.

The syntax version is a fixed value of 0001 which is entered in the template file by default.

You cannot omit this item.

- **Business Group Definition File Code label**

This is the character code used to create the business group definition file. Specify `Shift_JIS`, `EUC-JP`, `UTF-8`, `C`, or `GB18030`.

In this example, `Shift_JIS` is set as the character code.

You cannot omit this item.

3. Define the business group name, the JP1 resource group name (when using JP1 authentication mode), and the host name.

Define individual business groups. The definition of a business group is coded in the `Business Group Data` section. You must create a `Business Group Data` section for each business group definition.

When using PFM authentication mode

In this example, we define the business group `Accounting System A` that incorporates the hosts `keiri01` and `keiri02`.

Delete the hash marks (#) at the beginning of each line except the `JP1 Resource Group Name` label, and edit the lines as follows:

```
:
[Business Group Data]
Business Group Name=Accounting System A
#JP1 Resource Group Name=
Host Name=keiri01,keiri02
```

When using JP1 authentication mode

In this example, we associate the JP1 resource group `resource01` with the business group `Accounting System A` that incorporates hosts `keiri01` and `keiri02`.

Delete the hash marks (#) at the beginning of each line, and edit the lines as follows:

```
:
[Business Group Data]
Business Group Name=Accounting System A
JP1 Resource Group Name=resource01
Host Name=keiri01,keiri02
```

- **Business Group Name label**  
Define the business group name in 1 to 255 bytes. If the name includes spaces, enclose it in double quotation marks (").  
You cannot omit this item.
- **JP1 Resource Group Name label**  
When using JP1 authentication mode, specify the name of the JP1 resource group to associate with the business group. Only JP1 users who belong to the specified JP1 resource group will be able to access the business group.
- **Host Name label**  
Define the host names that belong to the business group in 1 to 128 bytes.  
When defining a business group containing multiple hosts, separate the host names with commas (,).

For details on the values you can specify, see the chapter on commands in the manual *JP1/Performance Management Reference*.

4. After making the necessary changes, save the `/tmp/businessgroup01.cfg` file.

## (2) Checking the business group definition file

Check the validity of the business group definition file you created. You can use the `jpccconf bgdef check` command to validate the contents of a business group definition file.

1. Log on to the host where PFM - Manager is installed.
2. Make sure that the PFM - Manager services are running.  
Use the `jpctool service list` command to find out whether the PFM - Manager services are running. If the services are not running, start the services now.
3. Execute the `jpccconf bgdef check` command.

Execute the command as follows:

```
jpccconf bgdef check -f /tmp/businessgroup01.cfg
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

If any errors are found in the business group definition file, the system generates an error message for the first error it finds, indicating the detail of the error and the line number in the file. Fix any errors by referring to the message contents.

For details on the `jpccconf bgdef check` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

## (3) Importing a business group definition file

Register the business groups in Performance Management by importing the business group definition file you created. Use the `jpccconf bgdef import` command to import the business group definition file.

1. Log on to the host where PFM - Manager is installed.
2. Make sure that the PFM - Manager services are running.  
Use the `jpctool service list` command to find out whether the PFM - Manager services are running. If the services are not running, start the services now.
3. Execute the `jpccconf bgdef import` command.

Execute the command as follows:

```
jpccconf bgdef import -f /tmp/businessgroup01.cfg
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

For details on the `jpccconf bgdef import` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

### 2.7.3 Using business groups defined in JP1/IM

You can use business groups defined in JP1/IM by exporting business group definition information from JP1/IM, and then validating and importing the information in Performance Management. You also need to add the JP1 permission levels that allow JP1 users to use Performance Management.

#### (1) Exporting business group definition information from JP1/IM

Use the `jclexport` command to export the business group information defined in JP1/IM. For details, see the *JP1/Integrated Management - Manager Configuration Guide*.

#### (2) Checking the business group definition information

Check the validity of the business group definition information you exported. You can use the `jpccconf bgdef check` command to validate business group definition information exported from JP1/IM.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpccconf bgdef check` command.

In this example, we check the validity of the business group definition information exported to the `/tmp/imb01` directory.

Execute the command as follows:

```
jpccconf bgdef check -im /tmp/imb01
```

If any errors are found in the business group definition information, the system generates an error message for the first error it finds, indicating the detail of the error and the line number in the file. Fix any errors in the JP1/IM business group settings by referring to the message contents.

For details on the `jpccconf bgdef check` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

#### (3) Importing business group definition information

Import the business group information you exported from JP1/IM into Performance Management. In this example, we import the business group definition information exported to the `/tmp/imb01` directory.

#### Important

When you execute the `jpccconf bgdef import -im` command in the procedure below, all business group information defined in Performance Management is deleted. This means that after the import process,

only the business groups exported from JP1/IM and then imported to Performance Management can be used.

1. Log on to the host where PFM - Manager is installed.
2. Make sure that the PFM - Manager services are running.  
Use the `jpctool service list` command to find out whether the PFM - Manager services are running. If the services are not running, start the services now.

3. Execute the `jpccconf bgdef import` command.

Execute the command as follows:

```
jpccconf bgdef import -im /tmp/imb01
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

For details on the `jpccconf bgdef import` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

## (4) Setting operating permissions for JP1 users

In JP1/IM, business groups are associated with a JP1 resource group, and you need to add the JP1 permission level `JP1_PFM_Operator` to the JP1 resource group associated with the business group. This permission allows JP1 users to operate Performance Management.

For details on how to assign operating permissions to JP1 users, see the *JP1/Base User's Guide*.

## 2.7.4 Using business groups

### (1) Checking business group definitions

Use the `jpccconf bgdef display` command to check the business group definitions.

1. Log on to the host where PFM - Manager is installed.
2. Make sure that the PFM - Manager services are running.  
Use the `jpctool service list` command to find out whether the PFM - Manager services are running. If the services are not running, start the services now.
3. Execute the `jpccconf bgdef list` command to check the business group names.

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

The output is shown below. In this example, you can see that `groupA`, `groupB`, and `groupC` are defined as business groups.

```
groupA
groupB
groupC
```

For details on the `jpccnfbgdef list` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

4. Execute the `jpccnfbgdef display` command to check the definitions of the business groups.

For example, to check the definition of the business group `groupA`, execute the command as follows:

```
jpccnfbgdef display -group groupA
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

The output is shown below. In this example, you can confirm that the business group contains `HostA` and `HostB`, and the JP1 resource group `resourceA` is associated with the business group.

```
KAVE05444-I Business group definitions will now be displayed.
Business Group Name      :groupA
JP1 Resource Group Name:resourceA#
Host Name:
  HostA
  HostB
```

#

Not output when you use PFM authentication mode.

For details on the `jpccnfbgdef display` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

## (2) Changing the business group configuration

### (a) Changing the configuration of business groups defined in Performance Management

You can change the configuration of business groups defined in Performance Management by exporting the business group definitions to a file, editing the file, and then importing the file into Performance Management.

This process uses the following commands:

- To export the business group definition information:

```
jpccnfbgdef export command
```

- To import the business group definition information:

```
jpccnfbgdef import command
```

1. Log on to the host where PFM - Manager is installed.

2. Make sure that the PFM - Manager services are running.

Use the `jpctool service list` command to find out whether the PFM - Manager services are running. If the services are not running, start the services now.

3. Execute the `jpccnfbgdef list` command and identify the name of the business group whose configuration you want to change.

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

The output is shown below. In this example, you can see that `groupA`, `groupB`, and `groupC` are defined as business groups.

```
groupA
groupB
groupC
```

For details on the `jpccconf bgdef list` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

4. Execute the `jpccconf bgdef export` command.

For example, execute the command as follows to export the definition information for business group `groupA` to the file `/tmp/businessgroup01.cfg`.

```
jpccconf bgdef export -f /tmp/businessgroup01.cfg -group groupA
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

For details on the `jpccconf bgdef export` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

5. Open the `/tmp/businessgroup01.cfg` file in a text editor or similar.

6. Edit the `/tmp/businessgroup01.cfg` file.

For details on how to edit the definitions in a business group definition file, see [2.7.2\(1\)\(b\) Creating a business group definition file](#).

7. Validate the contents of the `/tmp/businessgroup01.cfg` file.

Execute the command as follows:

```
jpccconf bgdef check -f /tmp/businessgroup01.cfg
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

If any errors are found in the business group definition file, the system generates an error message for the first error it finds, indicating the detail of the error and the line number in the file. Fix any errors in the file by referring to the message contents.

For details on the `jpccconf bgdef check` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

8. Execute the `jpccconf bgdef import` command.

Execute the command as follows:

```
jpccconf bgdef import -f /tmp/businessgroup01.cfg
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

For details on the `jpccconf bgdef import` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

## (b) Changing the configuration of business groups defined in JP1/IM

To change the configuration of a business group defined in JP1/IM, modify the definition in JP1/IM and then import the modified definition information into Performance Management. For details on how to do so, see [2.7.3 Using business groups defined in JP1/IM](#).



If changes to the business group configuration require that you remove a JP1 user with a business group assigned, remove `JP1_PFM_Operator` permission from the JP1 resource group associated with the business group assigned to the JP1 user. `JP1_PFM_Operator` is the permission level that allows the JP1 user to operate Performance Management.

For details on how to change the operating permissions of JP1 users, see the *JP1/Performance Management User's Guide*.

### (3) Deleting business groups

#### (a) Deleting business groups defined in Performance Management

Use the `jpccconf bgdef delete` command to delete business groups.

1. Log on to the host where PFM - Manager is installed.

2. Make sure that the PFM - Manager services are running.

Use the `jpctool service list` command to find out whether the PFM - Manager services are running. If the services are not running, start the services now.

3. Check the name of the business group you are deleting by executing the `jpccconf bgdef list` command.

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

The output is shown below. In this example, you can see that `groupA`, `groupB`, and `groupC` are defined as business groups.

```
groupA
groupB
groupC
```

For details on the `jpccconf bgdef list` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

4. Execute the `jpccconf bgdef delete` command.

For example, to delete the business group `groupB`, execute the command as follows:

```
jpccconf bgdef delete -group groupB
```

If PFM - Manager is running on a logical host, execute the command with the logical host name specified in the `-lhost` option.

For details on the `jpccconf bgdef delete` command, see the chapter on commands in the manual *JP1/Performance Management Reference*.

5. Confirm that the business group has been deleted by executing the `jpccconf bgdef list` command.

Execute the command in the same manner as in step 3.

The output is shown below. In this example, you can see that the business group `groupB` has been deleted.

```
groupA
groupC
```

## **(b) Deleting business groups defined in JP1/IM**

You can delete business groups defined in JP1/IM by deleting the business groups in JP1/IM, and then importing the modified group definitions into Performance Management. For details on how to do so, see [2.7.3 Using business groups defined in JP1/IM](#).

When you delete a business group defined in JP1/IM, delete the `JP1_PFM_Operator` permission level that allows the JP1 user to operate Performance Management from the JP1 resource group associated with the business group. Delete the permission level for each user.

For details on how to change the operating permissions of JP1 users, see the *JP1/Base User's Guide*.

# 3

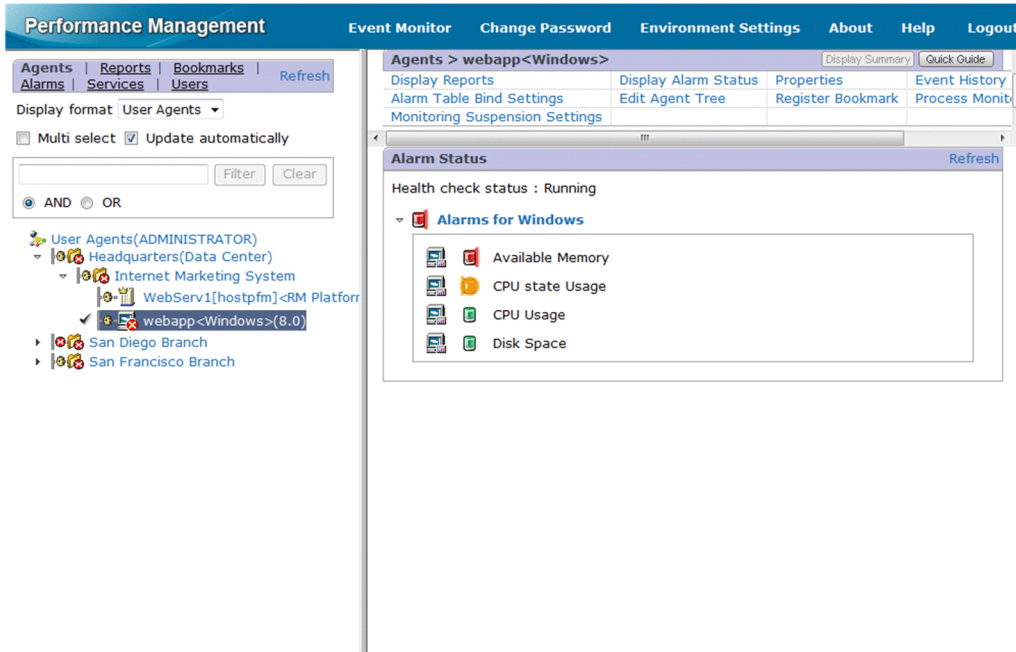
## Monitoring Agents

This chapter describes how to monitor agent operations by using the monitoring console.

## 3.1 Monitoring by using the Agents tree

You can monitor the status of agent operations in the Agents window of PFM - Web Console. The Agents tree window displays in a tree format the connection between PFM - Agent or PFM -RM agents and PFM - Manager. You can use icons to check the operating status of each agent.

Figure 3–1: Example of the Agents window



The icons in the Agents tree that appear in the navigation frame on the left side of the window indicate the status of PFM - Agent or PFM - RM operation. You can display related reports and check the alarm status and event history by selecting an agent in the Agents tree.

You can monitor by using the Agents tree in the following two formats:

- Monitoring by agent tree grouped for each product  
Use this format to monitor by using the Agents tree with items grouped in PFM - Agent product folders.
- Monitoring by using the Agents tree with items grouped for each logged-on user  
Use this format to monitor by using an Agents tree that is optionally created by each logged-on user. Users can create and freely compose folders in units such as system structures or organizations.

For details on the components in the Agents tree, see the chapter describing the navigation frame of the Main window in the manual *JPI/Performance Management Reference*.

Supplemental information:

- A user-created agent tree can contain a maximum of eight levels. You can create a maximum of 64 folders and 128 agents at the root level or in a folder.
- In the case of a tree organized by each product (when the selected display format is **Products**), the **Unknown** folder stores the PFM - RMs or PFM - Agents that are not registered in the Performance Management system. For details on how to register PFM - Agents or PFM - RMs, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.



## Tip

- You can use keywords to filter the information displayed in the navigation frame or the information frame. To filter the displayed components, enter part of a component name in the text box and click **Filter**. To remove the filter, click **Clear**.
- If **Multi select** is selected, clicking the root icon or a folder in the Agents tree selects or deselects all its subordinate nodes. If you click a folder in which all nodes are deselected or only some nodes are selected, all of the folder's subordinate nodes will be selected. If you click a folder whose nodes are all selected, all of the folder's subordinate nodes will be deselected. If the folder you clicked contains subfolders, the selection status of the nodes in those folders also changes. This means that you can change the selection status of every node in the tree by clicking the root icon.

### 3.1.1 Agent types

You can use the following three types of agents in Performance Management.

- Agent for PFM - Agent

This is an agent used by PFM - Agent to monitor a program.

Each agent corresponds to a different monitored program. That is, you must install a separate PFM - Agent agent for each program to be monitored.

- PFM - RM remote agent

This is an agent used by PFM - RM to monitor a program. This agent is created for each PFM-RM program to be monitored.

PFM - RM uses a single service to monitor multiple objects. This remote agent is a virtual agent that is used to monitor PFM - RM objects in the same way that the PFM - Agent agent is used to monitor programs.

- PFM - RM group agent

This is an agent used by PFM - RM to monitor multiple programs simultaneously. Like the remote agent, this is a virtual agent.

A group agent groups multiple remote agent sets in the same PFM - RM. Performance data from a group agent is a collection of performance data from each remote agent in the group. You can summarize the data in various ways, such as totaling or averaging the data.

## 3.2 Creating and editing an Agents tree in a Web browser

### 3.2.1 Creating an Agents tree

The process flow for creating a user-created Agents tree is as follows:

1. Create a folder to manage agents.
2. Place agents in each folder.



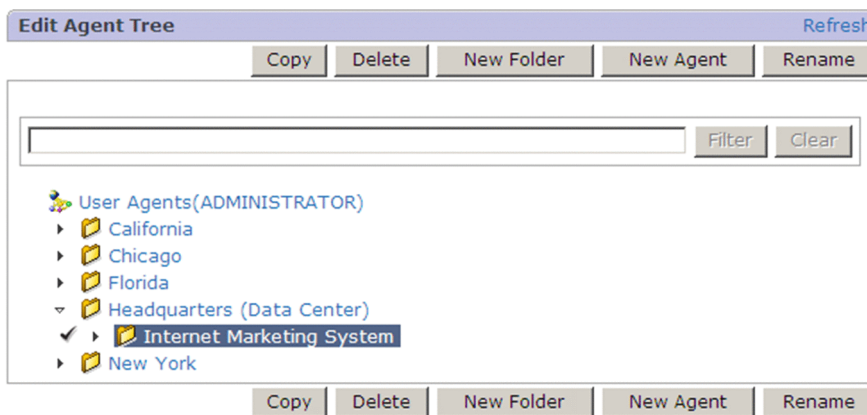
#### Tip

An Agents tree can be created for each logged-on user.

### (1) Creating a new agent management folder

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.  
In the navigation frame of the Agents window, **User Agents (logged-on-user-name)** is displayed at the root of the Agents tree.
  - When logging on for the first time:  
Only the root **User Agents (logged-on-user-name)** appears.
  - If the logged-on user has already created components in the Agents tree:  
All folders under the root appear.
3. In the method frame, choose the **Edit Agent Tree** method.  
The Edit Agent Tree window appears.
  - When logging on for the first time:  
Only the root **User Agents (logged-on-user-name)** appears in the information frame.
  - If the logged-on user has already created components in the Agents tree:  
All folders under the root appear.

Figure 3–2: Example of Edit Agents window





## Tip

To search for a particular agent, enter a search string in the text box and click **Filter**.

4. In the Agents tree displayed in the information frame, select a higher component of the folder to be created.

- When logging on for the first time:  
Select **User Agents** (*logged-on-user-name*).
- When the logged-on user has already created components in the Agents tree, select **User Agents** (*logged-on-user-name*) or a higher folder of the folder to be created.  
The selected component is marked with a checkmark.  
Select **User Agents** (*logged-on-user-name*) or a folder to activate the **New Folder** button.

5. Click the **New Folder** button.

6. In the Edit Agent Tree > New Folder window, enter a folder name in the **New name of the folder** field.

### New name of the folder

Enter the folder name using 1 to 64 single or double-byte characters. You can enter a combination of single and double-byte characters.

7. Click the **OK** button.

The newly created folder appears under **User Agents** (*logged-on-user-name*) or under the folder selected in step 4.

8. Repeat steps 1 to 7 to create folders as necessary.

## (2) Placing agents in a management folder

1. Log on to PFM - Web Console from the monitoring console Web browser.

2. In the navigation frame of the main window, choose the **Agents** tab.

The Agents window appears.

In the navigation frame, **User Agents** (*logged-on-user-name*) is displayed at the root of the Agents tree.

- When logging on for the first time:  
Only the Agent tree root **User Agents** (*logged-on-user-name*) appears.
- If the logged-on user has already created components in the Agents tree:  
All folders under the root appear.

3. In the method frame, choose the **Edit Agent Tree** method.

The Edit Agent Tree window appears.

- When logging on for the first time  
Only the root **User Agents** (*logged-on-user-name*) appears in the information frame.
- When the logged-on user has already created components of the Agents tree  
All folders under the root appear.

4. Select a folder in the Agents tree displayed in the information frame where you want to place agents.

Select a folder where you want to place agents. Select **User Agents** (*logged-on-user-name*) to place agents immediately under the root.

The selected component is marked with a checkmark.

Select a folder or **User Agents** (*logged-on-user-name*) to activate the **New Agent** button.

5. Click the **New Agent** button.

The Edit Agent Tree > New Agent window appears.

The Agents connected to the PFM - Manager appear in a product-based tree in the information frame.

Figure 3–3: Example of the Edit Agent Tree > New Agent window

The screenshot shows a dialog box titled "Edit Agent Tree > New Agent". At the top right is a "Refresh" button. Below the title bar are "OK" and "Cancel" buttons. The main area contains several options: a checked checkbox "Create a folder by using the host name", a collapsed "Destination Folder" section with a text box containing "User Agents(ADMINISTRATOR)/Headquarters/Marketing System /<HOSTNAME>", an unchecked checkbox "Display separately by business group", another unchecked checkbox "Display only unregistered agents" with a text box and "Filter" and "Clear" buttons, and radio buttons for "AND" (selected) and "OR". At the bottom is a tree view under "Products" with sub-items "HealthCheck", "RM Platform", and "Windows". A second set of "OK" and "Cancel" buttons is at the bottom right.

**Tip**

To filter the displayed agents, enter part of an agent name in the text box and click **Filter**. To remove the filter, click **Clear**.

If you select **Display only unregistered agents**, only agents that are not registered in the User Agents tree appear in the list. If you clear the check box, the list shows all the agents in the system.

Reference note:

Agents are listed by their service IDs. The format of the service ID depends on whether the product name display function is enabled. For example, if the host name for a PFM - RM Platform remote agent is `remmon`, its instance name is `inst01`, its monitored host name is `rma1`, and the product name display function is enabled, the service ID is displayed as `inst01[rma1@remmon]<RMPlatform>`. If the product name display function is disabled, the same service ID is displayed as `7A1inst01[rma1@remmon]`.

For details on service IDs, see the description of the service naming rules in the appendixes of the *JPI/Performance Management Planning and Configuration Guide*. For details on the product name display function, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.

6. In the Agents tree displayed in the information frame, select an agent to be placed in the folder selected in step 4. The selected agent is marked with a checkmark.

7. Click the **OK** button.

The agent selected in step 6 appears under the folder selected in step 4.



## 3.2.2 Editing the Agents tree

### (1) Copying a folder

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. In the Agents window, choose the **Edit Agents** method in the method frame.  
The Edit Agents window appears in the information frame, showing the Agents tree created by the logged-on user.
4. In the Agents tree displayed in the information frame, select a resource folder of copying.  
The selected folder is marked with a checkmark.
5. Click the **Copy** button.
6. In the Edit Agents > Copy [Select a destination] window, select the destination folder.  
The selected folder is marked with a checkmark.
7. Click the **OK** button.  
The folder selected in step 4 is copied to under the folder selected in step 6. This procedure also copies folders and agents that are under the copied folder.

### (2) Deleting a folder

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. In the Agents window, choose the **Edit Agents** method in the method frame.  
The Edit Agents window appears in the information frame, showing the Agents tree created by the logged-on user.
4. In the information frame, select a folder to be deleted from the Agents tree.  
The selected folder is marked with a checkmark.
5. Click the **Delete** button.
6. Click **OK** in the confirmation dialog box.  
The folder selected in step 4 is deleted.  
This procedure also deletes folders and agents that are under the deleted folder.

### (3) Renaming a folder

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. In the Agents window, choose the **Edit Agents** method in the method frame.  
The Edit Agents window appears in the information frame, showing the Agents tree created by the logged-on user.
4. In the Agents tree in the information frame, select a folder to be renamed.  
The selected folder is marked with a checkmark.

5. Click the **Rename** button.
6. In the Edit Agents > Rename window, enter the new folder name in **New name of the folder**.

#### **New name of the folder**

Enter the folder name using 1 to 64 single or double-byte characters. You can enter a combination of single and double-byte characters.

7. Click the **OK** button.  
The changed name of the folder selected in step 4 takes effect.

## **(4) Copying an existing agent to a different folder**

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. In the Agents window, choose the **Edit Agents** method in the method frame.  
The Edit Agents window appears in the information frame, showing the Agents tree **User Agents** (*logged-on-user*).
4. In the information frame, select an agent to be copied in the Agents tree.  
The selected agent is marked with a checkmark.

Note:

You can copy one agent at a time. You cannot specify multiple agents at the same time.

5. Click the **Copy** button.
6. Select the folder that is the copy destination.  
The selected folder is marked with a checkmark.
7. Click the **OK** button.  
The agent selected in step 4 is copied to the folder selected in step 6.

## **(5) Deleting an agent**

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. In the Agents window, choose the **Edit Agents** method in the method frame.  
The Edit Agents window appears in the information frame, showing the Agents tree **User Agents** (*logged-on-user*).
4. In the information frame, select an agent to be deleted from the Agents tree.  
The selected agent is marked with a checkmark.
5. Click the **Delete** button.
6. Click **OK** in the confirmation dialog box.  
The agent selected in step 4 is deleted.

### 3.2.3 Limiting the agents available to users with general user permission

You can limit the agents that appear to users with general user permission in the Agents window of PFM - Web Console.

You can enable this setting by specifying on for `agentTreeAccessLimit` parameter in the initialization file (`config.xml`). For details on the initialization file (`config.xml`), see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

After you enable this setting, the **Display format** drop-down list no longer appears in the Agents window of PFM - Web Console, and the display format is fixed as **User Agents**. You cannot select **Products** as the display format.

You cannot change the contents of the User Agents tree in the Agents window. To edit the agents displayed in the User Agents tree after you enable the setting, use the `jpccconf agttree` command. For details on how to edit the Agents tree using the `jpccconf agttree` command, see [3.3 Using commands to create and edit an Agents tree](#).

## 3.3 Using commands to create and edit an Agents tree

You can use the `jpccconf agttree` command to create and edit an Agents tree. In the examples in this section, the command is executed in interactive mode. However, the `jpccconf agttree` command can also be executed in non-interactive mode. For details on the `jpccconf agttree` command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

### 3.3.1 Creating an Agents tree

1. Export the template of the Agents tree definition file.

To export the template file, execute the `jpccconf agttree export` with the `-template` option specified. For example:

```
jpccconf agttree export -template -f agttree_def.xml
```

2. Edit the exported Agents tree definition file.

For details on the format of the Agents tree definition file, see the chapter on commands in the manual *JPI/Performance Management Reference*.

The following is an example of the contents of an Agent tree definition file:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE tree SYSTEM "agttree_param.dtd">

<tree owner="pfm-user">
  <folder name="Test Company">
    <folder name="Business Department">
      <agent name="7A1inst_BD[tHOST_01@host_111]"/>
    </folder>
    <folder name="Development Department">
      <agent name="7A1inst_DD[tHOST_02@host_111]"/>
      <agent name="7A1inst_DD[tHOST_03@host_111]"/>
    </folder>
    <agent name="TA1host_111"/>
  </folder>
  <agent name="TA1host_999"/>
</tree>
```

3. Import the Agents tree definition file.

Use the `jpccconf agttree import` command to import the Agents tree definition file. For example:

```
jpccconf agttree import -f agttree_def.xml
```

If you want to specify an agent not recognized by Performance Management (an agent that does not appear in the Products tree), specify the `-nocheck` option. If you do not specify the `-nocheck` option, processing stops when Performance Management encounters an agent it does not recognize.

In a logical host environment, specify the logical host name in the `-lhost` option.

The Agents tree you created appears in the Agents window when you refresh the window contents or you log off from PFM - Web Console and log on again.

## 3.3.2 Editing an Agents tree

1. Export the Agents tree information to an Agents tree definition file.

To export Agents tree information, execute the `jpccconf agttree export` command with the user who defined the Agent tree you are outputting specified in the `-owner` option.

```
jpccconf agttree export -owner pfm-user -f agttree_def.xml
```

In a logical host environment, specify the logical host name in the `-lhost` option.

2. Edit the Agents tree definition file you exported.

For details on the format of the Agents tree definition file, see the chapter on commands in the manual *JPI/Performance Management Reference*.

3. Import the Agents tree definition file.

To import the Agents tree definition file, execute the `jpccconf agttree import` command. For example:

```
jpccconf agttree import -f agttree_def.xml
```

If you want to specify an agent not recognized by Performance Management (an agent that does not appear in the Products tree), specify the `-nocheck` option. If you do not specify the `-nocheck` option, processing stops when Performance Management encounters an agent it does not recognize.

In a logical host environment, specify the logical host name in the `-lhost` option.

The changes to the Agents take effect when you refresh the Agents window, or you log out from PFM - Web Console and log in again.

## 3.4 Monitoring the status of agent operations

You can check the status of each agent by using the Agents tree icons displayed in the navigation frame of the Agents window.

### 3.4.1 Checking the status of agents






You can check the status of agents by using the Agents tree icons displayed in the navigation frame of the Agents window.

#### Note

You cannot check the status of the group agent.

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. From the **Display format** pull-down menu in the navigation frame of the Agents window, choose the display format for the Agents tree.
  - When **User Agents** is selected:  
**User Agents** (*logged-on-user-name*) is displayed at the root of the Agents tree.
  - When **Products** is selected:  
**Products** is displayed at the root of the Agents tree.
4. Check the icon displayed on the left of the Agents tree.

Table 3–1: Status indicated by folder icons

Icon	Description
	This icon indicates that all of the alarms in the alarm table bound to an agent under the folder are in normal status.
	This icon indicates that no alarm in the alarm table bound to an agent under the folder is in abnormal status and at least one alarm is in warning status.
	This icon indicates that at least one alarm in the alarm table bound to an agent under the folder is in abnormal status.
	This icon indicates that no alarm in the alarm table bound to an agent under the folder is in Abnormal status or in Warning status and at least one agent is under monitoring suspension.
	This icon indicates the operating status of the agents in the folder. <sup>#</sup>







Note:

The folder icon indicates the most severe status level among those of the agents in the folder. The severity levels starting from the most severe are: Abnormal, Warning, Suspended, and Normal.

#

For details on the icons that indicate the health check status of an agent, see [Table 3-3 Health check status indicated by icons](#).








Table 3–2: Status indicated by agent icons

Icon	Description
	This icon indicates that all of the alarms in the alarm table bound to an agent are in normal status.
	This icon indicates that no alarm in the alarm table bound to an agent is in abnormal status and at least one alarm is in warning status.
	This icon indicates that at least one alarm in the alarm table bound to an agent is in abnormal status.
	This icon indicates that the status of monitoring for this agent is Suspended.
 (when <b>Display format</b> is <b>User Agents</b> )	This icon indicates that the agent is unavailable for one of the following reasons: <ul style="list-style-type: none"> <li>Service information for the agent was deleted, and the changes were applied to PFM - Web Console by the <code>jpccconf service sync</code> command</li> <li>As a result of changes to the business group configuration, the user no longer has permission to view the agent</li> </ul>
	This icon indicates the operating status of the agent.#

#

For details on the icons that indicate the health check status of an agent, see [Table 3-3 Health check status indicated by icons](#).

Table 3–3: Health check status indicated by icons

Icon	Description
	Not Supported
	Running
	Monitoring suspended
	Incomplete
	Stopped
	Unconfirmed#
	Host Not Available

Note:

For details on the status indicated by each health check event icon, see [16.2.2 Checking operating statuses](#).

#

For details about how to respond to a Not Supported or Unconfirmed health check status for an agent, see [17.2.6\(2\) The operating status of a server or agent is Unconfirmed or Not Supported](#).

### 3.4.2 Checking the status of alarms

You can check the status of each alarm defined in the alarm table bound to each agent. You can also display reports that are bound to alarms.







## Note:

You cannot display the status of alarms if an alarm table is not bound to agents. For details on how to bind an alarm table to agents, see [6.6.1 Changing the association between an alarm table and a monitoring agent](#).

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. From the **Display format** pull-down menu in the navigation frame of the Agents window, choose the display format for the Agents tree.
  - When **User Agents** is selected:  
**User Agents** (*logged-on-user-name*) is displayed at the root of the Agents tree.
  - When **Products** is selected:  
**Products** is displayed at the root of the Agents tree.
4. In the Agents tree of the navigation frame, select the agent for which you want to check the alarm status. The selected agent is marked with a checkmark.
5. Select the **Display Alarm Status** method in the method frame.  
The Alarm Status window appears.  
A list of alarms appears displaying alarms defined in the alarm table that is bound to the agent selected in step 4. You can check the status of alarms by examining the color of the alarm icons.






### Alarm table status indicator icons

In the alarm table, the icon to the left of the alarm table name indicates the status of greatest importance. The icon color represents the status of the alarm table as follows:


-  : Indicates that the alarm table is expanded (with the definitions shown).
-  : Indicates that the alarm table is collapsed (with the definitions hidden).
-  (Green): This icon indicates normal status.
-  (Yellow): This icon indicates warning status.
-  (Red): This icon indicates abnormal status.
-  : This icon indicates monitoring-suspended status.

### Alarm icons

An alarm icon appears to the left of each alarm name. The icon color represents the alarm status. The status of alarms indicated by icon colors are as follows:

-  (gray): Indicates that the alarm is inactive.
-  (green): Indicates normal status.
-  (yellow): Indicates warning status.
-  (red): Indicates abnormal status.
-  #: Always appears regardless of the alarm status.




-  : Indicates monitoring-suspended status.

# Only when **Always notify** is selected in the alarm definition

Reference note:

The color of an alarm icon changes based on the thresholds and other conditions that you set in the Alarms window. For details on these thresholds and conditions, see [6.4 Setting alarms using the Web browser \(Alarms tree\)](#) and [6.7 Setting alarms by using commands](#).

Report icons (for example, ) appear on the left of the alarm when you have bound a report to alarms. Click the report icon to display related reports.

For details on how to bind a report to alarms, see [5.7.1\(2\) Displaying a report associated with an alarm](#).

A message indicating the health check status also appears.

For details on each health check status, see [16.2.2 Checking operating statuses](#).

### 3.4.3 Displaying reports

Items that display performance data collected in each agent in graphical formats such as graphs and tables are called *reports*.

You can display various reports for each agent in the Agents window of PFM - Web Console.

Templates, called *monitoring templates*, are available for reports to be displayed. You can also create your own reports as desired. For details on how to display and create reports, see [5.7 Displaying reports](#) or [5.8 Displaying combination reports](#).

### 3.4.4 Displaying event history

You can view a history of events that occurred in the Performance Management system. You can check the event history for each agent in the Event History window. You can also output event history data to a text file in CSV or HTML format.

For details, see [7.2 Displaying the event history](#).

### 3.4.5 Using summary display to check the operating status

You can view a summary of results for operating status, stopped status, and Normal and Abnormal status counts to check the operating status of servers and agents, as well as the alarm status of agents. You can also view alarm and agent events with Abnormal status and Warning status. A view showing summarized results together with Abnormal and Warning status events is called a *summary display*.

#### (1) Prerequisite conditions

Requirements for server operating status monitoring

To be able to monitor server operating status, the version of the PFM - Manager for the connection destination must be 08-11 or later, the version of PFM - Web Console must be 09-00 or later, and the health check function must be enabled.

## Requirements for agent operating status monitoring

To be able to monitor agent operating status, the version of the PFM - Manager for the connection destination must be 08-11 or later, the version of PFM - Web Console must be 09-00 or later, and the health check function must be enabled. In addition, you must set the following health check agent properties in the Service Properties window of the PFM - Web Console Services tree window:

- **Monitoring Level in Health Check Configurations:** Service

For details on the health check function, see [16.2 Using the health check function to check the operating status of monitoring agents and their hosts](#).

## (2) Agent types for which summary displays are supported

Table 3–4: Types of agents for which summary displays are supported

Agent type	Areas in the System Operational Status Summary window		
	Server Operational Status	Agent Operational Status	Agent Alarm Status
PFM - Agent	Yes	Yes	Yes
Remote agent	Yes	Yes	Yes
Group agent	No	No	Yes
Remote Monitor Collector service	Yes	Yes	No

Legend:

Yes: Count supported

No: Count not supported

Summary displays are not supported for the following agents:

- Any agent that has been deleted from the Products tree in the Agents tree window using the `jpctool service delete` command, but remains in the User Agents tree.
- Any agent that was registered by the `jpccconf agttree import` command with the `-nocheck` option specified, but is not yet recognized by Performance Management
- Any agent that does not belong to a business group available to the user, but remains in the User Agents tree  
To apply the results of the `jpctool service delete` command to the contents of the Products tree, execute the `jpctool service sync` command after you execute the `jpctool service delete` command. To apply the results to the contents of the User Agents tree, use the Edit Agents method in the method frame to delete the agents manually.

## (3) Procedure for displaying a summary

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, select the Agents tree tab.
3. From the **Display format** pull-down menu in the navigation frame of the Agents window, choose the display format for the Agents tree.
  - When **User Agents** is selected:  
The Agents tree that has **User Agents** (*logged-on-user-name*) as the root appears.
  - When **Products** is selected:  
The Agents tree that has **Products** as the root appears.

4. In the navigation frame, select the folders to be counted for the summary display.

Depending on whether you select the root of the Agents tree, or you select a desired folder other than the root, the counting unit and counting range for summary display differ. For details on the counting unit and counting range for summary displays, see [3.4.5\(5\) Counting unit and counting range for a summary display](#).

5. From the method frame, select the **View Summary** button.

The following describes the items displayed in the Server Operational Status, Agent Operational Status, and Agent Alarm Status areas of the System Operational Status Summary window.

- ▾ : Indicates that an Operational Status or Monitoring Status view is currently displayed.
- ▶ : Indicates that an Operational Status or Monitoring Status view is not currently displayed.

**Table 3–5: Items displayed in the Server Operational Status and Agent Operational Status areas of the System Operational Status Summary window**

Item	Meaning
Pie chart	<p>A pie chart showing the operating status of the servers or agents in the folder selected in the navigation frame. The meanings of the colors are as follows:</p> <ul style="list-style-type: none"> <li>• Green: Percentage of operating servers or agents.</li> <li>• Red: Percentage of stopped servers or agents.</li> <li>• Blue: Percentage of servers or agents with Unconfirmed status<sup>#1</sup>.</li> <li>• Gray: Percentage of servers or agents with monitoring-suspended status.</li> </ul> <p>For details on operating statuses, see <a href="#">3.4.5(4) Operational status classifications</a>.</p>
Table	<p>A table listing the operating status of the servers or agents in each folder selected in the navigation frame. The meanings of the items in a table are as follows:</p> <ul style="list-style-type: none"> <li>• Number operating: Number of servers or agents that are operating normally.</li> <li>• Number stopped<sup>#2</sup>: Number of servers or agents that are currently stopped (if the number stopped is one or greater, the cell is colored red).</li> <li>• Total: Total number of servers or agents (including those with Unconfirmed status).</li> <li>• Operating rate: Percentage of operating servers or agents (green indicates the percentage with Operating status, red indicates the percentage with Stopped status, blue indicates the percentage with Unconfirmed status<sup>#1</sup>, and gray indicates the percentage with monitoring-suspended status).</li> </ul> <p>The table shows the servers or agents with the five largest stopped counts, in descending order. The remaining servers are shown as Others.</p> <p>You can specify in the initialization file (<code>config.xml</code>) the number of servers or agents to be displayed. For details on the <code>config.xml</code>, see the chapter that describes installation and setup in the <i>JP1/Performance Management Planning and Configuration Guide</i>.</p>
[User tree view] check box	<p>This check box appears in the <b>Agent Operational Status</b> area when you select <b>User Agents</b> in the Agents tree. Selecting this check box displays the operating status at the level of folders that the logged-on user has created in the Agents tree.</p>
[Product type view] check box	<p>This check box appears in the <b>Agent Operational Status</b> area when you select <b>User Agents</b> in the Agents tree. Selecting this check box displays the operating status at the level of folders grouped according to the product (PFM - Agent or PFM - RM) with which they are associated.</p>

#1:

For details on how to take action when operational statuses become unknown, see [17.2.6\(2\) The operating status of a server or agent is Unconfirmed or Not Supported](#).

#2:

When the Server Operational Status area contains one or more stopped servers, you can display the Stopped Host List window by clicking the number of stopped servers. If you do this, you can check the host names of the stopped servers.

Table 3–6: Items displayed in the Agent Alarm Status area of the System Operational Status Summary window

Item	Description
Pie chart	<p>A pie chart showing the alarm monitoring status of agents in each folder selected in the navigation frame. Each color in the chart indicates an alarm status<sup>#</sup>. The meanings of the colors are as follows:</p> <ul style="list-style-type: none"> <li>• Green: Percentage of agents with Normal alarm status.</li> <li>• Yellow: Percentage of agents with Warning alarm status.</li> <li>• Red: Percentage of agents with Abnormal alarm status.</li> <li>• Gray: Percentage of agents with monitoring-suspended status.</li> </ul> <p>The numbers in the pie chart indicate the number of agents for each alarm status. The numbers do not indicate the number of bound alarms.</p>
Table	<p>A table showing the alarm monitoring status of agents in the folder selected in the navigation frame. The meanings of the items in a table are as follows:</p> <ul style="list-style-type: none"> <li>• Normal count: Number of agents with Normal alarm status.</li> <li>• Warning count: Number of agents with Warning alarm status.</li> <li>• Abnormal count: Number of agents with Abnormal alarm status (if the number of Abnormal alarm status agents is one or greater, the cell is colored red).</li> <li>• Status ratio: Alarm event status ratio (green indicates the percentage with Normal status, yellow indicates the percentage with Warning status, red indicates the percentage with Abnormal status, and gray indicates the percentage with monitoring-suspended status).</li> </ul> <p>The table shows agents with the five greatest Abnormal status counts in the Alarm Monitoring Status view, in descending order. The remaining agents are shown as Others.</p> <p>You can specify the number of alarms to be displayed by setting the <code>maxDisplayAlarm</code> parameter in the initialization file (<code>config.xml</code>). For details on the <code>config.xml</code>, see the chapter that describes installation and setup in the <i>JPI/Performance Management Planning and Configuration Guide</i>.</p>

#

The alarm status is determined as follows:

- Normal
  - All bound alarms show a Normal status or there are no bound alarms.
- Warning
  - No bound alarm shows an Abnormal status, but at least one bound alarm shows a Warning status.
- Abnormal
  - At least one bound alarm shows an Abnormal status.
- Monitoring suspended
  - No bound alarm shows an Abnormal or Warning status, but at least one agent shows a Suspended status.

When the **Always notify** check box is selected for an alarm, the alarm always shows a Normal (green) status, because the alarm is not evaluated. However, remote and group agents are evaluated. The Remote Monitor Collector service is not evaluated because an alarm cannot be bound to it and it is not counted as a parameter in the pie chart.

If more than one alarm is bound to a single agent, these alarms are evaluated in order of priority. The priority starting from the highest is abnormal, warning, and normal.

Reference note:

The number of agents is counted as follows:

(Example 1) An agent has six alarms bound to it, where two alarms each show Normal, Warning, and Abnormal statuses.

The agent is classified with an Abnormal status of the highest priority. Thus, the agent is counted as an Abnormal agent.

(Example 2) An alarm for which the **Always notify** check box is selected is bound and the alarm status is Abnormal.

An alarm status for which the **Always notify** check box is selected is classified as Normal. Thus, the agent is counted as a Normal agent.

You can check for Abnormal and Warning alarm events and agent events in the **Events** area of the System Operational Status Summary window. Unlike the Event Monitor window that displays all alarm and agent events that have been issued, the Events view displays only those alarms and agent events that have been issued with an Abnormal or Warning status and are currently pending. Any alarm event that is returning to Normal status is not shown. For details on the contents of each event, see [7. Displaying Events](#) or the description of the Event Monitor window in the manual *JP1/Performance Management Reference*.

The target alarms of the Agent Alarm Status window are those for which the **Always notify** check box is not selected. For details, see [6.9.3 Notes on evaluating alarms](#).

## (4) Operational status classifications

### (a) Operating statuses in the Server Operational Status area of the System Operational Status Summary window

The operating statuses displayed in the **Server Operational Status** area are based on the health check results from an agent monitoring the server. The health check results for the server are classified into four operating statuses: Operating, Stopped, Unconfirmed, and Suspended.

In the **Server Operational Status** area, a single operating status is shown for each server. If more than one agent monitors a single server, the health check results from the agents might differ. In such a case, the health check result determined to have the highest priority in the range based on [3.4.5\(5\) Counting unit and counting range for a summary display](#) appears as the operating status of the server in the Server Operational Status area.

Table 3–7: Agent health check results, resulting operated statuses and priority levels

Agent type	Health check result	Judgment of operational status	Judgment priority
<ul style="list-style-type: none"> <li>• PFM - Agent</li> <li>• Remote Monitor Collector service</li> </ul>	Host Not Available	Stop	1
	Not Supported	Running	2
	Running		3
	Incomplete		4
	Stopped		5
	Unconfirmed		6
Remote agent	Host Not Available	Stop	7
	Running	Running	8
	Incomplete		9
<ul style="list-style-type: none"> <li>• PFM - Agent</li> <li>• Remote Monitor Collector service</li> <li>• Remote agent</li> </ul>	Suspended	Monitoring suspended	10
Remote agent	Unconfirmed	Unknown	11
	Not Supported		12

The following is an example of where the health check results from a PFM - Agent differ from those of a remote agent, while both are monitoring the same server.

In this example, the following health check results are assumed:

- The health check result from the PFM - Agent is Host Not Available.  
This health check result is determined to have priority level 1.
- The health check result from the remote agent is Not Supported.  
This health check result is determined to have priority level 12.

The operating status for the server is determined as follows:

- If PFM - Agent and the remote agent are in the same folder  
For both the pie chart and the table, Host Not Available with the higher priority is selected. Therefore, the operating status of the server is Stopped.
- If PFM - Agent and the remote agent are in different folders  
For the pie chart, Host Not Available with the higher priority is selected. Therefore, the operating status of the server is Stopped.  
For the table, the result depends on the folder where the agent is located. A Host Not Available status is selected in the folder where PFM - Agent is located. Therefore, the operating status of the server is Stopped. A Not Supported status is selected in the folder where the remote agent is located. Therefore, the operating status of the server is Unconfirmed.

## (b) Operating statuses in the Agent Operational Status area of the System Operational Status Summary window

The operating statuses displayed in the **Agent Operational Status** area are based on the health check results from an agent. The health check results are classified into four operating statuses: Operating, Stopped, Unconfirmed, and Suspended.

Table 3–8: Agent health check results and resulting operating statuses

Agent type	Health check result	Judgment of operational status
<ul style="list-style-type: none"> <li>• PFM - Agent</li> <li>• Remote agent</li> <li>• Remote Monitor Collector service</li> </ul>	Running	Running
	Incomplete	Stop
	Stopped	
	Host Not Available	
	Not Supported	Unknown
	Unconfirmed	
	Suspended	Monitoring suspended

## (5) Counting unit and counting range for a summary display

Table 3–9: Counting units and counting range for a summary display

Selected folder in the Agents tree	Pie graph /table	Counting unit	Counting range
Desired folder	Pie graph	Selected folder	All of the agents under the selected folder

Selected folder in the Agents tree	Pie graph /table	Counting unit	Counting range
Desired folder	Table	Folders directly under the selected folder (The selected folder will be counted as <b>Other</b> .)	All of the agents under the folders directly under the selected folder (The agents directory under the selected folder will be counted as <b>Other</b> .)

The following figures show examples of summarized units and ranges for summarized display.

Figure 3–4: Example of Summarized units and ranges for summary display (when root is selected)

**Performance Management** | Event Monitor | Change Password | Environment Settings | About | Help | Logout

Agents | Reports | Bookmarks | Refresh  
Alarms | Services | Users

Display format: User Agents  
 Multi select  Update automatically  
 Filter   
 AND  OR

**Folder > User Agents** | Display Summary | Quick Guide  
 Event History | Edit Agent Tree | Monitoring Suspension Settings

**System Operational Status Summary** | Refresh | Stop  
 Display operational status of filtered results  
 Refresh date: 07 15 2014 10:42:39 GMT+09:00

**Server Operational Status** | Stopped (1) / Total (4)

	Server operational status			Ru
	Running	Stopped	Total	
San Diego Branch	3	1	4	100%
Headquarters(Data Center)	1	0	2	100%
San Francisco Branch	2	0	2	100%

● Running: 3  
● Stopped: 1

**Agent Operational Status** | Stopped (1) / Total (5)

User tree view  Product type view

	Agent operational status			Ru
	Running	Stopped	Total	
San Diego Branch	3	1	4	100%
Headquarters(Data Center)	1	0	2	100%
San Francisco Branch	2	0	2	100%

● Running: 3  
● Stopped: 1  
● Suspended: 1

**Agent Alarm Status** | Abnormal count (1) / Total (4)

	Alarm monitoring status		
	Normal count	Warning count	Abnormal count
San Diego Branch	2	1	1
Headquarters(Data Center)	1	0	0
San Francisco Branch	1	1	0

● Normal: 2  
● Warning: 1  
● Abnormal: 1

**Event**

	Date and Time	Agent	Report	Alarm	Message
	07 15 2014 10:42:00	webapp3<Windows>	n/a	n/a	State change
	07 15 2014 10:42:00	webapp3<Windows>	-		CPU is at 2.084406
	07 15 2014 10:41:00	hostpfm<Windows>	n/a	n/a	State change
	07 15 2014 10:41:00	hostpfm<Windows>	-		CPU is at 22.38765
	07 15 2014 10:39:31	webapp<Windows>	n/a	n/a	HC:Active , Alarm:



Figure 3–5: Example of Summarized units and ranges for summary display (when a folder is selected)

The screenshot shows the Performance Management console interface. The main content area displays the 'System Operational Status Summary' for the 'Headquarters(Data Center)' folder. It includes a pie chart showing 1 Running (green), 0 Stopped (red), and 1 Suspended (grey) units. Below the chart is a table for 'Server operational status' for the 'Internet Marketing System'.

	Running	Stopped	Total	Run
Internet Marketing System	1	0	2	1

Below this is the 'Agent Operational Status' section, which also shows a pie chart and a table for 'Agent operational status' for the 'Internet Marketing System'.

	Running	Stopped	Total	Run
Internet Marketing System	1	0	2	1

The 'Agent Alarm Status' section shows a pie chart and a table for 'Alarm monitoring status' for the 'Internet Marketing System'.

	Normal count	Warning count	Abnormal count
Internet Marketing System	1	0	0

At the bottom, there is an 'Event' table with the following data:

Date and Time	Agent	Report	Alarm	Message
07 15 2014 10:39:31	webapp<Windows>	n/a	n/a	HC:Active , Alarm:A

## (6) Printing a summary display

To print a summary display, click the **Stop** button on the System Operation Status Summary Monitoring window and click the **Print** button.

### 3.4.6 Displaying agent properties

You can display the properties of each agent (Collector service) to view settings of data collection intervals and collecting conditions. You cannot change property settings.

1. Log on to PFM - Web Console from the monitoring console Web browser.
2. In the navigation frame of the main window, choose the **Agents** tab.



3. From the **Display format** pull-down menu in the navigation frame of the Agents window, choose the display format for the Agents tree.
  - When **User Agents** is selected:  
**User Agents** (*logged-on-user-name*) is displayed at the root of the Agents tree.
  - When **Products** is selected:  
**Products** is displayed at the root of the Agents tree.
4. In the Agents tree of the navigation frame, select the agent whose properties you want to display.  
 The selected agent is marked with a checkmark.
5. In the method frame, choose the **Properties** method.  
 The Service Properties window appears.  
 The tree appears at the top of the information frame. The properties of the node selected in the tree appear at the bottom of the information frame, allowing you to view the settings for data collection intervals and conditions.  
 Displayed property settings differ depending on each agent. For details on property settings, see the appendixes of appropriate agent manual.

### 3.4.7 Editing agent properties

Users whose accounts have administrator user permissions can modify the properties in the Services window. For details, see [4. Managing Operation Monitoring Data](#).

### 3.4.8 Distributing agent properties as a batch

Agent properties can be distributed as a batch to any services with the same product name and data model version. This feature has the following benefits:

- When managing multiple agents of the same type, you can define the same settings for each agent as a batch
- When you add a new agent, it can be configured with the same settings as existing agents.

The following table lists the nodes whose properties can be distributed as a batch.

Table 3–10: Nodes whose properties can be viewed and selected when performing batch distribution

Service	Node name	Description
Agent Collector and Remote Monitor Collector	JP1 Event Configurations	These nodes contain the properties that define the conditions for issuing JP1 events. For details, see <a href="#">12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring</a> .
	Detail Records	These nodes contain the properties that define how performance data is recorded. For details, see <a href="#">4. Managing Operation Monitoring Data</a> .
	Interval Records	
	Log Records	
	Restart Configurations	These nodes contain the properties that configure automatic restart of PFM services. For details on automatic restart of PFM services, see <a href="#">16.4 Using the PFM service automatic restart functionality to restart PFM services</a> .

Service	Node name	Description
Agent Collector and Remote Monitor Collector	Node count variation property <sup>#1</sup>	These nodes contain the properties for which the number of nodes increases or decreases. The properties subject to batch distribution differ depending on the type of agent. For details, see the appendixes of the appropriate PFM - Agent or PFM - RM manual.
Agent Store and Remote Monitor Store <sup>#2</sup>	Retention	These nodes contain the properties that define how performance data is stored. For details, see <a href="#">4. Managing Operation Monitoring Data</a> .
	RetentionEx	
	Disk Usage	
	Configuration	
Remote agent and group agent	Detail Records <sup>#3</sup>	These nodes contain the properties that define how performance data is recorded. For details, see <a href="#">4. Managing Operation Monitoring Data</a> .
	Interval Records <sup>#3</sup>	
	Log Records <sup>#3</sup>	

#1

You must be using version 08-11 or later of PFM - Manager and PFM - Web Console to perform batch distribution of properties for which the number of nodes increases or decreases.

#2

Whether properties can be distributed from one Agent Store or Remote Monitor Store service to another depends on the versions of the Agent Store and Remote Monitor Store services and the Store database serving as the source and destination in the distribution process. For details, see [3.4.8\(2\) Property distribution capability by Agent Store and Remote Monitor Store versions](#).

#3

Only the Log property can be distributed.

Properties cannot be distributed among the Remote Monitor Collector service and the remote or group agents.

## (1) Procedure for distributing agent properties

- Log on to PFM - Web Console from the monitoring console Web browser.  
Log on to a user account that has administrator user permissions.  
You must have administrator user permissions to use the Services window.
- In the navigation frame of the main window, select the **Services** tab.
- In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.  
The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by the service ID. For details on the service ID, see the appendix describing service naming rules in the *JP1/Performance Management Planning and Configuration Guide*, and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.  
The format of the service ID depends on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *JP1/Performance Management Planning and Configuration Guide*.
- Select the distribution source agent node.  
You can select any of the following services to be the distribution source node:
  - Agent Collector and Remote Monitor Collector

- Agent Store and Remote Monitor Store
- Remote agent
- Group agent

The selected node is marked with a checkmark.

5. In the method frame, select the **Distribute Property** method.

The Distribute Properties > Select Service window appears, showing a list of services available for selection as the distribution destination. The list is populated with services that have the same product name and data model version as the distribution source.

6. Select the distribution destination service.

If access control based on business groups is enabled, you can refine the list of distribution destination services by business group.



**Tip**

You can search for a service by entering a search string in the text box and clicking **Filter**.

7. Click the **Next** button.

The Distribute Properties > Select Service window appears, showing a list of properties you can distribute to the distribution destination, with check boxes you can use to select the properties.

8. Select the properties to distribute.

When you select a node in the tree, a list of the properties you can select appears at the bottom of the information frame.

Click the **Select All** button to select all of the properties in the list. Click the **Unselect All** button to clear all selections.

If you want to select a different distribution destination service, click the **Back** button in the Distribute Properties > Select Property window. You are returned to the Distribute Properties > Select Service window in step 6.

9. Click the **Finish** button.

The batch distribution process begins, and the Distribute Property > Progress Reports window appears.

When batch distribution to a service has finished, **OK** appears in the **Property Distribution** column for that service.

The **OK** button becomes available when batch distribution has finished for all services.



**Note**

In step 8, you can select additional properties to distribute by repeating the process of selecting another node in the tree and selecting the properties to distribute from that node, before clicking the **Finish** button.

10. Click the **OK** button.

The contents of the information frame are cleared.

## (2) Property distribution capability by Agent Store and Remote Monitor Store versions

Whether properties can be distributed from one Agent Store service to another depends on the versions of the Agent Store and Remote Monitor Store services and the Store database serving as the source and destination in the distribution process.

Table 3–11: Property distribution capability by Agent Store and Remote Monitor Store versions

Distribution source Agent Store and Remote Monitor Store	Distribution destination Agent Store and Remote Monitor Store		
	08-00 or earlier	08-11 or later with Store 2.0	08-11 or later with Store 1.0
08-00 or earlier	Y	N	Y
08-11 or later with Store 2.0	N	Y	N
08-11 or later with Store 1.0	Y	N	Y

Legend:

Y: Can be distributed.

N: Cannot be distributed.

### (3) Batch distribution of properties for which the number of nodes increases or decreases

Some properties for which the number of nodes increases or decreases can change the structure of the tree by adding or deleting higher-level nodes. For example, nodes below the Application monitoring setting node of PFM - Agent for Platform can change the tree structure by adding or deleting nodes.

This type of property, for which the number of nodes increases or decreases, can be included in batch distribution even when the source and destination of the distribution have different tree structures. You can also choose to match the structure of the distribution destination to that of the distribution source. Note that you must be using version 08-11 or later of PFM - Manager and PFM - Web Console to perform batch distribution of properties for which the number of nodes increases or decreases.

#### (a) Operations by batch distribution of the properties for which the number of nodes increases or decreases

By using the feature that distributes, in a batch, properties for which the number of nodes increases or decreases, you can operate the Performance Management system in the following ways:

- Configure all agents identically when building a new system
- Configure all agents identically during operation of the Performance Management system
- Update specific properties on multiple agents during operation of the Performance Management system
- Add a node to multiple agents during operation of the Performance Management system
- Remove a node from multiple agents during operation of the Performance Management system

By adding and deleting nodes and setting properties on a single agent, and then distributing the properties of that agent in a batch, you can match the property settings of the distribution destinations including the tree structure to those of the distribution source.

The following provides examples of configuring batch-distribution of agent properties.

For details on how to add or remove nodes from a single agent, see the appropriate PFM - Agent or PFM - RM manual. For details on how to distribute properties in a batch, see [3.4.8\(3\)\(b\) Procedure for batch distribution of properties for which the number of nodes increases or decreases](#).

Configuring all agents identically when building a new system:

In the Distribute Properties > Select Property window, select **Add** as the **Operation** for each node in the properties list area.

The nodes are added to the distribution destination so that the tree structure mirrors that of the distribution source. The values of the properties all match the values on the distribution source.

Configuring all agents identically during operation of the Performance Management system:

In the Distribute Properties > Select Property window, select **Add** as the **Operation** for each node in the properties list area, and select the **Delete nodes that only exist at the distribution destination** check box.

Any nodes that do not exist on the distribution destination agent are added in the distribution process. In this case, the property settings of the added nodes match those of the destination agent. The settings of any node that already exists at the distribution destination agent will match the settings of that node on the source agent. Any nodes that only exist at the distribution destination agent will be removed.

As a result of this process, the tree structure of the distribution destination agent will match that of the distribution source agent.

Updating the value of specific properties on multiple agents during operation of the Performance Management system:

In the Distribute Properties > Select Property window, select **Update** as the **Operation** for each node where there are properties you want to update.

Also, select the **Apply** check box for each property you want to update.

The update operation only updates the values of properties with the **Apply** check box selected.

Adding a node to multiple agents during operation of the Performance Management system:

In the Distribute Properties > Select Property window, select **Add** as the **Operation** for the node that you want to add.

The node is added to the distribution target agent, so that the tree structure mirrors that of the distribution source. The property settings of the added node will match those of the destination agent.

If you perform batch distribution with **Add** selected for a node that exists at the distribution-target agent, the values of the properties on that node are overwritten regardless of whether the **Apply** check box is selected.

Removing a node from multiple agents during operation of the Performance Management system:

In the Distribute Properties > Select Property window, select **Delete** as the **Operation** for the node you want to delete.

The node for which **Delete** is selected is deleted if it exists at the distribution destination.



#### Tip

The **Delete** operation does not delete the corresponding node from the distribution source agent. For this reason, the distribution source and distribution destination agents will have different tree structures after the batch distribution process.

## (b) Procedure for batch distribution of properties for which the number of nodes increases or decreases

Use the procedure below to distribute, in a batch, properties for which the number of nodes increases or decreases. This example distributes the tree structure below the Application monitoring setting node available with version 08-11 or later of PFM - Agent for Platform. The following procedure assumes that the properties have been set on the distribution source agent.

1. Log on to PFM - Web Console from the monitoring console Web browser.  
Log on to a user account that has administrator user permissions.  
You must have administrator user permissions to use the Services window.
2. In the navigation frame of the main window, select the **Services** tab.
3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID.

4. Select the node of the service to act as the distribution source.

*For PFM - Agent hosts*

Expand the hierarchy under the folder named for the host running the Agent Store or Agent Collector service whose properties you want to distribute, and select the service to act as the distribution source.

*For PFM - RM hosts*

Expand the hierarchy under the folder named for the host running the Remote Monitor Store or Remote Monitor Collector service whose properties you want to distribute, and then select the service to act as the distribution source.

Because this procedure involves distributing the Application monitoring setting of PFM - Agent for Platform, select an Agent Collector service that begins with TA.

For details on service IDs, see the description of the service naming rules in the appendixes of the *JPI/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

The selected Agent Collector service is marked with a checkmark.

5. In the method frame, select the **Distribute Property** method.

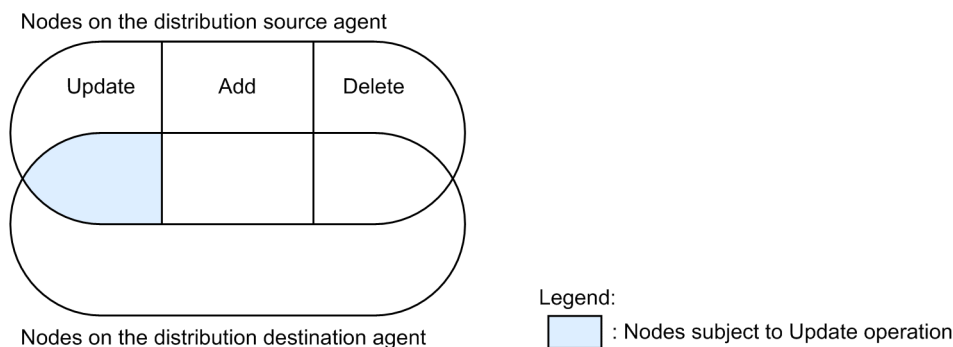
The Distribute Properties > Select Service window appears, showing a list of services available for selection as the distribution destination. The list is populated with services that have the same product name and data model version as the distribution source.

6. Select the distribution destination service and click **Next**.

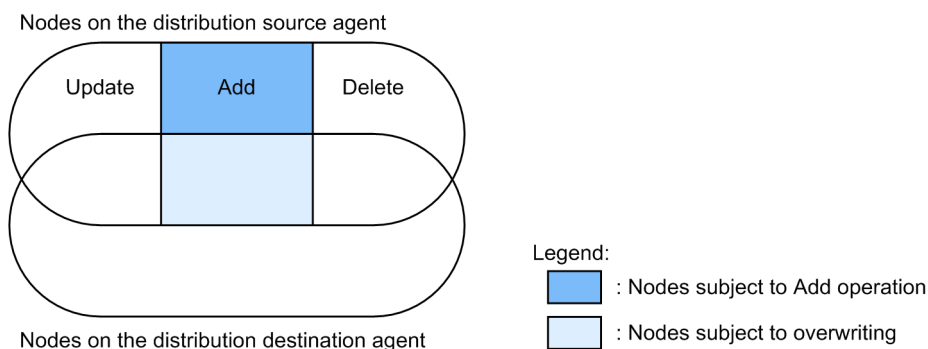
7. In the Distribute Properties > Select Property window, select **Application monitoring setting** in the tree in the information frame.

8. Select **Update**, **Add**, or **Delete** for the nodes under Application monitoring setting in the property list area at the bottom of the information frame.

The following figure indicates the nodes that are subject to an **Update** operation.

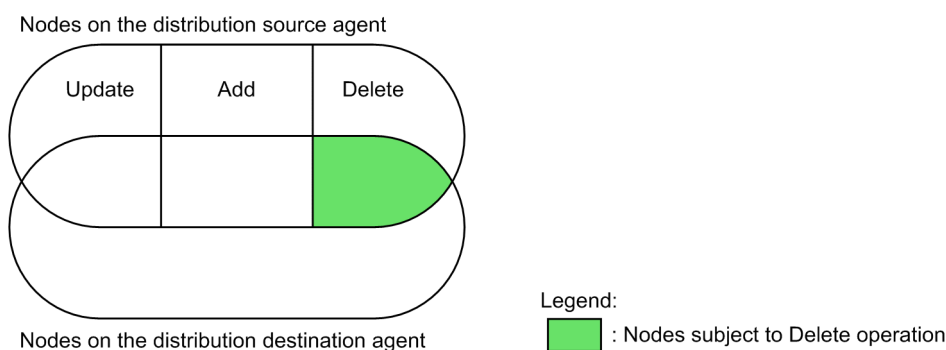


The update operation only updates the values of properties for which you selected the **Apply** check box in step 10. The following figure indicates the nodes that are subject to an **Add** operation.



If you perform batch distribution with **Add** selected for a node that exists at the distribution-target agent, the values of the properties on that node are overwritten regardless of whether the **Apply** check box is selected.

The following figure indicates the nodes that are subject to a **Delete** operation.

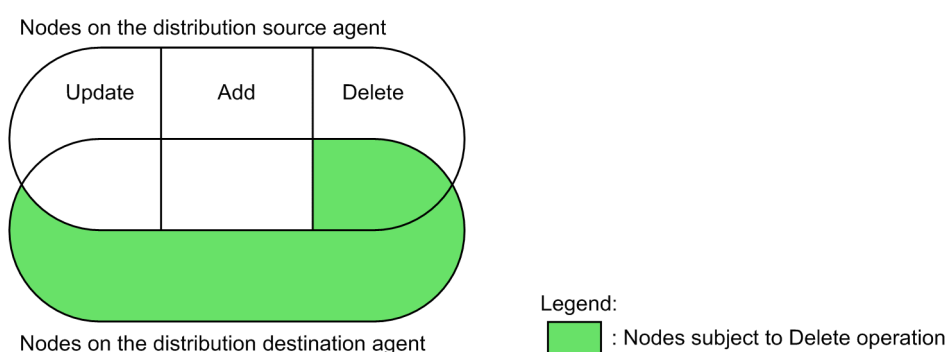


**Tip**

The **Delete** operation does not delete the corresponding node from the distribution source agent. For this reason, the distribution source and distribution destination agents will have different tree structures after the batch distribution process.

- To delete a node that exists on the distribution target agent but not on the distribution source agent, select the **Delete nodes that only exist at the distribution destination** check box.

The following figure indicates the nodes that are subject to a **Delete** operation when the **Delete nodes that only exist at the distribution destination** check box is selected.



- For nodes for which you selected **Update** in step 8, select the properties whose values you want to update. Select the node in the tree to display a list of properties.

When the **Update** operation is selected, properties for which the **Apply** check box is selected in the properties list are included in the batch distribution process.

You can select all of the properties in the list by clicking the **Select All** button, and unselect all selected properties by clicking the **Unselect All** button.

11. Click the **Finish** button.

After selecting the nodes for which to distribute properties and which properties to distribute, click the **Finish** button. The batch distribution process begins, and the Distribute Property > Progress Reports window appears.

When batch distribution to a service has finished, **OK** appears in the **Property Distribution** column for that service. The **OK** button becomes available when batch distribution has finished for all services.

12. Click the **OK** button.

The contents of the information frame are cleared.



# 4

## Managing Operation Monitoring Data

This chapter describes how to manage performance data and event data collected with Performance Management.

## 4.1 Managing performance data

---

Performance data is collected by an Agent Collector or Remote Monitor Collector service on a monitoring agent and stored in a Store database managed by the Agent Store or Remote Monitor Store service.

For details on how to distribute the recording options and retention conditions for performance data, see [3.4.8 Distributing agent properties as a batch](#). For details on how to modify the storage location for performance data, see the chapters explaining installation and setup in each PFM - Agent or PFM - RM manual. For further details on the commands used in this section, see the chapter explaining commands in the manual *JPI/Performance Management Reference*.

### 4.1.1 Modifying the recording options for performance data

You can modify the recording options for performance data collected by Agent Collector and Remote Monitor Collector services. The recording options for performance data include:

- The data to be recorded
- The frequency of data collection
- The offset at which to start collecting data
- Conditional expressions for selecting records to be recorded in the Store database

Each record has specific recording options for performance data. For some records, however, you cannot modify the options. For details, see the description of properties in an appendix of the appropriate PFM - Agent or PFM - RM manual.

#### (1) Modifying the recording options for performance data by using the monitoring console

You can modify the recording options for performance data in the monitoring console from the Services window of PFM - Web Console.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You need to log on as a user with administrator user permissions. You must have administrator user permissions to use the Services window.
2. In the navigation frame of the main window, select the **Services** tab.
3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.  
The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID. For details on service IDs, see the description of the service naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.  
The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.
4. Expand the hierarchy under the folder with the name of the host for which you want to modify the recording options for performance data, and select a node for which you want to modify the recording options for performance data.

For PFM - RM, select the node according to which performance data recording option you would like to change. The following table lists the corresponding node to select for the option to be changed.

**Table 4–1: Items to be modified and nodes to be selected**

Item to be modified	Node to be selected	
	Remote Monitor Collector service	Remote agent or group agent
The data to be recorded	No	Yes
The frequency of data collection	Yes	No
The offset at which to start collecting data	Yes	No
Specifies the condition for registering records in the store database.	Yes	No

Legend:

Yes: Can be selected.

No: Cannot be selected.

The selected node is marked with a checkmark.

5. In the method frame, select **Properties**.

The Properties window for the selected node appears, showing the properties of the node in a hierarchy.

6. Expand the hierarchy under the node that contains the record whose recording options you want to change, and select a record in the tree.

When you expand the node for a record type, the nodes in the tree represent records. The name of each record is the record ID without the database ID.

The selected record is marked with a tick, and the recording options set for the selected record appear at the bottom of the information frame.

The following table lists the record type corresponding to each node.

**Table 4–2: Record type corresponding to each node**

Node	Record type
Detail Records	PD record type
Interval Records	PI record type
Log Records	PL record type

7. Modify the definitions of the recording options for the record.

The properties of the selected record are displayed at the bottom of the information frame.

Modify the property settings. The following table lists descriptions, settings, and nodes that can be modified for each property.

**Table 4–3: Description and settings and nodes that can be modified for each property**

Property name	Description and settings	Node that can be modified.
Description	Displays the description for the selected record.	--
Log <sup>#1</sup>	Specifies whether to record collected records in the Store database. <ul style="list-style-type: none"> <li>• Yes: Records</li> <li>• No: Does not record</li> </ul>	<ul style="list-style-type: none"> <li>• Agent Collector<sup>#2</sup></li> <li>• Remote agent<sup>#2</sup></li> <li>• Group agent<sup>#2</sup></li> </ul>

Property name	Description and settings	Node that can be modified.
Log (ITSLM) <sup>#3</sup>	Displays whether records collected from JP1/SLM are recorded in the Store database. <ul style="list-style-type: none"> <li>• Yes: Records</li> <li>• No: Does not record</li> </ul>	--
Monitoring (ITSLM)	Displays whether the system is configured to send collected records to JP1/SLM. <ul style="list-style-type: none"> <li>• Yes: Sends</li> <li>• No: Does not send</li> </ul>	--
Collection Interval <sup>#4</sup>	Specifies a numerical value from 0 to 2,147,483,647 for the interval time for collecting records. The time is in seconds. 0 means that records will not be collected.	<ul style="list-style-type: none"> <li>• Agent Collector</li> <li>• Remote Monitor Collector</li> </ul>
Collection Offset <sup>#4#5</sup>	Specifies a numerical value from 0 to 32,767 for the offset at which to start collecting records. The time is in seconds. For example, all records with the offset value of 0 are collected simultaneously each time. A record with the offset value of 20 is collected 20 seconds after the records with the value of 0.	<ul style="list-style-type: none"> <li>• Agent Collector</li> <li>• Remote Monitor Collector</li> </ul>
Sync Collection With <sup>#4</sup>	A record appears to synchronize collection with.	--
LOGIF	Allows you to specify the conditional expression to use for records to be recorded in the database. Records are recorded according to the condition specified here. Because the condition set here is applied to data stored in the Store database, it does not affect data collection performed by the Agent Collector service or the Remote Monitor Collector service. When you click the text box, the LOGIF Expression Editor window appears in a new window. In the LOGIF Expression Editor window, you can create conditional expressions composed of fields, operators, judgment criteria, and other components. Click the <b>OK</b> button to accept the settings, and the conditional expression you have just created is inserted in the LOGIF text box. For details, see the chapter that describes the LOGIF Expression Editor window in the manual <i>JP1/Performance Management Reference</i> .	<ul style="list-style-type: none"> <li>• Agent Collector</li> <li>• Remote Monitor Collector</li> </ul>

Legend:

--: Not applicable

#1

Even if the value of this property is No, the records will be stored in the Store database if the value of the Log (ITSLM) property is Yes.

#2

You might be unable to modify the node depending on the nature of the PFM - Agent or PFM - RM records. For details, see the documentation for PFM - Agent or PFM - RM.

#3

Even if the value of this property is No, the records will be stored in the Store database if the value of the Log property is Yes.

#4

The Sync Collection With property and either the Collection Interval or Collection Offset property are mutually exclusive.

#5

The data collection behavior differs depending on whether a Collection Offset value is specified. For details, see [17.2.9\(3\) Collection of performance data is skipped and the KAVE00213-W message is output](#).

Notes:

- Increasing the number of records for which performance data is collected might affect your disk space or system performance. When you set up records to be collected, make sure you only set those items that are necessary for monitoring, always considering your requirements for performance data collection, such as the required free disk space and the record collection interval. For information on the required free disk space, see the appendix describing system estimation in the appropriate PFM - Agent or PFM - RM manual. For details on disk space requirements, see the appendix describing system estimation in the appropriate PFM - Agent or PFM - RM manual.
- For the Collection Interval for record collection, either use the default value or specify a value that is both 60 seconds or more and a factor of 3,600. When you have to specify a value that is more than 3,600 seconds (one hour) for the Collection Interval, choose a number that is both a multiple of 3,600 and a factor of 86,400 (24 hours). If the Collection Interval is set to a value less than the default value or to less than 60 seconds, the Agent Collector and Agent Store services on the PFM - Agent host or the Remote Monitor Collector and Remote Monitor Store services on the PFM - RM host might be overloaded, which might make it impossible to save the collected performance data.
- When you modify the value for the Collection Offset, which is the offset value at which to start collecting records, choose a number with the overall load of the data collection in mind.
- Even if the Collection Interval for the PI record type is set to a value that is not a multiple of 60 seconds, the performance data is summarized together with other record types at the same collection times. The seconds portion is discarded and the data is saved with only the minute values.

Examples:

When 30 seconds is specified for the Collection Interval:

Collection time	Time of the performance data to be saved
12:01:00	12:01:00
12:01:30	12:01:00
12:02:00	12:02:00
12:02:30	12:02:00

When 90 seconds is specified for the Collection Interval:

Collection time	Time of the performance data to be saved
12:00:00	12:00:00
12:01:30	12:01:00
12:03:00	12:03:00
12:04:30	12:04:00

8. Click **Finish** or **Apply**.

The settings that you have modified take effect.

Valid values or default values vary with each record. For details on valid values, ranges of values, or default values, see the chapter explaining records in each PFM - Agent or PFM - RM manual.

## (2) Modifying the recording options for performance data by using commands

To modify the recording options for collecting performance data in the database, follow these general procedures:

1. Use the `jpcasrec output` command to output the current definitions of the recording options to an XML file.
2. Based on the resulting XML file, modify the definitions of the recording options.

3. Use the `jpcasrec update` command to update the definitions of the recording options with the modified XML file.

Each procedure is described below.

## (a) Using the `jpcasrec output` command to output the definitions of the recording options

On the host where PFM - Web Console is installed, execute the `jpcasrec output` command. The `jpcasrec output` command connects to the agent to obtain the definition information of the recording options for the Store database, and outputs this information to an XML file.

To output the definition of the recording options by using the `jpcasrec output` command:

1. Log on to the host where PFM - Web Console is installed.

You need to log on as a special user with special permissions, as shown below:

- In Windows:  
Administrator permissions
- In UNIX:  
root user permissions

2. Execute the `jpcmkkey` command.

Execute the command to create an authentication key file.

```
jpcmkkey -user administrator
```

3. Execute the `jpcasrec output` command.

For example, if you want to output to the parameter file named `asrec.xml` the definition information of the recording options for the Store database of PFM - Agent with the service ID of `TA1host1`, use the following command:

```
jpcasrec output -o asrec.xml TA1host1
```

When the command is executed, the definition information of the recording options is output to the specified XML file.

An example of this output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "asrec_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-record-definition>
<service id="TA1host1">
<record id="PD_DEV">
<!-- Description : Devices Detail -->
<log>Yes</log>
<collection-interval>60</collection-interval>
<collection-offset>0</collection-offset>
<logif> </logif>
</record>
<record id="PD_GEND">
<!-- Description : Generic Data Detail -->
<log>No</log>
<collection-interval>60</collection-interval>
<collection-offset>0</collection-offset>
<logif> </logif>
```

```

</record>
    ...
    ...
    ...
</service>
</agent-store-db-record-definition>
</pr-cli-parameters>

```

## (b) Modify the definitions output by the jpcasrec output command

Modify the definitions of the recording options in the XML file generated by the `jpcasrec` output command. You can use any text editor or XML editor to edit the XML file.

The file format and the settings for each tag are described below. Edit the file if necessary.

- Format

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "asrec_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-record-definition>
    <service id="service-ID">
        <record id="record-ID">
            <!-- Description : Content Index Detail -->
            <log>whether-to-record-in-the-database</log>
            <collection-interval>collection-interval</collection-interval>
            <collection-offset>offset-at-which-to-start-collection</
collection-offset>
            <logif>
                <and>
                    <or>
                        <expression>field-condition-"value"</expression>
                        <expression>field-condition-"value"</expression>
                    </or>
                        <expression>field-condition-"value"</expression>
                    ...
                </and>
            </logif>
        </record>
        ...
    </service>
</agent-store-db-record-definition>
</pr-cli-parameters>

```

- Definitions

The XML declaration goes on the first line, and the document type declarations go on the second and third lines. You must write them exactly as shown below:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "asrec_params.dtd">
<pr-cli-parameters ver="0110">

```

The following table describes the tags defined on the forth line and below. These tags must be defined in the order listed in the table.

Legend:

Yes: Required and cannot be omitted.

No: Not required and can be omitted.

Table 4–4: XML definitions

Tag name	Required	Description and settings
<code>&lt;agent-store-db-record-definition&gt; ... &lt;/agent-store-db-record-definition&gt;</code>	Yes	The root tag of the definition information of the recording options for the Store database.
<code>&lt;service id="service-ID"&gt; ... &lt;/service&gt;</code>	Yes	Specifies the service ID that identifies PFM - Agent or PFM - RM. The service ID of an Agent Collector or Remote Monitor Collector service has an <b>A</b> as the second character. For details on service IDs, see the description of the service naming rules in an appendix of the <i>JP1/Performance Management Planning and Configuration Guide</i> . A <code>&lt;service&gt;</code> tag contains <code>&lt;record&gt;</code> tags. More than one <code>&lt;service&gt;</code> tag can be specified.
<code>&lt;record id="record-ID"&gt; ... &lt;/record&gt;</code>	Yes	Specifies the record ID for which you want to modify the recording options. A <code>&lt;record&gt;</code> tag contains <code>&lt;log&gt;</code> , <code>&lt;collection-interval&gt;</code> , <code>&lt;collection-offset&gt;</code> , and <code>&lt;logif&gt;</code> tags. For further details, see <a href="#">Table 4-5</a> . More than one <code>&lt;record&gt;</code> tag can be specified.

The following table describes tags contained in a `<record>` tag (for recording options for a record) and their settings. More than one `<record>` tag can be specified. Tags contained in a `<record>` tag must be defined in the order listed in the table.

Table 4–5: Recording options for a record (`<record>` tag)

Tag name	Required	Settings
<code>&lt;log&gt; ... &lt;/log&gt;</code>	No	Specifies whether to record collected performance data in the Store database. One of the following values can be specified: <ul style="list-style-type: none"> <li>Yes: Records</li> <li>No: Does not record</li> </ul> Only one <code>&lt;log&gt;</code> tag can be used in a <code>&lt;record&gt;</code> tag.
<code>&lt;collection-interval&gt; ... &lt;/collection-interval&gt;</code>	No	Specifies a numerical value from 0 to 2,147,483,647 for the collection interval of performance data. The time is in seconds. 0 means that performance data will not be collected. Only one <code>&lt;collection-interval&gt;</code> tag can be used in a <code>&lt;record&gt;</code> tag.
<code>&lt;collection-offset&gt; ... &lt;/collection-offset&gt;</code>	No	Specifies a numerical value from 0 to 32,767 for the offset at which to start collecting performance data. The time is in seconds. 0 means that all performance data will be collected simultaneously. Only one <code>&lt;collection-offset&gt;</code> tag can be used in a <code>&lt;record&gt;</code> tag.
<code>&lt;logif&gt; ... &lt;/logif&gt;</code>	No	Allows you to specify a conditional expression to use for recording performance data in the database. For further details, see <a href="#">Table 4-6</a> . Only one <code>&lt;logif&gt;</code> tag can be used in a <code>&lt;record&gt;</code> tag.



Note that the values for the omitted items are not updated.

Notes:

- Increasing the number of records for which performance data is collected might affect your disk space or system performance. When you set up records to be collected, make sure you only set those items that are necessary for monitoring, always considering your requirements for performance data collection, such as the required free disk space and the record collection interval. For details on the required disk space, see the description of system estimates in an appendix of each PFM - Agent or PFM - RM manual.
- For the Collection Interval for record collection, either use the default value or specify a value that is both 60 seconds or more and a factor of 3,600. When you have to specify a value that is greater than 3,600 seconds (one hour) for the Collection Interval, choose a number that is both a multiple of 3,600 and a factor of 86,400 (24 hours). Specifying a value less than the default value or 60 seconds might increase both the number of open files and the amount of memory use. That would prevent the Store database from functioning normally, causing the collected performance data to be lost without being saved.

Valid values or default values vary with each record. For details on valid values, ranges of values, or default values, see the chapter explaining records in each PFM - Agent or PFM - RM manual.

- When you modify the value for the Collection Offset, which is the offset value at which to start collecting records, choose a number while keeping in mind the overall load of the data collection.

The following table describes tags contained in a `<logif>` tag (for conditional expressions for recording in the database), and their settings.

Table 4–6: Conditional expression for recording in the database (`<logif>` tag)

Tag name	Required	Settings
<code>&lt;and&gt; ... &lt;/and&gt;</code>	No	Used to combine two <code>&lt;expression&gt;</code> tags with AND operation when more than one <code>&lt;expression&gt;</code> tag (logical expressions) is used. The two <code>&lt;expression&gt;</code> tags to be combined with AND operation are enclosed in an <code>&lt;and&gt;</code> tag pair. Conditional expressions consist of binary operations that can be nested. More than one <code>&lt;and&gt;</code> tag can be used when more than one <code>&lt;expression&gt;</code> tag is used.
<code>&lt;or&gt; ... &lt;/or&gt;</code>	No	Used to combine two <code>&lt;expression&gt;</code> tags with OR operation when more than one <code>&lt;expression&gt;</code> tag (logical expressions) is used. The two <code>&lt;expression&gt;</code> tags to be combined with OR operation are enclosed in an <code>&lt;and&gt;</code> tag pair. Conditional expressions consist of binary operations that can be nested. More than one <code>&lt;or&gt;</code> tag can be used when more than one <code>&lt;expression&gt;</code> tag is used.
<code>&lt;expression&gt; ... &lt;/expression&gt;</code>	No	Specifies the condition for determining whether to record to the database. Use the following format: Specifies field condition " <i>value</i> " (without any intervening spaces) <i>field</i> : Specifies the field to be compared. For details on available fields, see the chapter explaining the records in each PFM - Agent or PFM - RM manual.

Tag name	Required	Settings
<expression> ... </expression>	No	<p><i>condition:</i></p> <p>Use one of the operators shown below. Note that you must use <code>&amp;lt;</code> for <code>&lt;</code> and <code>&amp;gt;</code> for <code>&gt;</code> according to XML file conventions.</p> <ul style="list-style-type: none"> <li>• = The value of the field is equal to the <i>value</i>.</li> <li>• &lt; The value of the field is less than the <i>value</i>.</li> <li>• &lt;= The value of the field is equal to or less than the <i>value</i>.</li> <li>• &gt; The value of the field is more than the <i>value</i>.</li> <li>• &gt;= The value of the field is equal to or more than the <i>value</i>.</li> <li>• &lt;&gt; The value of the field is not equal to the <i>value</i>.</li> </ul> <p><i>value</i></p> <p>Specifies the criteria value to determine whether to record performance data. You can specify an integer, a decimal, or a character string of no more than 2,048 bytes. A valid value varies with the specified field.</p>

Note that the values for the omitted items are not updated.

### (c) Using the `jpcasrec update` command to update the definitions of the recording options

On the host where PFM - Web Console is installed, execute the `jpcasrec update` command. The `jpcasrec update` command updates the definition information of the recording options for the Store database with the modified XML file.

1. Log on to the host where PFM - Web Console is installed.

You need to log on as a special user with special permissions, as shown below:

- In Windows:  
Administrator permissions
- In UNIX:  
root user permissions

2. Execute the `jpcasrec update` command.

For example, when you want to update the definition of the recording options based on the contents of the file `asrec.xml`, use the following command:

```
jpcasrec update asrec.xml
```

## 4.1.2 Modifying the retention conditions for performance data (in Store 2.0)

Store 2.0 allows you to modify the retention period for performance data in the retention conditions for performance data recorded in the database.

The following table describes the available retention conditions applicable to each record type.

Table 4–7: Available retention conditions by record type

Record type	Retention condition
PI record type	Retention period of records
PD record type	
PL record type	

## (1) Modifying the retention conditions for performance data from the monitoring console

To modify the retention conditions for performance data from the monitoring console, use the Services window in PFM - Web Console.

1. From the monitoring console Web browser, log on to PFM - Web Console.  
Log on to a user account that has administrator user permissions. You must have administrator user permissions to use the Services window.
2. In the navigation frame of the main window, select the **Services** tab.
3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.  
The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID. The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.
4. Expand the hierarchy under the folder that has the same name as the host whose retention conditions you want to change, and select an Agent Store or Remote Monitor Store service.  
If the product name display function is enabled, the Agent Store or Remote Monitor Store service is indicated by *host-name<service-key> (Store)*.  
If the product name display function is not enabled, select an Agent Store or Remote Monitor Store service with an ID that does not begin with a P and has an S as the second character. (Service IDs that begin with PS refer to a Master Store service.)  
For details on service IDs, see the description of the service naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.  
The selected Agent Store or Remote Monitor Store service is marked with a checkmark.
5. In the method frame, select the **Properties** method.
6. In the Properties window of the Agent Store or Remote Monitor Store service, select the **RetentionEx** node from the tree.  
At the bottom of the information frame, the properties of the **RetentionEx** node are displayed.  
You can modify the property settings. The following table gives a description of each property and lists the available settings.

Table 4–8: Description and settings for each property

Record type	Node name	Property name	Settings
PI record type	Product Interval - <i>record-ID-of-PI-record-type</i>	Period - Minute Drawer (Day)	The retention period for performance data collected on a per-minute basis for each record ID of PI-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.
		Period - Hour Drawer (Day)	The retention period for performance data collected on an hourly basis for each record ID of PI-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.
		Period - Day Drawer (Week)	The retention period for performance data collected on a daily basis for each record ID of PI-type records. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
		Period - Week Drawer (Week)	The retention period for performance data collected on a weekly basis for each record ID of PI-type records. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
		Period - Month Drawer (Month)	The retention period for performance data collected on a monthly basis for each record ID of PI-type records. Specify the retention period (in months) as an integer in the range from 0 to 120.
		Period - Year Drawer (Year)	The retention period for performance data collected on a yearly basis for each record ID of PI-type records. No retention period applies to data collected on a yearly basis.
PD record type	Product Detail - <i>record-ID-of-PD-record-type</i>	Period (Day)	The retention period for performance data for each record ID of PD-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.
PL record type	Product Log - <i>record-ID-of-PL-record-type</i>	Period (Day)	The retention period for performance data for each record ID of PL-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.

7. Click **Finish** or **Apply**.

The new settings take effect.

## (2) Modifying the retention conditions for performance data by using commands

To modify the retention conditions for performance data by using commands, follow these general procedures:

1. Use the `jpcaspsv output` command to output the current definitions of the retention conditions to an XML file.
2. Based on the resulting XML file, modify the definitions of the retention conditions.

3. Use the `jpcaspsv update` command to update the definitions of the retention conditions from the modified XML file.

Each procedure is described below.

### (a) Using the `jpcaspsv output` command to output the definition of the retention conditions

On a host where PFM - Web Console is installed, execute the `jpcaspsv output` command. The `jpcaspsv output` command connects to the agent to obtain the definition information for retention conditions in the Store database and outputs this information to an XML file.

1. Log on to the host where PFM - Web Console is installed.

Log on as a user with the following permissions:

- In Windows:  
Administrator permissions
- In UNIX:  
root user permissions

2. Execute the `jpcaspsv output` command.

For example, when you want to output the definition information of the retention conditions for the Store database of PFM - Agent with the service ID of `TS1host1` to the parameter file named `aspsv.xml`, use the following command:

```
jpcaspsv output -o aspsv.xml TS1host1
```

When the command is executed, the definition information of the retention conditions is output to the specified XML file.

An example of this output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
<service id="TS1host1">
<ex-product-interval>
<ex-interval-record id="PI">
<minute-drawer-days period="10"/>
<hour-drawer-days period="10"/>
<day-drawer-weeks period="10"/>
<week-drawer-weeks period="10"/>
<month-drawer-months period="10"/>
<!-- year-drawer-years period="10" -->
</ex-interval-record>
:
</ex-product-interval>
<ex-product-detail>
<ex-detail-record id="PD" period="10"/>
<ex-detail-record id="PD_THRD" period="10"/>
<ex-detail-record id="PD_ADRS" period="10"/>
<ex-detail-record id="PD_PDI" period="10"/>
<ex-detail-record id="PD_PEND" period="10"/>
</ex-product-detail>
<ex-product-log>
<ex-log-record id="PL" period="10"/>
```

```

<ex-log-record id="RM" period="10"/>
</ex-product-log>
</service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>

```

## (b) Modify the definitions output by the jpcaspsv output command

Modify the definitions of the recording options in the XML file generated by the `jpcaspsv` output command. You can use any text editor or XML editor to edit the XML file.

The file format and the settings for each tag are described below. Edit the file as required.

- Format:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
  <service id="service-ID">
    <ex-product-interval>
      <ex-interval-record id="record-ID">
        <minute-drawer-days period="retention-period-for-per-minute-
data"/>
        <hour-drawer-days period="retention-period-for-hourly-
data"/>
        <day-drawer-weeks period="retention-period-for-daily-data"/>
        <week-drawer-weeks period="retention-period-for-weekly-
data"/>
        <month-drawer-months period="retention-period-for-monthly-
data"/>
        <!-- year-drawer-years period="10" -->#
      </ex-interval-record>
    </ex-product-interval>
    <ex-product-detail>
      <ex-detail-record id="record-ID" period="record-retention-
period"/>
      :
      :
    </ex-product-detail>
    <ex-product-log>
      <ex-log-record id="record-ID" period="record-retention-period"/>
      :
    </ex-product-log>
  </service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>

```

# You cannot set a retention period for yearly records.

- Definitions:

The XML declaration goes on the first line, and the document type declarations go on the second and third lines. You must write them exactly as shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
```

The following table describes the tags defined on the forth line and below. These tags must be defined in the order listed in the table.

Legend:

Yes: Required and cannot be omitted.

No: Not required and can be omitted.

Table 4–9: XML definitions

Tag name	Required	Description and settings
<code>&lt;agent-store-db-preserve-definition&gt; ...&lt;/agent-store-db-preserve-definition&gt;</code>	Yes	The root tag of the definition information of the retention conditions for the Store database.
<code>&lt;service id="service-ID"&gt; ... &lt;/service&gt;</code>	Yes	Specifies the service ID that identifies PFM - Agent or PFM - RM. Specify a service with an ID that does not begin with a <b>P</b> but has an <b>S</b> as the second character. (Service IDs that begin with <b>PS</b> refer to a Master Store service.) For details on service IDs, see the description of the service naming rules in an appendix of the <i>JPI/Performance Management Planning and Configuration Guide</i> . A <code>&lt;service&gt;</code> tag contains <code>&lt;ex-product-interval&gt;</code> , <code>&lt;ex-product-detail&gt;</code> , and <code>&lt;ex-product-log&gt;</code> tags. More than one <code>&lt;service&gt;</code> tag can be specified.
<code>&lt;ex-product-interval&gt; ...&lt;/ex-product-interval&gt;</code>	No	Specifies the retention period of PI-type records. It contains <code>&lt;minute-drawer-days period=retention-period-for-per-minute-data&gt;</code> , <code>&lt;hour-drawer-days period=retention-period-for-hourly-data&gt;</code> , <code>&lt;day-drawer-weeks period=retention-period-for-daily-data&gt;</code> , <code>&lt;week-drawer-weeks period=retention-period-for-weekly-data&gt;</code> , and <code>&lt;month-drawer-months period=retention-period-for-monthly-data&gt;</code> tags. For further details, see <a href="#">Table 4-10 Retention periods for PI-type records (&lt;ex-product-interval&gt; tag)</a> . You can specify more than one <code>&lt;ex-product-interval&gt;</code> tag in a <code>&lt;service&gt;</code> tag.
<code>&lt;ex-product-detail&gt; ...&lt;/ex-product-detail&gt;</code>	No	Specifies the maximum number of stored records for the PD record type. It contains <code>&lt;ex-detail-record&gt;</code> tags. Only one <code>&lt;ex-product-detail&gt;</code> tag can be used in a <code>&lt;service&gt;</code> tag. For further details, see <a href="#">Table 4-11 Retention periods for PD-type records (&lt;ex-product-detail&gt; tag)</a> .
<code>&lt;ex-product-log&gt; ...&lt;/ex-product-log&gt;</code>	No	Specifies the maximum number of stored records for the PL record type. It contains <code>&lt;ex-log-record&gt;</code> tags. For further details, see <a href="#">Table 4-12 Retention periods for PL-type records (&lt;ex-product-log&gt; tag)</a> . Only one <code>&lt;ex-product-log&gt;</code> tag can be used in a <code>&lt;service&gt;</code> tag.

Note that the values for any omitted items are not updated.

The following table describes the tags contained in an `<ex-product-interval>` tag (for the retention period of PI-type records) and their settings. Tags contained in an `<ex-product-interval>` tag must be defined in the order listed in the table.

**Table 4–10: Retention periods for PI-type records (`<ex-product-interval>` tag)**

Tag name	Required	Description and settings
<code>&lt;minute-drawer-days period="retention-period-for-per-minute-data"&gt;</code>	No	Sets the retention period for performance data collected on a per-minute basis. Specify the retention period (in days) as an integer in the range from 0 to 366.
<code>&lt;hour-drawer-days period="retention-period-for-hourly-data"&gt;</code>	No	Sets the retention period for performance data collected on an hourly basis. Specify the retention period (in days) as an integer in the range from 0 to 366.
<code>&lt;day-drawer-weeks period="retention-period-for-daily-data"&gt;</code>	No	Sets the retention period for performance data collected on a daily basis. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
<code>&lt;week-drawer-weeks period="retention-period-for-weekly-data"&gt;</code>	No	Sets the retention period for performance data collected on a weekly basis. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
<code>&lt;month-drawer-months period="retention-period-for-monthly-data"&gt;</code>	No	Sets the retention period for performance data collected on a monthly basis. Specify the retention period (in months) as an integer in the range from 0 to 120.

Note that the values for any omitted items are not updated.

The following table describes the tags contained in an `<ex-product-detail>` tag (for the retention period of PD-type records) and their settings.

**Table 4–11: Retention periods for PD-type records (`<ex-product-detail>` tag)**

Tag name	Required	Description and settings
<code>&lt;ex-detail-record id="record-ID" period="retention-period-for-specified-record" /&gt;</code>	No	Specifies the retention period for a specific PD-type record. Specify the retention period (in days) as an integer in the range from 0 to 366. Only one <code>&lt;ex-detail-record&gt;</code> tag can be specified for each PD record.

Note that the values for any omitted items are not updated.

The following table describes the tags contained in an `<ex-product-log>` tag (for the retention period of PL-type records) and their settings.

**Table 4–12: Retention periods for PL-type records (`<ex-product-log>` tag)**

Tag name	Required	Description and settings
<code>&lt;ex-log-record id="record-ID" period="retention-period-for-specified-record" /&gt;</code>	No	Specifies the retention period for a specific PL-type record.



Tag name	Required	Description and settings
<code>&lt;ex-log-record id="record-ID" period="retention-period-for-specified-record" /&gt;</code>	No	Specify the retention period (in days) as an integer in the range from 0 to 366. Only one <code>&lt;ex-log-record&gt;</code> tag can be specified for each PL record.

Note that the values for any omitted items are not updated.

### (c) Using the `jpcaspsv update` command to update the definitions of the retention conditions

On the host where PFM - Web Console is installed, execute the `jpcaspsv update` command. The `jpcaspsv update` command updates the definition information of the retention conditions for the Store database from the modified XML file.

1. Log on to the host where PFM - Web Console is installed.

Log on as a user with the following permissions:

- In Windows:  
Administrator permissions
- In UNIX:  
root user permissions

2. Execute the `jpcaspsv update` command.

For example, if you want to update the definition information with the retention conditions specified in the file `aspsv.xml`, use the following command:

```
jpcaspsv update aspsv.xml
```

### 4.1.3 Modifying the retention conditions for performance data (in Store 1.0)

In the retention conditions for performance data recorded in the database, you can modify the retention period of data or the maximum number of records. The kind of retention condition allowed for performance data depends on the type of record.

The following table describes the available retention conditions applicable to each record type.

Table 4–13: Available retention conditions for each record type

Record type	Available retention condition
PI record type	Retention period of data
PD record type	Maximum number of records
PL record type	

# (1) Modifying the retention conditions for performance data by using the monitoring console

To modify the retention conditions for performance data by using the monitoring console, use the Services window in PFM - Web Console.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You need to log on as a user with Administrator user permissions. You must have administrator user permissions to use the Services window.
2. In the navigation frame of the main window, select the **Services** tab.
3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.  
The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID. The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.
4. Expand the hierarchy under the folder with the name of the host for which you want to modify the retention conditions, and select an Agent Store service.  
If the product name display function is enabled, the Agent Store service is indicated by *host-name<service-key> (Store)*.  
If the product name display function is not enabled, select an Agent Store service with an ID that does not begin with a P and has an S as the second character. (Service IDs that begin with PS refer to a Master Store service.)  
For details on service IDs, see the description of the service naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent manual.  
The selected Agent Store service is marked with a checkmark.
5. In the method frame, select **Properties**.
6. In the Properties window for the Agent Store service, select the **Retention** node from the tree.  
At the bottom of the information frame, the properties of the **Retention** node are displayed.  
You can modify the property settings. The following table lists descriptions and settings for each property.

**Table 4–14: Description and settings for each property**

Record type	Property name	Settings
PI record type	Product Interval - Minute Drawer	<p>Specifies a retention period (in minutes) for the stored performance data.</p> <p>You can select one of the following items in the pull-down menu:</p> <ul style="list-style-type: none"> <li>• <b>Minute</b></li> <li>• <b>Hour</b></li> <li>• <b>Day</b></li> <li>• <b>2 Days</b></li> <li>• <b>3 Days</b></li> <li>• <b>4 Days</b></li> <li>• <b>5 Days</b></li> <li>• <b>6 Days</b></li> <li>• <b>Week</b></li> <li>• <b>Month</b></li> </ul>

Record type	Property name	Settings
PI record type	Product Interval - Minute Drawer	<ul style="list-style-type: none"> <li>• <b>Year</b></li> </ul>
	Product Interval - Hour Drawer	<p>Specifies a retention period (in hours) for the stored performance data.</p> <p>You can select one of the following items in the pull-down menu:</p> <ul style="list-style-type: none"> <li>• <b>Hour</b></li> <li>• <b>Day</b></li> <li>• <b>2 Days</b></li> <li>• <b>3 Days</b></li> <li>• <b>4 Days</b></li> <li>• <b>5 Days</b></li> <li>• <b>6 Days</b></li> <li>• <b>Week</b></li> <li>• <b>Month</b></li> <li>• <b>Year</b></li> </ul>
	Product Interval - Day Drawer	<p>Specifies a retention period (in days) for the stored performance data.</p> <p>You can select one of the following items in the pull-down menu:</p> <ul style="list-style-type: none"> <li>• <b>Day</b></li> <li>• <b>2 Days</b></li> <li>• <b>3 Days</b></li> <li>• <b>4 Days</b></li> <li>• <b>5 Days</b></li> <li>• <b>6 Days</b></li> <li>• <b>Week</b></li> <li>• <b>Month</b></li> <li>• <b>Year</b></li> </ul>
	Product Interval - Week Drawer	<p>Specifies a retention period (in weeks) for the stored performance data.</p> <p>You can select one of the following items in the pull-down menu:</p> <ul style="list-style-type: none"> <li>• <b>Week</b></li> <li>• <b>Month</b></li> <li>• <b>Year</b></li> </ul>
	Product Interval - Month Drawer	<p>Specifies a retention period (in months) for the stored performance data.</p> <p>You can select one of the following items in the pull-down menu:</p> <ul style="list-style-type: none"> <li>• <b>Month</b></li> <li>• <b>Year</b></li> </ul>
	Product Interval - Year Drawer	<p>The retention period, in years, for the stored performance data. The setting defaults to <b>Year</b> and cannot be modified.</p>
	PD record type	Product Detail - <i>record-ID-of-PD-record-type</i>

Record type	Property name	Settings
PD record type	Product Detail - <i>record-ID-of-PD-record-type</i>	For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines.
PL record type	Product Log - <i>record-ID-of-PL-record-type</i>	Specifies the maximum number of stored records for each record ID of PL record type. For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records. For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines.

7. Click **Finish** or **Apply**.

Your settings are enabled.

## (2) Modifying the retention condition for performance data by using commands

To modify the retention conditions for performance data recorded in the database, follow these general procedures:

1. Use the `jpcaspsv output` command to output the current definitions of the retention conditions to an XML file.
2. Based on the resulting XML file, modify the definitions of the retention conditions.
3. Use the `jpcaspsv update` command to update the definitions of the retention conditions with the modified XML file.

Each procedure is described below.

### (a) Using the `jpcaspsv output` command to output the definition of the retention condition

On a host where PFM - Web Console is installed, execute the `jpcaspsv output` command. The `jpcaspsv output` command connects to the agent to obtain the definition information for retention conditions in the Store database and outputs this information to an XML file.

1. Log on to the host where PFM - Web Console is installed.

You need to log on as a special user with special permissions, as shown below:

- In Windows:  
Administrator permissions
- In UNIX:  
root user permissions

2. Execute the `jpcaspsv output` command.

For example, when you want to output to the parameter file named `aspsv.xml` the definition information of the retention conditions for the Store database of PFM - Agent with the service ID of `TS1host1`, use the following command:

```
jpcaspsv output -o aspsv.xml TS1host1
```

When the command is executed, the definition information of the retention conditions is output to the specified XML file.

An example of this output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
<service id="TS1host1">
<product-interval>
<minute-drawer>Day</minute-drawer>
<hour-drawer>Week</hour-drawer>
<day-drawer>Year</day-drawer>
<week-drawer>Year</week-drawer>
<month-drawer>Year</month-drawer>
<!-- year-drawer : Year -->
</product-interval>
<product-detail>
<detail-record id="PD" max-rec="10000"/>
<detail-record id="PD_PDI" max-rec="100000"/>
<detail-record id="PD_PEND" max-rec="10000"/>
<detail-record id="PD_PAGF" max-rec="10000"/>
<detail-record id="PD_GEND" max-rec="10000"/>
<detail-record id="PD_SVC" max-rec="10000"/>
<detail-record id="PD_DEV" max-rec="10000"/>
<detail-record id="PD_ELOG" max-rec="10000"/>
</product-detail>
</service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>
```

## (b) Modify the definitions output by the jpcaspsv output command

Modify the definitions of the recording options in the XML file generated by the jpcaspsv output command. You can use any text editor or XML editor to edit the XML file.

The file format and the settings for each tag are described below. Edit the file if necessary.

- Format:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
  <service id="service-ID">
    <product-interval>
      <minute-drawer>retention-period-in-minutes</minute-drawer>
      <hour-drawer>retention-period-in-hours</hour-drawer>
      <day-drawer>retention-period-in-days</day-drawer>
      <week-drawer>retention-period-in-weeks</week-drawer>
      <month-drawer>retention-period-in-months</month-drawer>
      <!-- year-drawer : Year -->#
    </product-interval>
    <product-detail>
      <detail-record id="record-ID" max-rec="maximum-number-of-records"/>
      ...
    </product-detail>
  </service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>
```

```

        ...
    </product-detail>
    <product-log>
        <log-record id="record-ID" max-rec="maximum-number-of-records"/>
        ...
    </product-log>
</service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>

# The retention period in years defaults to Year and cannot be modified.

```

- **Definitions:**

The XML declaration goes on the first line, and the document type declaration goes on the second and third lines. You must write them exactly as shown below:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">

```

The following table describes the tags defined on the fourth line and below. These tags must be defined in the order listed in the table.

**Legend:**

Yes: Cannot be omitted.

No: Can be omitted.

**Table 4–15: XML definitions**

Tag name	Required	Description and settings
<agent-store-db-preserve-definition> ... </agent-store-db-preserve-definition>	Yes	The root tag of the definition information of the retention conditions for the Store database.
<service id="service-ID"> ... </service>	Yes	Specifies the service ID that identifies PFM - Agent. Specify a service with an ID that does not begin with a <b>P</b> but has an <b>S</b> as the second character. (Service IDs that begin with <b>PS</b> refer to a Master Store service.) For details on service IDs, see the description of the service naming rules in an appendix of the <i>JPI/Performance Management Planning and Configuration Guide</i> . A <service> tag contains <product-interval>, <product-detail>, and <product-log> tags. More than one <service> tag can be specified.
<product-interval> ... </product-interval>	No	The tag that specifies the retention period of records for the PI record type. It contains <minute-drawer>, <hour-drawer>, <day-drawer>, <week-drawer>, and <month-drawer> tags. For further details, see <a href="#">Table 4-16 Retention period of the records for the PI record type (&lt;product-interval&gt; tag)</a> . Only one <product-interval> tag can be used in a <service> tag.
<product-detail> ... </product-detail>	No	The tag that specifies the maximum number of stored records for the PD record type.

Tag name	Required	Description and settings
<code>&lt;product-detail&gt; ... &lt;/product-detail&gt;</code>	No	It contains <code>&lt;detail-record&gt;</code> tags. Only one <code>&lt;product-detail&gt;</code> tag can be used in a <code>&lt;service&gt;</code> tag. For further details, see <a href="#">Table 4-17 The Maximum number of stored records for the PD record type (&lt;product-detail&gt; tag)</a> .
<code>&lt;product-log&gt; ... &lt;/product-log&gt;</code>	No	The tag that specifies the maximum number of stored records for the PL record type. It contains <code>&lt;log-record&gt;</code> tags. For further details, see <a href="#">Table 4-18 The Maximum number of stored records for the PL record type (&lt;product-log&gt; tag)</a> . Only one <code>&lt;product-log&gt;</code> tag can be used in a <code>&lt;service&gt;</code> tag.

Note that the values for the omitted items are not updated.

The following table describes tags contained in a `<product-interval>` tag (for the retention period of records for the PI record type) and their settings. Tags contained in a `<product-interval>` tag must be defined in the order listed in the table.

**Table 4–16: Retention period of the records for the PI record type (<product-interval> tag)**

Tag name	Required	Settings
<code>&lt;minute-drawer&gt; ... &lt;/minute-drawer&gt;</code>	No	Specifies a retention period (in minutes) for the stored performance data. One of the following values can be specified: <ul style="list-style-type: none"> <li>Minute: one minute</li> <li>Hour: one hour</li> <li>Day: one day</li> <li><i>n</i> Days: <i>n</i> days (<i>n</i> = 2-6)</li> <li>Week: one week</li> <li>Month: one month</li> <li>Year: one year</li> </ul> Only one <code>&lt;minute-drawer&gt;</code> tag can be used in a <code>&lt;product-interval&gt;</code> tag.
<code>&lt;hour-drawer&gt; ... &lt;/hour-drawer&gt;</code>	No	Specifies a retention period (in hours) for the stored performance data. One of the following values can be specified: <ul style="list-style-type: none"> <li>Hour: one hour</li> <li>Day: one day</li> <li><i>n</i> Days: <i>n</i> days (<i>n</i> = 2-6)</li> <li>Week: one week</li> <li>Month: one month</li> <li>Year: one year</li> </ul> Only one <code>&lt;hour-drawer&gt;</code> tag can be used in a <code>&lt;product-interval&gt;</code> tag.
<code>&lt;day-drawer&gt; ... &lt;/day-drawer&gt;</code>	No	Specifies a retention period (in days) for the stored performance data. One of the following values can be specified: <ul style="list-style-type: none"> <li>Day: one day</li> <li><i>n</i> Days: <i>n</i> days (<i>n</i> = 2-6)</li> <li>Week: one week</li> </ul>

Tag name	Required	Settings
<code>&lt;day-drawer&gt; ... &lt;/day-drawer&gt;</code>	No	<ul style="list-style-type: none"> <li>Month: one month</li> <li>Year: one year</li> </ul> <p>Only one <code>&lt;day-drawer&gt;</code> tag can be used in a <code>&lt;product-interval&gt;</code> tag.</p>
<code>&lt;week-drawer&gt; ... &lt;/week-drawer&gt;</code>	No	<p>Specifies a retention period (in weeks) for the stored performance data.</p> <p>One of the following values can be specified:</p> <ul style="list-style-type: none"> <li>Week: one week</li> <li>Month: one month</li> <li>Year: one year</li> </ul> <p>Only one <code>&lt;week-drawer&gt;</code> tag can be used in a <code>&lt;product-interval&gt;</code> tag.</p>
<code>&lt;month-drawer&gt; ... &lt;/month-drawer&gt;</code>	No	<p>Specifies a retention period (in months) for the stored performance data.</p> <p>One of the following values can be specified:</p> <ul style="list-style-type: none"> <li>Month: one month</li> <li>Year: one year</li> </ul> <p>Only one <code>&lt;month-drawer&gt;</code> tag can be used in a <code>&lt;product-interval&gt;</code> tag.</p>

Note that the values for the omitted items are not updated.

The following table describes tags contained in a `<product-detail>` tag (for the maximum number of stored records for the PD record type) and their settings.

**Table 4–17: The Maximum number of stored records for the PD record type (`<product-detail>` tag)**

Tag name	Required	Settings
<code>&lt;detail-record id="record-ID" max-rec="maximum-number-of-records" /&gt;</code>	No	<p>Specifies the maximum number of stored records for each record ID of PD record type.</p> <p>For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records.</p> <p>For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines.</p> <p>Only one <code>&lt;detail-record&gt;</code> tag can be used for a PD record.</p>

Note that the values for the omitted items are not updated.

The following table describes tags contained in a `<product-log>` tag (for the maximum number of stored records for the PL record type) and their settings.

**Table 4–18: The Maximum number of stored records for the PL record type (`<product-log>` tag)**

Tag name	Required	Settings
<code>&lt;log-record id="record-ID" max-rec="maximum-number-of-records" /&gt;</code>	No	<p>Specifies the maximum number of stored records for each record ID of PL record type.</p> <p>For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records.</p>



Tag name	Required	Settings
<code>&lt;log-record id="record-ID" max-rec="maximum- number-of-records" /&gt;</code>	No	For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines. Only one <code>&lt;log-record&gt;</code> tag can be used for a PL record.

Note that the values for the omitted items are not updated.

## (c) Using the `jpcaspsv update` command to update the definitions of the retention conditions

On the host where PFM - Web Console is installed, execute the `jpcaspsv update` command. The `jpcaspsv update` command updates the definition information of the retention conditions for the Store database with the modified XML file.

1. Log on to the host where PFM - Web Console is installed.

You need to log on as a special user with special permissions, as shown below:

- In Windows:  
Administrator permissions
- In UNIX:  
root user permissions

2. Execute the `jpcaspsv update` command.

For example, if you want to update the definition information with the retention conditions specified in the file named `aspsv.xml`, use the following command:

```
jpcaspsv update aspsv.xml
```

## 4.1.4 Exporting performance data

You can export the performance data stored in the Store database to a text file. Use the `jpctool db dump` command to export data.

The purpose of this command is to output performance data to a text file. The file it creates cannot be imported using the `jpctool db import` command.

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool service list` command to make sure that the Name Server, Master Manager, and Master Store services are running.
3. Execute the `jpctool db dump` command.

For example, if you want to export to the file named `pcsr.out` that contains the performance data collected from 02:00:00 (GMT) to 14:59:00 (GMT) on July 10, 2006, which is stored in the Processor Overview (PI\_PCSR) record on PFM - Agent for Platform (Windows) host `host02`, use the following command:

```
jpctool db dump -id TS* -host host02 -stime 2006/07/10 02:00 -etime 2006/07/10 14:59 -f pcsr.out -dbid PI -rec PCSR
```

When the command finishes normally, the export file for the performance data is created in the following location:

On physical hosts:

- In Windows:

```
environment-directory\jplpc\xxxx#1\store[\instance-name]#2\dump\pcsr.out
```

- In UNIX:

```
environment-directory/jplpc/xxxx#1/store[/instance-name]#2/dump/pcsr.out
```

#1

xxxx indicates the service key of PFM - Agent or PFM - RM. Every PFM - Agent or PFM - RM has a specific service key, such as `agto` for PFM - Agent for Oracle and `agtt` for PFM - Agent for Platform (Windows). For details on service keys, see the description of the naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

#2

If PFM - Agent or PFM - RM is monitoring an application program that can start multiple service sets on a host, there is one more directory created under the `store` directory bearing the same name as the instance name.

## 4.1.5 Checking the disk space used for performance data

You can use the Services window of PFM - Web Console to check the disk space used by the Store database.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.

You need to log on as a user with Administrator user permissions. You must have administrator user permissions to use the Services window.

2. In the navigation frame of the main window, select the **Services** tab.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by the service ID. The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.

4. Select an Agent Store or Remote Monitor Store service in the folder with the same name as the host for which you want to check the disk space.

If the product name display function is enabled, the Agent Store or Remote Monitor Store service is indicated by `host-name<service-key>(store)`.

If the product name display function is not enabled, an Agent Store or Remote Monitor Store service is indicated by the service with an ID that does not begin with a `P` and has an `S` as the second character. (Service IDs that begin with `PS` refer to a Master Store service.)

For details on service IDs, see the description of the service naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

The selected Agent Store or Remote Monitor Store service is marked with a checkmark.

5. In the method frame, select **Properties**.

6. In the Properties window for the Agent Store or Remote Monitor Store service, select the **Disk Usage** node in the tree.

Information about the disk space used by the database managed by the Agent Store or Remote Monitor Store service appears at the bottom of the Properties window.

## 4.1.6 Erasing performance data

You can erase the performance data that you no longer need from the Store database. Use the `jpctool db clear` command to erase data in the Store database.

Note:

You must execute the `jpctool db clear` command on the host where PFM - Manager is installed.

1. Log on to the host where PFM - Manager is installed.

You need to log on with special user permissions, as shown below:

- In Windows:  
Administrators or Backup Operators permissions
  - In UNIX:  
root user permissions
2. Execute the `jpctool service list` command to make sure that the Agent Store or Remote Monitor Store service managing the Store database from which you want to erase the performance data is up and running.
  3. Execute the `jpctool db clear` command to erase the specified record type of data stored in the Store database. For example, if you want to erase all of the performance data stored in the Store database on the host `host02` of PFM - Agent for Platform (Windows), use the following command:

```
jpctool db clear -id TS* -host host02 -dbid *
```

## 4.1.7 Importing backup data (with Store 2.0)

By importing backup data, you can make historical performance data available for reference. Use the `jpctool db import` command to import backup data, specifying either a full or additional import.

After the import process, the imported data can be viewed in parallel with the data in the Store database currently in use. When you import a unit database that covers a division period already represented in the Store database, the data in the Store database is given priority when performance data is displayed.

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool service list` command to make sure that the Agent Store or Remote Monitor Store service is running.
3. Execute the `jpctool db import` command.

Use the following commands:

For a full import:

When you execute the command, the files in the import directory are deleted and replaced with the backup files.

```
jpctool db import -key XXXX#1 -d D:\backup01#2
```

For an additional import:

When you execute the command, data is added to the backup files that are stored in the import directory.

```
jpctool db import -key XXXX#1 -d D:\backup01#2 -add
```

#1

xxxx indicates the service key of PFM - Agent or PFM - RM. Every PFM - Agent or PFM - RM has a specific service key, such as Oracle for PFM - Agent for Oracle and Windows for PFM - Agent for Platform (Windows). For details on service keys, see the description of the naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

#2

D:\backup01 indicates the backup directory.

### 4.1.8 Converting the data model of backup data (with Store 2.0)

When you upgrade PFM - Agent or PFM - RM, you can also upgrade the data model of the backup data. You cannot import backup data into Store 2.0 if the data model of the backup data is different from that used by the Store database.

If the data model of the backup data is an older version than that used by the Store database, you can use the `jpctool db dmconvert` command to upgrade the data model of the backup data, and then you can import it. The `jpctool db dmconvert -d` command requires free disk space in the specified directory that is equal to twice the size of the data to be converted.

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool db dmconvert` command.

Use the following command:

```
jpctool db dmconvert -d D:\backup01#
```

#

D:\backup01 indicates the backup directory.

### 4.1.9 Displaying information about the Agent Store and Remote Monitor Store services or backup directory (in Store 2.0)

You can check the version of the Store and the data model for the currently used service by viewing information on the Agent Store or the Remote Monitor Store service and the backup directory. Use the `jpconf db display` command to display the information.

Table 4–19: Items that can be displayed by the `jpconf db display` command

Item	Without -d option		With -d option
	Single-instance agent	Multi-instance agent	
Service key	Yes	Yes	Yes
Instance name	No	Yes	No

Item	Without -d option		With -d option
	Single-instance agent	Multi-instance agent	
Store version	Yes	Yes	Yes
Data model version	Yes	Yes	Yes

Legend:

Yes: Can be displayed.

No: Cannot be displayed.

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool service list` command to make sure that the Agent Store or Remote Monitor Store service is running.
3. Execute the `jpccconf db display` command.

Use the following command:

To display information about the backup directory:

```
jpccconf db display -d D:\backup01#
```

To display information about the Agent Store or Remote Monitor Store service:

```
jpccconf db display
```

#

D:\backup01 indicates the backup directory.

## 4.2 Managing event data

Event data is stored in the Store database managed by the Master Store service of PFM - Manager. In the Store database, you can:

- Change the maximum number of records for event data
- Change the storage location of event data
- Export event data
- Check the amount of disk space used by event data
- Erase event data

Note:

You cannot initialize the settings for the Store database that stores event data.

The steps for each procedure are described below. For details on how to modify the storage location for event data, see the chapters explaining installation and setup in the *JPI/Performance Management Planning and Configuration Guide*. For details on the commands used in this section, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

### 4.2.1 Changing the maximum number of records for event data

In the Services window of PFM - Web Console, you can change the number of event data records that the Store database can store for each agent or Remote Monitor Collector service.

Note:

You need to have Administrator user permissions to use the Services window.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You need to log on as a user with Administrator user permissions.
2. In the navigation frame of main window, select the **Services** tab.
3. In the navigation frame of the Services window, expand the hierarchy under the **PFM - Manager** folder.  
Services provided by PFM - Manager are displayed. The name of each service is represented by the service ID.
4. Select the Master Store service.  
The name of the Master Store service begins with **PS** or is **<Master Store>**.  
The selected Master Store service is marked with a checkmark.
5. In the method frame, select **Properties**.
6. In the Properties window for the Master Store service, select the **Retention** node from the tree.  
At the bottom of the information frame, the properties of the **Retention** node are displayed.  
Modify the property settings. The following table gives a description and setting for the property.

Table 4–20: Description and settings for each property

Record type	Property name	Settings
PA record type	Product Alarm - PA	Sets the maximum number of event data records to store for each agent or Remote Monitor Collector

Record type	Property name	Settings
PA record type	Product Alarm - PA	service. Set a value that satisfies the following equation as the number of event data records to store. $a \times \text{number-of-event-data-records-to-store} \times 0.015 < 2000$ (megabytes)

Legend:

*a*: Total number of the Agent Collector services, Remote Monitor Collector services, Remote Agents, and Group Agents to be connected

7. Click **Finish** or **Apply**.

Your settings are enabled.

## 4.2.2 Exporting event data

You can export the event data stored in the Store database to a text file. Use the `jpctool db dump` command to export data.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool service list` command to make sure that the Name Server, Master Manager, and Master Store services are all up and running.
3. Execute the `jpctool db dump` command.

For example, of the events in the Store database of the monitoring manager, if you want to export the events collected from 02:00:00 (GMT) to 14:59:00 (GMT) on July 10, 2006 to the file `pa.out`, use the following command:

```
jpctool db dump -id PS* -stime 2006/07/10 02:00 -etime 2006/07/10 14:59 -
f pa.out -dbid PA -rec *
```

When the command finishes normally, the export file for the event data is created in the following location:

On physical hosts:

- In Windows:  
`installation-folder\mgr\store\dump\pa.out`
- In UNIX:  
`/opt/jp1pc/mgr/store/dump/pa.out`

On logical hosts:

- In Windows:  
`environment-directory\jp1pc\mgr\store\dump\pa.out`
- In UNIX:  
`environment-directory/jp1pc/mgr/store/dump/pa.out`

## 4.2.3 Checking the disk space used for event data

You can use the Services window of PFM - Web Console to check the disk space used by the Store database.

Note:

You need to have Administrator user permissions to use the Services window.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You need to log on as a user with Administrator user permissions.
2. In the navigation frame of the main window, select the **Services** tab.  
The Services window appears.
3. In the navigation frame of the Services window, expand the hierarchy under the PFM - Manager folder.  
Services provided by PFM - Manager are displayed. The name of each service is represented by the service ID.
4. Select the Master Store service.  
The name of the Master Store service begins with **PS** or is **<Master Store>**.  
The selected Master Store service is marked with a checkmark.
5. In the method frame, select **Properties**.
6. In the Properties window for the Master Store service, select the **Disk Usage** node from the tree.  
The disk space used by the database managed by the Master Store service appears at the bottom of the Properties window.

## 4.2.4 Erasing event data

You can erase the event data stored in the Store database if the data is no longer required. Use the `jpctool db clear` command to erase data in the Store database.

Note:

You must execute the `jpctool db clear` command on the host where PFM - Manager is installed.

1. Log on to the host where PFM - Manager is installed.  
You need to log on as a special user with special permissions, as shown below:
  - In Windows:  
Administrators or Backup Operators permissions
  - In UNIX:  
root user permissions
2. Execute the `jpctool service list` command to make sure that the Name Server, Master Manager, and Master Store services are all up and running.
3. Execute the `jpctool db clear` command.  
To erase the event data stored in the Store database managed by the Master Store service, use the following command:

```
jpctool db clear -id PS* -dbid PA
```

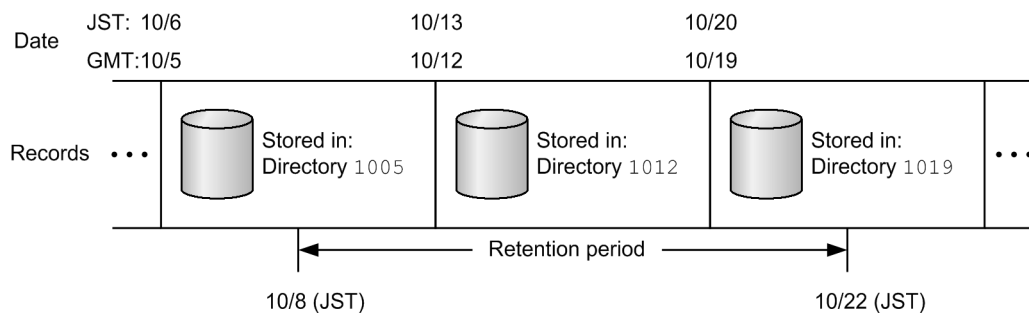


## 4.3 Notes on working with operation monitoring data in Performance Management

### 4.3.1 Record retention periods in the Store database

The names of the directories used to store the Store database data are based on the date on which data was first stored in the directory. The date is based on GMT. For this reason, in a system whose time zone is earlier than GMT, there might be more storage directories than the value specified for the retention period. For example, in a system set to JST (GMT +09:00), the name of the directory is based on the date nine hours before the point when data was first stored in the directory. As a result, the name of the directory can indicate an earlier date than the date from which the data in the directory was collected.

For example, in a system in the JST time zone with the retention period for weekly records set to 2 (weeks), weekly records will be stored across three directories. When the current date is October 22nd (Wed), the Store database contains records for the period from 10/8 to 10/22. The performance data for 10/8 is stored in the directory 1005, which is the GMT equivalent of the date (10/6) on which weekly records were first stored in the directory. Similarly, performance data for the current week is stored in the directory 1019. Accordingly, there are three storage directories, 1005, 1012, and 1019, as shown in the following figure.



### 4.3.2 Size limits that apply to the Store database

#### (1) With Store 2.0

With Store 2.0, data is stored in multiple files, each covering a specific time period. Also, the data for each record type is stored in a different data file. For this reason, a size limit of 2 GB applies to each individual data file, rather than to the total amount of data in the database. Also, you cannot exceed the file size limit imposed by the `ulimit` command on UNIX systems or other restrictions on the file system.

You can calculate the size of each data file by using an expression to estimate the amount of disk space occupied by the Store database and setting the retention period for historical data to zero. For the expression used to estimate the amount of disk space occupied by the Store database, see the appendix describing the amount of disk space occupied by the Store database (Store version 2.0) for PFM - Agent 08-00 and later in the *JP1/Performance Management Planning and Configuration Guide*, or an appropriate PFM - Agent manual.

Data for each record type is written to a data file in the Store database that is switched periodically. If the size of the data file reaches the limit within the allotted time period, the KAVE00227-W message is output, and no more data of that record type is written to the database. However, the Agent Store and Remote Monitor Store services continue to run.

When the allotted time period elapses and the data file is switched, the KAVE00228-I message is output and the Agent Store and Remote Monitor Store services resume writing data to the database.

## (2) With Store 1.0

The maximum overall file size of the Store database used in Performance Management is 2 GB. Also, you cannot exceed the file size limit imposed by the `ulimit` command on UNIX systems or other restrictions on the file system.

The Store service stops when the file size of the Store database has reached the limit.<sup>#</sup> In this case, the KAVE00182-E message is output to the system log (Windows Event Log in Windows or `syslog` on UNIX systems) and the common message log.

#

If this symptom occurs, the Agent Store service stops, but the Agent Collector service does not stop.

If the file size of the Store database has reached the limit, perform the following steps:

1. Access the Agent Collector properties from PFM - Web Console, and change the settings so that no records are collected.

In this situation, only the Agent Store service stops. The Agent Collector service is still running.

2. Use the `jpccspm start` command to restart the Agent Store service.

For details on the `jpccspm start` command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

3. Back up data.

To do so, use the `jpctool db dump` or `jpccrpt` command, or output reports to a file in CSV or HTML format. For details on how to use the `jpctool db dump` command to back up performance data and event data, see [4.1.4 Exporting performance data](#) and [4.2.2 Exporting event data](#), respectively.

For details on the `jpccrpt` command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

For details on how to output reports to files in CSV or HTML format, see [5.9.1 Exporting reports in CSV or HTML format by using a Web browser](#).

4. Erase data.

Erase the performance data. For details on how to erase performance data and event data, see [4.1.6 Erasing performance data](#) and [4.2.4 Erasing event data](#), respectively.

5. Access the Agent Collector properties from PFM - Web Console.

Configure the Agent Collector service to collect records, and then resume operation.

### 4.3.3 When the Agent Store or Remote Monitor Store service stops abnormally

- If the Agent Store or Remote Monitor Store service stops abnormally while writing to the Store database, an integrity check is performed as part of the startup process the next time the Agent Store or Remote Monitor Store service is started. Any invalid data found during the integrity check could be lost.
- If the Agent Store or Remote Monitor Store service could not finish normally (for example due to a power failure), the service reconstructs the index of the Store database at the next startup. In this case, the Agent Store or Remote Monitor Store service might take longer than usual to start.

## 4.3.4 When the system has insufficient disk capacity

The Store database stops accepting more data when it cannot use sufficient required disk space. If this occurs, a KAVE00105-E message is output, and the Master Store, Agent Store, or Remote Monitor Store service stops.

If you receive the above message, perform one of the following procedures:

- Reserve sufficient disk space
- Reduce the disk space occupied by the Store database

### (1) Reserving sufficient disk space

Estimate how much disk space is used by the Store database and change the storage location of the Store database to a disk with enough free space. For details on how to estimate the amount of disk space occupied by the Store database, see the appendix describing system estimation in the appropriate PFM - Agent or PFM - RM manual. For details on how to change the storage location of the Store database for event data, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*. For details on how to change the storage location of the Store database for performance data, see the appropriate PFM - Agent or PFM - RM manual.

### (2) Reducing the disk space occupied by the Store database (Store 1.0 only)

First, you must change the current settings to decrease the maximum size of the disk space occupied exclusively by the Store database. To decrease the maximum size of data, you can restrict the number or type of records to be collected by the Agent Collector service, or set shorter retention periods or smaller numbers of stored records to be kept by the Store database. For details on how to change which records are collected by the Agent Collector service, see [4.1.1 Modifying the recording options for performance data](#). For details on how to change the retention conditions for the Store database, see [4.1.3 Modifying the retention conditions for performance data \(in Store 1.0\)](#) and [4.2.1 Changing the maximum number of records for event data](#).

You cannot, however, reduce the disk space occupied exclusively by the Store database only by setting the maximum size of data. To reduce the occupied disk space, perform the following procedures:

#### (a) For the Store database of the Agent Store service:

Follow steps 1-3 below:

1. Delete the performance data for records in the Store database that are no longer needed.

In the Store database, unnecessary data for a particular record is deleted when new performance data of that record is stored. If you configure the Agent Collector service to no longer collect particular records, the performance data for those records remains in the Store database, and the amount of disk space occupied by the Store database remains the same. Perform the following procedure to delete the performance data of records that are no longer being collected from the Store database. This procedure is not required for the Store database of the Master Store service, or for when you have not configured any records not to be collected by the Agent Collector service.

The following procedure shows an example of how to delete data of unwanted records from the Store database.

For example, suppose you are using PFM - Agent for Platform, and want to change the collection settings from *Yes* for *PI\_LOGD*, *Yes* for *PI\_NIND*, and *Yes* for *PD\_PD* to *No* for *PI\_LOGD*, *Yes* for *PI\_NIND*, and *No* for *PD\_PD*:

(1) Set *Yes* for records that you no longer want collected. Set *No* for all other records. In this example, set *Yes* for *PI\_LOGD* and *PD\_PD*, and *No* for the others.

(2) Modify the retention conditions as follows:

- For *PD* and *PL* record types, set the maximum number of records to 0.

- For the PI record type, set the retention period of records to the minimum for each collection period. For example, set `Minute` for performance data stored in minutes and `Hour` for performance data stored in hours.

(3) Store the performance data in the Store database at least once.

Note 1: For details on the timing when the performance data is stored in the Store database, see the chapter that describes the Performance Management functions in the *JP1/Performance Management Planning and Configuration Guide*.

Note 2: Tasks (1) to (3) invalidate the area in the Store database occupied by the records that you no longer want to collect (in this example, `PI_LOGD` and `PD_PD`). The invalidated areas can be eliminated from the database file by reorganizing the Store database. Note that you might be unable to invalidate the entire area occupied by the performance data if the record is a PI-type record or a Process Detail (PD) record of PFM - Agent for Platform. For details, see *[Notes about the data that cannot be deleted from the Store database even by storing the performance data of the record]* below.

(4) Set `No` as the collection setting for all records.

(5) Set your desired retention conditions of the Store database.

(6) Set your desired collection configurations.

## 2. Deleting the extra performance data in the Store database

If you reduce the number of records kept by the Store database or set shorter retention periods, you will have more performance data in the Store database than the retention conditions allow. This is because the data stored by using previous retention conditions still remains intact. If this is the case then you must perform the following procedure to delete the extra performance data that does not match the new retention conditions. This procedure is only required when you have set shorter retention periods or smaller numbers of stored records to be kept by the Store database.

(1) Set your desired retention conditions of the Store database.

(2) In the Store database store, at least once, the performance data of the records for which you modified the retention conditions.

Note 1: For details on the timing when the performance data is stored in the Store database, see the chapter that describes the Performance Management functions in the *JP1/Performance Management Planning and Configuration Guide*.

Note 2: The area of the performance data for a record that no longer matches the retention conditions is invalidated when a new record is stored and performance data in the Store database is increased. The invalidated areas can be eliminated from the database file by reorganizing the Store database. Note that you might be unable to invalidate the entire area occupied by the performance data if the record is a PI-type record or a Process Detail (PD) record of PFM - Agent for Platform. For details, see *[Notes about the data that cannot be deleted from the Store database even by storing the performance data of the record]*.

## 3. Reorganizing the Store database

Reorganize the Store database to reduce the disk space occupied exclusively by the Store database. For details on how to reorganize the Store database, see *4.3.5 Checking the database size and reorganizing the Store database*.

*[Notes about the data that cannot be deleted from the Store database even by storing the performance data of the record]*

When the performance data of a record is stored in the Store database, the area of the performance data for a record that does not match the retention conditions is invalidated when the performance data of the record increases in the Store database. There are, however, some records in the Store database where storing additional performance data for them does not increase the size of the data. None of the performance data for these records shall be invalidated. Records of PI record type or of the Process Detail (PD) of the PFM - Agent for Platform fall under this category.

In the case of the PI record type, in a summary block where new performance data is created by the process of storing performance data, the performance data for that summary block is deleted from the Store database. When new performance data is not created, the data remains in the Store database. Note that the performance data in the summary block of `year` always remains. For example, suppose that the Store database contains performance data for the `PI-LOGD` record that was all collected before 16:00:00 on May 23, 2006 (Tuesday), and you store performance

data for the `PI_LOGD` record at 10:00:00 on May 24, 2006 (Wednesday). The performance data in the summary block of `year` remains in the database. The performance data for May 2006 is consolidated into the performance data in the summary block of `month`, so no new performance data is created. Accordingly, all the performance data of the `PI_LOGD` record in the summary block of `month` remains in the Store database. Similarly, all the performance data in the summary block of `week` remains in the Store database. For the performance data in the summary block of `day`, the new performance data for May 24, 2006 is created, so all of the performance data of the `PI_LOGD` record in the summary block of `day` is invalidated in the Store database. Similarly, all of the performance data in the summary block of `hour` and `minute` is invalidated. Count all the remaining performance data in when you estimate the disk space occupied exclusively by the Store database.

In case of the Process Detail (PD) record of the PFM - Agent for Platform, when there is no difference between the data last collected and the one that has just been collected, the performance data remains in the Store database. For details on the Process Detail (PD) record of PFM - Agent for Platform, see the chapter explaining records in the manual *JPI/Performance Management - Agent Option for Platform Description, User's Guide and Reference*. Either make differences so that the old performance data will be deleted, or add such space as required for the Process Detail (PD) record to the estimated disk space occupied exclusively by the Store database when you operate the system.

## **(b) For the Store database of the Master Store service:**

Perform steps 1. to 3. below.

1. Set your desired retention conditions for the Store database.
2. Store the event data in the Store database at least once.

Note 1: For details on the timing when the event data is stored in the Store database, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.

Note 2: The area of the data that no longer matches the retention conditions is invalidated when event data for the record is stored in the Store database. The invalidated area can be deleted from the database file by reorganizing the Store database.

3. Reorganize the Store database.

Reorganize the Store database to reduce the disk space occupied exclusively by the Store database. For details on how to reorganize the Store database, see [4.3.5 Checking the database size and reorganizing the Store database](#).

If the Master Store service or the Agent Store service does not start even after taking these actions, there might be some unrecoverable logical errors in the Store database. In this case, you must restore the Store database from the backup data, and then restart the Master Store service or the Agent Store service. If you have no backup data, you must initialize the Store database, and then start the Master Store service or the Agent Store service. To initialize the Store database, delete all the files indicated below from the storage directory of the Store database.

- Files with the extension `.DB`
- Files with the extension `.IDX`

The default storage directories of the Store database are listed below.

The storage directory of the Store database for performance data:

For details, see each of the PFM - Agent manuals.

The storage directory of the Store database for event data:

- In Windows:  
`installation-folder\mgr\store\`
- In UNIX:

/opt/jplpc/mgr/store/

You can change the storage directories of the Store database for event data in the `jpctesto.ini` file. For details on how to change the storage directories, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

## 4.3.5 Checking the database size and reorganizing the Store database

The Store database consists of the data files, which store the actual data, and the index files, which manage the data indices for faster access. With Store 1.0, deleting data in the data files only invalidates the area of that data, and the size of the files does not decrease automatically. Although the invalidated area in the data files is reused, the reusing rate might suffer when the number of instances to store performance data varies with each collection, causing the size of the Store database to exceed the estimated size of the exclusively occupied disk space. For this reason, when using Store 1.0, we recommend that you check the size of the Store database regularly, and reduce the invalidated area by reorganizing the Store database when it occupies more than 90% of the estimated disk space. You do not need to reorganize the database when using Store 2.0.

### (1) Checking the size of the Store database

Check the sizes of all the files with extensions `.DB` and `.IDX` in the storage location of the Store database, and calculate the total size of the files. With Store 1.0, when the total size exceeds 90% of the estimated disk space, perform the following procedure to reorganize the Store database.

### (2) Reorganizing the Store database (Store 1.0 only)

1. Start the Performance Management service that will manage the Store database you want to reorganize.  
By using the `jpccspm start` command, start the PFM - Agent or PFM - Manager service to manage the Store database you want to reorganize, if it is not running already.
2. Use the `jpctool db backup` command to back up the Store database.  
Execute the `jpctool db backup` command to back up the Store database that you want to reorganize. The `jpctool db backup` command extracts data from the data file, except in the invalidated area, and saves the data.  
Note:  
For the `jpctool db backup` command to work properly, the corresponding backup file requires more than double the total size of the Store database calculated above. Make sure that you have enough free space before you run the command.
3. Stop the service of Performance Management that has been managing the Store database that you want to reorganize.  
By using the `jpccspm stop` command, stop the PFM - Agent or PFM - Manager service that has been managing the Store database that you want to reorganize.
4. Use the `jpctool db restore` command to restore the Store database.  
Execute the `jpctool db restore` command to restore the Store database from the backup you made in step 2.
5. Start the service of Performance Management.  
If necessary, start the service that you stopped in step 3 by issuing the `jpccspm start` command.



### 4.3.6 Deleting files and folders that remain in the system after exceeding the retention period

Records are automatically deleted only if they exceed the retention period and corresponding new records are collected. Therefore, if previously collected records are set so that they are not to be collected again, the record data will not be deleted.

To delete such unnecessary records and folders:

1. Use the `jpcspm stop` command to stop PFM - Agent or PFM - RM.
2. Search the appropriate directory in the Store database for DB/IDX files that contain the name of the record (*database-ID\_record-type*, such as `PI_PI`) you want to delete.
3. Manually delete the files that were found by the search.
4. When the DB/IDX files are deleted in step 3, some folders with names that consist of dates (such as 1212 and 1219) might be left empty. If so, delete these empty folders as well.

### 4.3.7 Default retention periods for records in Store 2.0

Store 2.0 can be used with version 08-11 or later of PFM - Manager or PFM - Base combined with version 08-00 or later of PFM - Agent for Platform. The default retention period of records differs whether PFM - Agent 08-11 or later is used or PFM - Agent 08-00 is used.

When PFM - Agent 08-11 or later is used:

For details on the default retention period of records, see the appropriate PFM - Agent manual.

When PFM - Agent 08-00 is used:

For PD-type and PL-type records, the default retention period of all records will be set to 10 days. The following table describes the default retention period of the PI record type.

Table 4–21: The default retention period of the PI record type

Retention period before setup	Retention period after setup				
	Summarization category				
	Minute (unit: days)	Hour (unit: days)	Day (unit: weeks)	Week (unit: weeks)	Month (unit: months)
1 minute	1	--	--	--	--
1 hour	1	1	--	--	--
1 day	1	1	1	--	--
2 days	2	2	1	--	--
3 days	3	3	1	--	--
4 days	4	4	1	--	--
5 days	5	5	1	--	--
6 days	6	6	1	--	--
1 week	7	7	1	1	--

Retention period before setup	Retention period after setup				
	Summarization category				
	Minute (unit: days)	Hour (unit: days)	Day (unit: weeks)	Week (unit: weeks)	Month (unit: months)
1 month	31	31	5	5	1
1 year	366	366	54	54	12

Legend:

--: Item that cannot be specified

### 4.3.8 Performance data stored after a data model upgrade

Upgrading the data model can result in a new field being added to existing records. If this occurs, the default performance data is stored in the Store database that existed prior to the upgrade. The following table lists the performance data stored by default.

Table 4–22: Performance data to be stored by default

Data type of the field	Performance data to be stored
char	Empty
double	0
float	0
long	0
short	0
string	Empty
time_t	0
timeval	0
ulong	0
utime	0
word	0
(Not applicable)	0



# 5

## Creation of Reports for Operation Analysis

This chapter describes how to create reports, and how to display and output reports based on performance data collected by Performance Management.

## 5.1 Overview of reports

---

### 5.1.1 About reports

Performance Management displays performance data collected by PFM - Agent or PFM - RM in the window of PFM - Web Console in graphical formats such as tables or graphs, allowing you to check and analyze the system operating status. Performance data represented in formats such as tables or graphs is called a *report*.

Define the information and conditions for displaying data in the report beforehand. There are several ways to define reports: use the *monitoring template* as is, use a customized monitoring template, or define a report by yourself.

### 5.1.2 Report types

There are two types of reports: *realtime report* and *historical report*.

#### *Realtime report*

Use this type of report to check the system status and problems at that time. You can specify settings so that a report is automatically updated at specified times and the latest data is displayed in the report. A realtime report collects performance data when the report is displayed, so realtime reports do not use the Store database.

#### *Historical report*

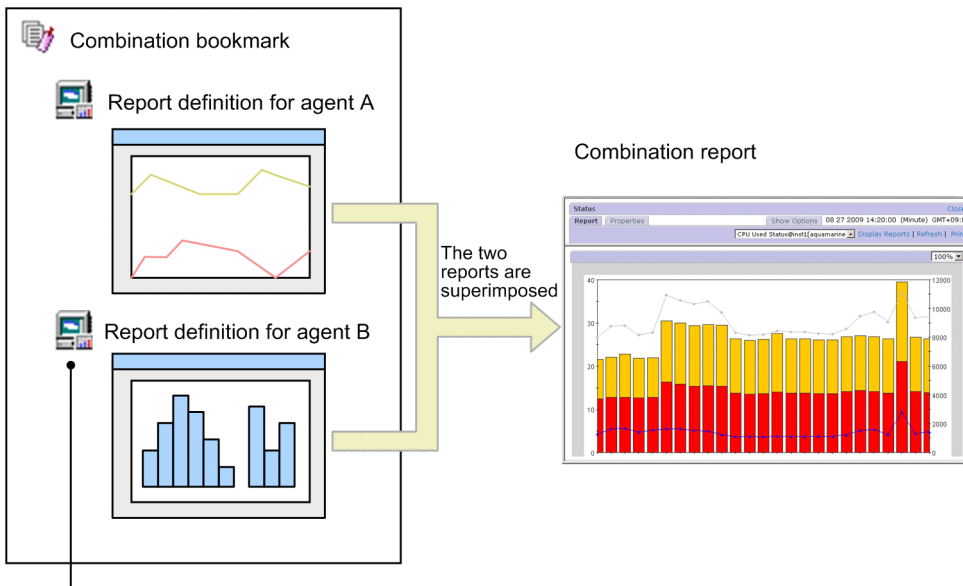
Create this type of report to analyze the trend of the system operating status from historical data until the present. Since past data must be retained, the historical report records performance data in the Store database. For details on how to record data into the Store database, see [4.1.1 Modifying the recording options for performance data](#).

Performance Management provides both normal and combination reports. A *combination report* combines multiple historical reports in the same graph. By registering reports that combine report definitions from multiple agents in a bookmark or combination bookmark, you can display reports and combination reports right away without needing to select each agent individually.

In addition to registered reports, combination bookmarks allow you to save reports created during a specific period in the past as reference reports for validating registered reports. Reports used as reference reports for validating registered reports are called *baselines*. By defining and managing multiple registered reports and baselines in a combination bookmark, you can display them on the same graph as a combination report. Such combination reports allow you to ascertain the operating status of the system in its entirety.

The following figure shows the relationship between the definition of a combination bookmark and a combination report.

Figure 5–1: Relationship between combination bookmark definition and combination report



Each agent-specific report registered in a combination bookmark is called a *registered report*.

As shown in the figure, by creating a combination bookmark that contains report definitions for more than one agent, you can display multiple reports in one graph. For example, you can visually check the correlation between the number of transactions handled by the HTTP service and its response time by superimposing the two values in a combination report.

For details on how to display normal reports, see [5.7 Displaying reports](#). For details on how to display combination reports, see [5.8 Displaying combination reports](#).

### 5.1.3 Display formats of reports

You can display reports as *tables*, *lists*, or *graphs*, whichever best meets your purpose.

#### (1) Tables

You can display historical data accumulated in a time sequence in table format. This format is suitable for seeing changes in each field value in a time series. The following figure shows an example of a table.

Figure 5–2: Example of a table





						First	Previous	1 - 20 OF 828	Next	Last
Date and Time	CPU %	Page Faults/sec	User CPU %	Threads (Total)	Date and Time					
06 05 2006 20:06:00	70.0738	1,700.0935	42.3339	940.0000	06 05 2006 20:06:00					
06 05 2006 20:07:00	8.3464	256.6573	3.6255	949.0000	06 05 2006 20:07:00					
06 05 2006 20:08:00	10.4551	81.6565	3.9272	946.0000	06 05 2006 20:08:00					
06 05 2006 20:09:00	8.4996	87.1172	4.0425	949.0000	06 05 2006 20:09:00					
06 05 2006 20:10:00	11.8752	102.5190	5.3161	952.0000	06 05 2006 20:10:00					
06 05 2006 20:11:00	1.6385	50.7475	0.9623	948.0000	06 05 2006 20:11:00					
06 05 2006 20:12:00	1.8466	83.1560	0.9623	945.0000	06 05 2006 20:12:00					
06 05 2006 20:13:00	1.2484	42.2945	0.7802	942.0000	06 05 2006 20:13:00					
06 05 2006 20:14:00	1.2741	39.0139	0.6760	941.0000	06 05 2006 20:14:00					
06 05 2006 20:15:00	1.4824	43.2589	0.7542	942.0000	06 05 2006 20:15:00					
06 05 2006 20:16:00	1.3524	42.2784	0.7802	941.0000	06 05 2006 20:16:00					
06 05 2006 20:17:00	1.6645	76.2327	0.8062	938.0000	06 05 2006 20:17:00					
06 05 2006 20:18:00	25.8518	134.0579	20.4161	947.0000	06 05 2006 20:18:00					
06 05 2006 20:19:00	29.1027	52.1157	25.0715	944.0000	06 05 2006 20:19:00					
06 05 2006 20:20:00	47.4642	287.1514	37.9194	947.0000	06 05 2006 20:20:00					
06 05 2006 20:21:00	42.8497	68.1587	35.5694	944.0000	06 05 2006 20:21:00					
06 05 2006 20:22:00	1.3210	34.9386	0.6605	936.0000	06 05 2006 20:22:00					
06 05 2006 20:23:00	2.5748	78.0643	1.1183	941.0000	06 05 2006 20:23:00					
06 05 2006 20:24:00	2.2627	52.4300	1.1704	940.0000	06 05 2006 20:24:00					
06 05 2006 20:25:00	11.3595	157.0211	6.5506	944.0000	06 05 2006 20:25:00					

## (2) Lists





You can display field values for each agent or instance in list format. This format is especially suitable for displaying multiple agents or instances.

The following figure shows an example of a list.

Figure 5–3: Example of a list

	<b>Date and Time</b>	2006 02 21 15:00:00
	<b>CPU %</b>	96.4544
1	<b>Page Faults/sec</b>	1,015.1283
OF	<b>User CPU %</b>	83.8529
1	<b>Threads (Total)</b>	28,645.0000
		
		

The list data is displayed for each data group. A data group is a group in which data with different agents or instances are organized by time.

To display information about other agents or instances in the same data group, click the  or  button at the left of the list. To display information for another data group, click the  or  button in the menu bar of the View Report window.

## (3) Graphs

Reports can be displayed in a variety of graphs. You can specify the most appropriate graph depending on the graph characteristics, the number of data instances, and the number of agents to be handled. An element displayed in a graph is called a *field*. In a report definition, you can specify the fields to be displayed in a graph. You can set numerical fields only.

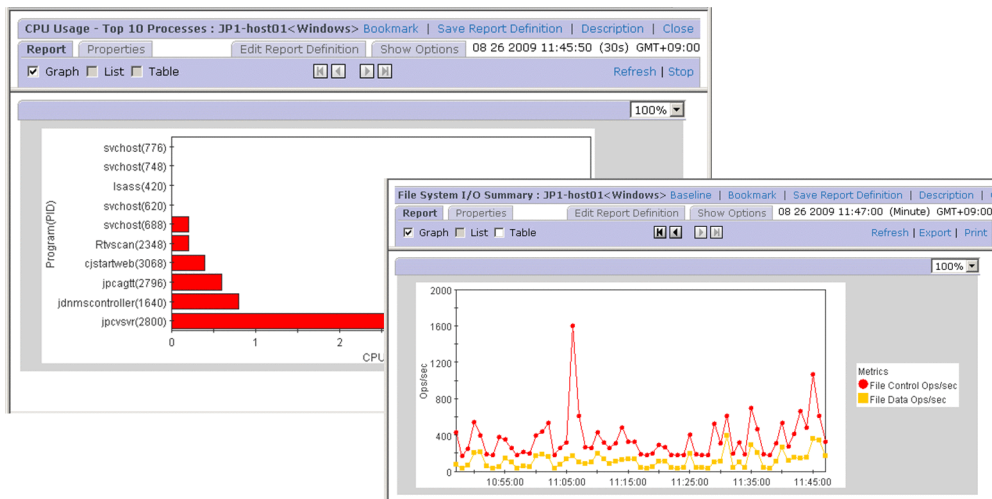
The graph types are as follows:

- Column graph
- Stacked column graph

- Bar graph
- Stacked bar graph
- Pie graph
- Line graph
- Area graph
- Stacked area graph

The following figure shows examples of graphs.

Figure 5–4: Examples of graphs



## 5.2 Overview and procedure for report creation

---

### 5.2.1 How to create reports

Create a report by using the Reports window of PFM - Web Console, the Quick Guide, or a command.

You can create a report in the following ways:

- Creating a new report

To create a new report to match your system environment, define a new report. You can also create a simplified report by using the Quick Guide.

- Using an existing report

You can use the following methods:

- Use the monitoring template.

The monitoring template is a set of reports, for which necessary information has been preset, included with each PFM - Agent or PFM - RM. When you use the monitoring template, at PFM - Agent or PFM - RM startup the system can start collecting the performance data required for displaying a report of the monitoring template, and can create the report.

- Customize the monitoring template.

You can copy the monitoring template and customize it to match your monitoring objectives.

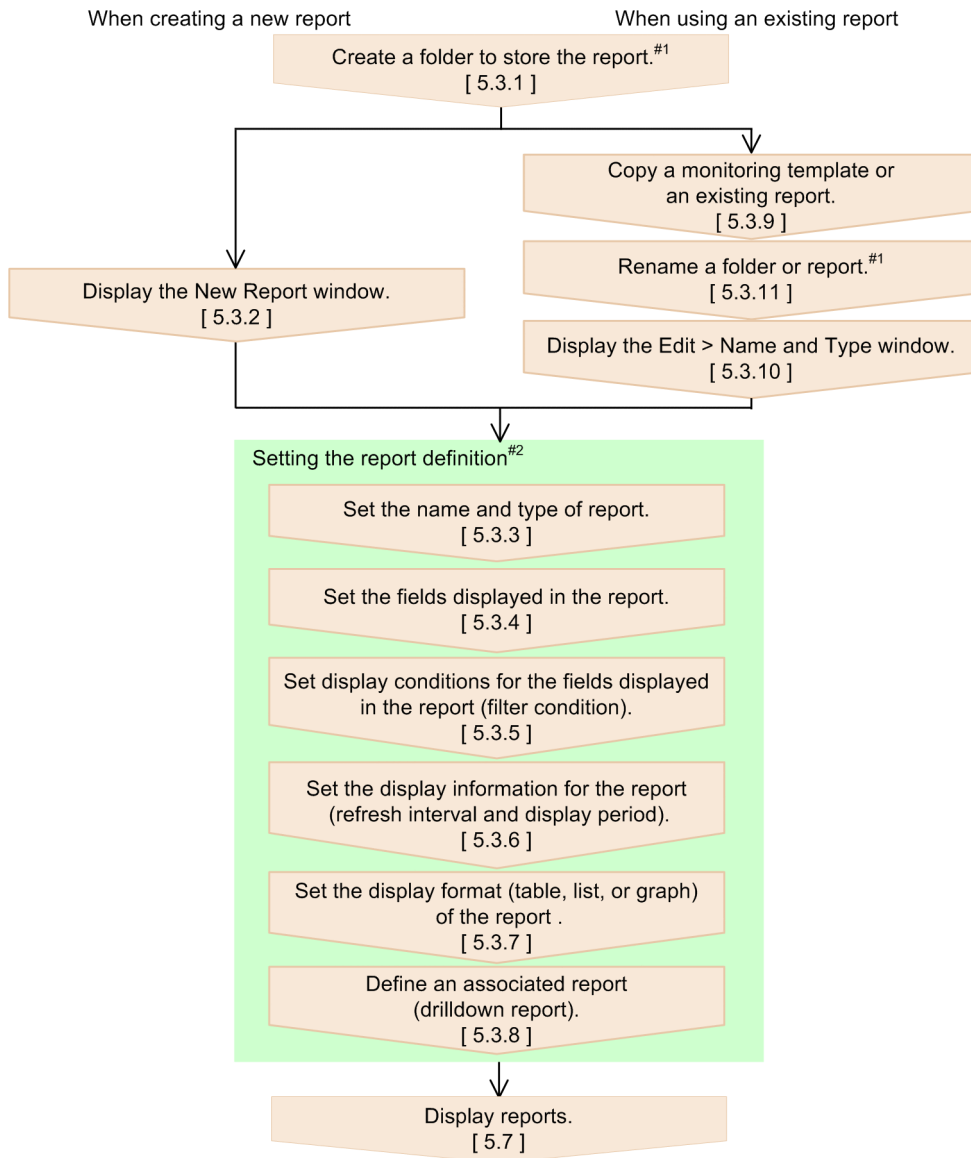
- Use a created report.

You can copy and customize a created report.

### 5.2.2 Process flow for creating reports

The following figure shows the process flow for creating a report. You can also use the Quick Guide to create reports. For details on how to create reports using the Quick Guide, see [5.4 Creating reports in the Web browser \(Quick Guide\)](#).

Figure 5–5: Process flow for creating a report (from defining to displaying a report)



Legend: [ ] : See the indicated section.

#1 Perform as needed.

#2 Edit as needed when using an existing report.

## 5.3 Creating reports in the Web browser (Reports tree)

---

For details on how to create a report by using commands, see [5.5 Creating reports by using commands](#).

You can use the Quick Guide to create simplified reports. For details on how to create reports using the Quick Guide, see [5.4 Creating reports in the Web browser \(Quick Guide\)](#).

### 5.3.1 Creating a report folder

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the Reports tree in the navigation frame of the Reports window, select **User Reports** or one of its subfolders in which to create the folder.  
The selected folder is marked with a checkmark.
4. In the method frame, select **New Folder**.
5. In the New Folder window in the information frame, enter a folder name in **New name of the folder**.

#### **New name of the folder**

Enter the folder name using 1 to 64 single or double-byte characters. You can enter a combination of single and double-byte characters.

6. Click the **OK** button.  
A folder is added in the **User Reports** folder selected in step 3 or below the folder.  
The following figure shows an example of creating a report folder:

### 5.3.2 Displaying the New Report window

Create a new report in the New Report window of the Reports window.

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the Reports tree in the navigation frame of the Reports window, select the folder in which you want to store the report.  
The selected folder is marked with a checkmark.
4. In the method frame of the Reports window, select the **New Report** method.  
In the information frame, the New Report > Name and Type window appears. Go to [5.3.3 Setting the name and type of a report](#).

### 5.3.3 Setting the name and type of a report

1. In the New Report > Name and Type window, set **Report name** and **Product**.



## Report name

Enter a report name of 64 or fewer single or double-byte characters. You can enter a report name that contains single and double-byte characters.

## Product

Select the data model version to be used.

For example, to define a realtime report of the top ten processes whose CPU usage ratio is high, whose Agent is PFM - Agent for Platform (Windows), and whose data model version is 6.0, specify the following settings:

**Report name:** CPU Usage - Top 10 Processes

**Product:** Windows (6.0)

## 2. Select Report type.

**Report type** has the following three types:

- **Realtime (Single Agent)**

This is a realtime report for displaying the status of the system at that time. The report collects and displays the data of a single agent at that time, ranks collected values, and displays these rankings. However, past data is not stored in the Store database, so you cannot retrieve and display such data. Realtime (Single Agent) reports handle single-instance and multi-instance records.

- **Historical (Single Agent)**

This is a historical report for collecting and displaying the data of a single agent. A report is displayed in a single View Report window for a single agent. If you select multiple agents, as many View Report windows as selected agents are displayed. Historical (Single Agent) reports handle single-instance and multi-instance records.

- **Historical (Multiple Agents)**

This is a historical report for collecting and displaying the data of multiple agents. A single View Report window is displayed regardless of whether one or more agents are selected. Historical (Multiple Agents) reports handle single-instance records only.

If this item is selected, you cannot select multi-row records (multi-instance records) in the next New Report > Field window.

The default is **Realtime (Single Agent)**.

For details on single-instance records and multi-instance records, see the chapter that describes the Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.

## 3. Click the Next > button.

The New Report > Field window appears. Go to [5.3.4 Setting fields displayed in a report](#).

### Note: Data model version and compatibility

The contents of the data model might vary according to the version, but upward compatibility is guaranteed. Therefore, if you create a report using an old data model, you can display a report in PFM - Agent or PFM - RM of a newer data model. For example, a report created in PFM - Agent for Platform Windows (3.0) can display the data of any version of PFM - Agent for Platform (Windows), but a report created in PFM - Agent for Platform Windows (4.0) can only display the data of version 07-00 and later of PFM - Agent for Platform (Windows). Depending on the PFM - Agent or PFM - RM, you can select multiple data model versions. For details on data model versions and compatibility, see the description of the compatibility among data model versions in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

### Note: When selecting a historical report

As a historical report uses past data, you must specify that the records of the monitoring performance data be recorded into the Store database. Make sure that the monitoring records have been set up to be recorded. For details on how to record the data into the Store database, see [4.1.1 Modifying the recording options for performance data](#).

## 5.3.4 Setting fields displayed in a report

The records and fields of the performance data set here might vary according to the agent. For details on records and fields for each agent, see the chapter describing the records in each PFM - Agent or PFM - RM manual.

If you want to use characters to search for a field, click the **Search fields** button in the New Report > Field window. For details on how to search for fields, see [5.3.4\(1\) Searching for fields](#).

1. Select the records to be displayed in the report in **Record** of the New Report > Field window.

If you select records, the fields of the selected records are displayed in **All fields**.

Note:

In the New Report > Name and Type window, if **Historical (Multiple Agents)** is selected as a report type, only single-row records can be selected in **Record**.

Reference note: Description of Record and Fields window


When you click the **Description** button to the right of **Record**, the Description of Record and Fields window is displayed for the product you selected in the New Report > Name and Type window.

Reference note: About single-row records and multi-row records


The description (**This is a single-instance record.**) or (**This is a multi-instance record.**) is displayed under **Record**. These messages indicate the record type. A single-row record indicates a single-instance record, and a multi-row record indicates a multi-instance record. For details on single-instance and multi-instance records, see the chapter describing Performance Management functions in the *JPI/Performance Management Planning and Configuration Guide*.



2. In **All fields**, select the fields to be displayed in the report.

Selected fields are displayed as selected. Use the **Shift** or **Ctrl** key to select multiple fields at a time.

3. Click the move button (  ).

The fields selected in step 2 are moved to **Selected fields**.

To undo a field already moved to **Selected fields**, select the fields to be undone in **Selected fields** and click the move button (  ).

Also, select the fields in **Selected fields** and click the move button (  ) or the move button (  ) to sort the fields. The order to be specified here will also apply to the order of fields in tables, lists, and graphs.

An example of settings in the New Report > Field window is as follows.

For a realtime report of the top ten processes whose CPU usage ratio is high and whose agent is PFM - Agent for Platform (Windows), if you specify three for the fields of Process Detail (PD) records, namely CPU % (PCT\_PROCESSOR\_TIME), PID (ID\_PROCESS), and Program (INSTANCE), set this window as follows:

**Record:** Process Detail (PD)

**Selected fields:** PID, Program, CPU %

4. Click the **Next >** button.

The New Report > Filter window appears. Go to [5.3.5 Setting display conditions for fields displayed in a report \(filter condition\)](#).

### (1) Searching for fields

The search results are included in **Selected fields** in the New Report > Field window.

1. Click the **Search fields** button in the New Report > Field window.

2. In the New Report > Field > Search Fields window, select the records you want to search from the **Records to search** pull-down menu.

The items of the pull-down menu are as follows:

- **--All records--**

Select this to search all records.

- A list of record names of the selected agent

A list of record names of the selected agent is displayed in alphabetical order.

3. Enter in **Keywords to find** the characters that you want to search for in a field, and then click the **Search** button.

- If **--All records--** is selected as the target

The search results are listed for each record in the Search results: record(s) window.

If you click the anchor part of the record name, the search results are listed in the New Report > Field > Search Fields window by field.

- If a record name is selected as the target

The searched fields are listed in the New Report > Field > Search Fields window.

4. Select the check boxes for the fields you want to select, and then click the **OK** button.

The New Report > Field window from which you opened the New Report > Field > Search Fields window appears, and the selected fields are added to **Selected fields**.

### 5.3.5 Setting display conditions for fields displayed in a report (filter condition)

Setting the display conditions for fields displayed in a report allows you to filter the data to be displayed in the report so that the displayed data best matches your purpose. You can also set multiple filter conditions.

1. In **Field** of the New Report > Filter window, select the fields to be filtered.

2. Set the display conditions for the fields.

For example, for a realtime report of the top ten processes whose CPU usage ratio is high and whose agent is PFM - Agent for Platform (Windows), if you specify the condition that the value of PID (ID\_PROCESS) field is not 0 for Process Detail (PD) records, set as follows:

**Field:** PID

**Condition:** <>

**Value:** 0

3. Click the **Add** button.

The condition set in step 2 is added to **Conditional expression**.

**Conditional expression:** PID <> "0"

If no conditional expression is set in **Conditional expression**, the report is registered as a report without any conditional expression.

4. Click the **Next >** button.

- When the report type is **Realtime (Single Agent)**:

The New Report > Indication settings (Realtime) window appears. Go to [5.3.6\(1\) Setting the display information for a realtime report](#).

- When the report type is **Historical (Single Agent)** or **Historical (Multiple Agents)**:  
The New Report > Indication settings (Historical) window appears. Go to [5.3.6\(2\) Setting the display information for a historical report](#).

Reference note: If you want to set filter conditions while displaying a report

If you select **Specify when displayed**, you can set filter conditions while displaying a report. Do not select **Specify when displayed** if you want to display a report using conditions defined beforehand in the New Report > Filter window.

## 5.3.6 Setting the display information for a report (refresh interval and display period)

The settings for a report here might differ depending on whether the report type is realtime or historical.

- When a realtime report is selected:  
Make sure that the New Report > Indication settings (Realtime) window has been displayed, and then go to [5.3.6\(1\) Setting the display information for a realtime report](#).
- When a historical report is selected:  
Make sure that the New Report > Indication settings (Historical) window has been displayed, and then go to [5.3.6\(2\) Setting the display information for a historical report](#).

### (1) Setting the display information for a realtime report

1. Set the display information.

For example, when defining a realtime report of the top ten processes whose CPU usage ratio is high in PFM - Agent for Platform (Windows), you could use the following conditions to set the display information for a realtime report of Process Detail (PD) records:

Conditions:

- The values of data displayed in the report are Delta values.
- The automatic refresh interval of the report display is initially set to 60 seconds and has a minimum of 30 seconds.
- Display the top ten data using the CPU % (PCT\_PROCESSOR\_TIME) field as the display criteria.

Set as follows:

**Specify when displayed:** Select

**Indicate delta value:** Select

Refresh interval

**Do not refresh automatically:** Do not select

**Initial value:** 60

**Minimum value:** 30

Display by ranking

**Field:** CPU%

**Display number:** 10

**In descending order:** Do not select

2. Click the **Next >** button.

The New Report > Components window appears. Go to [5.3.7 Setting the display format \(table, list, or graph\) of a report](#).

## (2) Setting the display information for a historical report

Note: Performance information displayed in historical reports

- If you change the time of the host where PFM - Agent or PFM - RM is operating from the current time to the future time, the performance information from before the change to after the change is not displayed.
- If you change the time of the server where PFM - Agent or PFM - RM is operating from the current time to the past time, the overwritten performance information from after the change to before the change is displayed.

### 1. Set the display information.

For example, when defining a historical report that summarizes CPU usages for each minute for the most recent one hour period in PFM - Agent for Platform (Windows), you could use the following conditions to set the display information for a historical report of System Overview (PI) records.

Condition

- The collection period of performance data is specified when displaying the report.
- The display interval of the report is set to one hour.
- Only the data whose User CPU % (PCT\_TOTAL\_USER\_TIME) field indicates the maximum value of the day is displayed.
- The maximum number of records displayable in the report is set to 1,440.

Set as follows:

**Specify when displayed:** optional

Settings for the report display period

**Date range:** specify when displayed

**Report interval:** Hour

Peak time

**Field:** User CPU%

**Maximum number of records:** 1440

### 2. Click the **Next >** button.

The New Report > Components window appears. Go to [5.3.7 Setting the display format \(table, list, or graph\) of a report](#).

## 5.3.7 Setting the display format (table, list, or graph) of a report

You can select the report display style from the following three formats, and you can also display data in multiple formats for a single report.

- Table
- List
- Graph

## (1) Setting components of a report

1. Set the necessary information for the display format.

For example, when defining a realtime report of the top ten processes whose CPU usage ratio is high in PFM - Agent for Platform (Windows), if you want to display the report of each field of Process Detail (PD) records in table format and display the CPU % (PCT\_PROCESSOR\_TIME) fields report in graph format, specify the following settings:

**CPU%:** Select **Table** and **Graph**

**PID:** Select **Table**

**Program:** Select **Table**

Display key

**Field:** CPU%

**In descending order:** Do not select

2. Click the **Next >** button.

- If **Graph** is selected one or more times in the New Report > Components window:  
The New Report > Graph window appears. Select a graph type. Go to [5.3.7\(2\) Setting a graph type](#).
- If **Graph** is not selected in the New Report > Components window:  
The New Report > Drilldown windows appears. Go to [5.3.8 Associating a report with another report \(drilldown report\)](#).

## (2) Setting a graph type

1. Set the graph type and the necessary information for the display format.

For example, when defining a realtime report of the top ten processes whose CPU usage ratio is high in PFM - Agent for Platform (Windows), you could use the following conditions to display the graph of CPU % (PCT\_PROCESSOR\_TIME) fields report of Process Detail (PD) records:

Conditions:

- The CPU % (PCT\_PROCESSOR\_TIME) field value is set for the vertical axis.
- The program (INSTANCE) field name is set for the horizontal axis and PID (ID\_PROCESS) field value is set for the data within the parentheses.
- The bar graph is set for the graph type.

Set as follows:

Graph types

**Column:** Select

Series direction

**By row:** Select

Axis labels

**X-axis:** Program (PID)

**Y-axis:** CPU%

Data label

**Data label 1:** Program

**Data label 2:** PID

2. Click the **Next >** button.

The New Report > Drilldown windows appears. Go to [5.3.8 Associating a report with another report \(drilldown report\)](#).

Supplemental information:

If you do not want to define a drilldown report, click the **Finish** button to close the report setting.

### 5.3.8 Associating a report with another report (drilldown report)

If necessary, set a drilldown report that is displayed by drilling down to the report, which is associated with the displayed report.

There are two types of drilldown reports that can be set according to which one best meets your purpose. You can also set both types.

- Setting a report-level drilldown report  
To set this type of drill-down report, go to [5.3.8\(1\) Defining a report-level drilldown report](#).
- Setting a field-level drilldown report  
To set this type of drill-down report, go to [5.3.8\(2\) Defining a field-level drilldown report](#).

#### (1) Defining a report-level drilldown report

1. Click the **Add** button in the New Report > Drilldown window.
2. In the New Report > Drilldown > Select Report window, select the drilldown report to associate with the report from the Reports tree.  
The selected report is marked with a checkmark. By selecting **Bookmarks** from the Tree type pull-down menu, you can assign a bookmark or combination bookmark as a drill-down report.



#### Tip

To search for a report or bookmark, enter the search terms in the text box and then click the **Filter** button.

3. Click the **OK** button.  
The drilldown report selected in step 2 is displayed in **Report** of the New Report > Drilldown window.
4. Click the **Finish** button.  
The New Report > Drilldown window closes and the report setting is finished.

#### (2) Defining a field-level drilldown report

1. From **Field**, select the field you want to associate with the drilldown report.  
Click the **Select** option button of the field to be selected.
2. Click the **Bind** button.
3. Select a drilldown report to be associated with the field from the Reports tree.  
The selected report is marked with a checkmark.
4. Click the **OK** button.  
The drilldown report selected in step 3 is displayed in **Report** of **Field drilldown** of the New Report > Drilldown window.

- To set a conditional expression when displaying selected fields, click the **Edit Expression** button.  
The New Report > Drilldown > Edit Conditional Expression for Drilldown window appears.
- In the New Report > Drilldown > Edit Conditional Expression for Drilldown window, set the conditional expressions for the drilldown report.  
For example, when displaying a drilldown report of the processes whose CPU usage ratio is higher than those of the processes displayed in the View Report window, set up the conditional expression as follows:  
**Conditional expression:** CPU % > CPU %  
CPU % at the left part indicates the CPU usage ratio displayed in the drilldown report. Specify this in the first **Field** of the New Report > Drilldown > Edit Conditional Expression for Drilldown window.  
CPU % at the right part indicates the CPU usage ratio, as the source of drilldown report, displayed in the View Report window. Specify this in the **Field** of **Select value or field**.
- Click the **OK** button.  
The New Report > Drilldown window appears. The conditional expression set in step 6 is displayed in **Conditional expression of Field drilldown**.
- Click the **Finish** button.  
The New Report > Drilldown window closes, and the report setting is finished.

### 5.3.9 Copying a report

- From the monitoring console Web browser, log on to PFM - Web Console.
- In the navigation frame of the main window, choose the **Reports** tab.
- In the Reports tree in the navigation frame of the Reports window, select the report you want to copy.  
The selected report is marked with a checkmark.
- In the method frame, select the **Copy** method.  
In the information frame, the Copy window appears, and the Reports tree of the copy destination is displayed.
- Select a folder as the copy destination or select **User Reports**.
- Click the **OK** button.  
The report selected in step 3 is copied to the folder or **User Reports** selected in step 5.



#### Note

If a report with the same name already exists at the copy destination, a report named **Copy of report-name** is created.

### 5.3.10 Editing a report

#### (1) Editing a report from the Reports window

- From the monitoring console Web browser, log on to PFM - Web Console.



2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the Reports tree in the navigation frame of the Reports window, select the report you want to edit.  
The selected report is marked with a checkmark.
4. In the method frame, select the **Edit** method.
5. In Edit > Name and Type window in the information frame, edit the report definition.  
The subsequent steps are similar to those when creating a new report.  
For details on the procedure, see from [5.3.3 Setting the name and type of a report](#) to [5.3.8 Associating a report with another report \(drilldown report\)](#).
6. When you are finished editing, click the **Finish** button.  
Now the edited report definition is valid.

Notes:

- You cannot change reports provided as a monitoring template. If you want to customize the report definition of a monitoring template, copy the necessary report of the monitoring template, and edit the copied report definition.
- When modifying the created report, you cannot change **Product**. In addition, if **Report type** and **Record** are changed, definitions such as the filter condition and indication settings are reset, so you must set them again.

## (2) Editing a report from the View Report window

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the Agents tab.
3. From the navigation frame in the Agents tree window, select an agent.  
The selected agent is marked with a checkmark.
4. From the method frame, select **Display Reports**.  
The Display Report > Select Report window appears in the information frame.
5. Choose a report in the information frame.
6. The View Report window appears in a new window. Click the **Edit Report Definition** tab.  
You can edit the items listed below. For details on how to set each item, see [5.3.4 Setting fields displayed in a report](#) to [5.3.7 Setting the display format \(table, list, or graph\) of a report](#). Note that you cannot edit **Name and Type** and **Drilldown**.
  - **Field** (Record names cannot be edited.)
  - **Filter**
  - **Indication settings**
  - **Components**
  - **Graph** (when a graph is selected)
7. When you are finished editing, click the **OK** button.  
Now the edited report definition is valid.  
To save the edited report definition, display the report again and click the **Save Report Definition** menu item.

## 5.3.11 Renaming a folder or report

You can rename a report or a folder for storing reports.

### (1) Renaming a report folder

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the navigation frame of the Reports window, select the folder whose name you want to change under **User Reports** in the Reports tree.  
The selected folder is marked with a checkmark.  
You cannot rename **User Reports**.

4. In the method frame, select the **Rename** method.  
The Rename window appears in the information frame.  
The current folder name is displayed in **Current folder name**.

5. In **Name of new folder**, enter a new folder name.

#### **Name of new folder**

Enter a folder name using 1 to 64 single or double-byte characters. You can enter a combination of single and double-byte characters.

6. Click the **OK** button.  
The folder selected in step 3 is renamed.

### (2) Renaming a report

To rename a report:

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the navigation frame of the Reports window, select the report you want to rename under **User Reports** in the Reports tree.  
The selected report is marked with a checkmark.
4. In the method frame, select the **Rename** method.  
The Rename window appears in the information frame,  
The current report name is displayed in **Current name of the report**.

5. In **New name of the report**, enter a new report name.

#### **New name of the report**

Enter a folder name using 1 to 64 single or double-byte characters. You can enter a combination of single and double-byte characters.

6. Click the **OK** button.  
The report selected in step 3 is renamed.

## 5.3.12 Deleting a folder or report

You can delete unnecessary folders or reports. When you delete a folder, folders and reports under the folder are also deleted.

### (1) Deleting a report folder

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the navigation frame of the Reports window, select the folder you want to delete under **User Reports** in the Reports tree.  
The selected folder is marked with a checkmark.
4. In the method frame, select the **Delete** method.  
A message box appears to confirm the deletion.
5. Click the **OK** button in the message box.  
The folder selected in step 3 is deleted.

### (2) Deleting a report

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the navigation frame of the Reports window, select the report you want to delete under **User Reports** in the Reports tree.  
The selected report is marked with a checkmark.
4. In the method frame, select the **Delete** method.  
A message box appears to confirm the deletion.
5. Click the **OK** button in the message box.  
The report selected in step 3 is deleted.

## 5.3.13 Exporting reports

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Reports** tab.
3. In the navigation frame of the Reports window, select the target you want to export in the Reports tree.  
The report is exported according to the selected target as follows:
  - When the root **User Reports** is selected:  
Folders and all reports under **User Reports** are exported.
  - When a folder is selected:  
The selected folder and reports under it are exported.

- When a report is selected:  
The selected report is exported.

4. In the method frame, select the **Export** method.

The operating system displays confirmation and Save As dialog boxes. Specify the file name and location and save the file. The selected report or reports are exported.

Note:

You can export a report definition file from the PFM - Web Console window in binary format.

### 5.3.14 Importing reports

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Reports** tab.

3. In the method frame of the Reports window, select the **Import** method.

4. In the Import window, click the **Browse** button beside **Import file name**.

The operating system displays a dialog box in which you can choose a file. Select the definition file for the report that you want to import.

5. To overwrite the existing report, click the **OK** button in the dialog box.

The report is imported.

## 5.4 Creating reports in the Web browser (Quick Guide)

---

You can use the Quick Guide to create a simplified report by setting the minimum items. For details on the default values of a report that was created by using the Quick Guide, see [5.4.3 Default values used for reports created with the Quick Guide](#).

### 5.4.1 Creating reports using Quick Guide

For details on how to create alarms, see [6.5 Setting alarms using the Web browser \(Quick Guide\)](#).

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents window, select the display format for the Agents tree from the **Display format** pull-down menu.
  - When **User Agents** is selected:  
The Agents tree that has **User Agents** (*logged-on-user-name*) as the root appears.
  - When **Products** is selected:  
The Agents tree that has **Products** as the root appears.
4. In the navigation frame, select the agent for which you want to create a report from the **Agents** tree.  
The selected agent is marked with a checkmark.
5. Choose the **Quick Guide** button in the method frame.
6. In the Quick Guide window, display the fields from which you want to compile a report.  
You can use either of the following methods to view fields:
  - Click the anchor for a record name to expand the tree under the record name, and select from the list of fields.
  - Search the fields for a specific character string and select a field from the results.  
To search for fields, enter the search terms in the **Keywords to find** text box and click **Search Fields**, or click **Search Fields** with the text box left empty. This displays the Quick Guide > Search Fields window. For details on the searching fields, see [5.4.2 Searching for fields](#).
7. Click a report icon in the realtime or historical report field.
8. In the View Report window, click the **Save Report Definition** menu command and save the report under a name of your choice.  
The Save Report Definition window appears. Specify a destination folder and a name for the report, and then click the **OK** button to save the report.

### 5.4.2 Searching for fields

The following describes only how to perform a keyword search for fields from the Quick Guide window. For details on the tasks you can perform from the search results, see the steps after fields have been displayed in [5.4.1 Creating reports using Quick Guide](#).

1. Click the **Search fields** button in the Quick Guide window.

The Quick Guide > Search Fields window appears.

If you entered a search keyword into **Keywords to find** in the Quick Guide window the search results will be displayed. For details on the search results, see the description in step 3.

2. Select an option from the **Records to search** pull-down menu.

The pull-down menu provides the following options:

- **--All records--**  
Select this option to search all records.
- **--Records where Log=Yes--**  
Select this option to search records with the Log property set to Yes. This option is available if the agent is running when the window opens.
- A list of record names for the selected agent  
A list of record names for the selected agent appears in alphabetical order.

3. Enter a character string for the field search into **Keywords to find** and click the **Search** button.

The search results are shown in **Search Result**.

- If **--All records--** is selected for the record search  
Results are listed by record in the Search Results: record(s) window.  
Click the anchor part of the record name to display a list of fields.
- If **--Records where Log=Yes--** is selected for the record search  
Results are listed by record in the Search Result: record(s) window.  
Click the anchor part of the record name to display a list of fields.
- If a record name is selected for the record search  
A list of resulting fields appears.

### 5.4.3 Default values used for reports created with the Quick Guide

The table below describes the default values for reports created using the Quick Guide. The same default values are used for reports whether you click the Realtime Reports or Historical Reports icon on the Quick Guide > Create Alarm window.

Table 5–1: Default values used for reports created with the Quick Guide

Item		Default value	Edition
Name and Type	Report name	(New report)	--
	Product	Product type of the selected agent	--
	Report type	Report type of the selected agent	Y#1
Field	Record	Record to which the field selected in the Quick Guide or <b>Search Results: List of field(s) found in record</b> <i>record-name</i> window belongs.	Y
	Whether the field is selected	The field selected in the Quick Guide or <b>Search Results: List of field(s) found in record</b> <i>record-name</i> window. If the record has ODBC key fields, those are included.	Y#2
Filter		None	--
Indication settings	Realtime report	Specify when displayed: Off	--

Item		Default value	Edition
Indication settings	Realtime report	Indicate delta value: On Refresh interval Do not refresh automatically: Off Initial value: 60 Minimum value: 60 Display by ranking Field: None In descending order: Off	--
	Historical report	Specify when displayed: Off Maximum number of records: 1440 Settings for the report display period Date range: Within the past hour Report interval: None (Minute when the specified record is the PI record) Field in Peak time: None	--
Components	Field	Table: On List: Off Graph: On only if the value stored in the selected field is numerical.	--
	Display key	Display name: Off Display key: Off	--
Drilldown		None	--

Legend:

Y: You need to specify the setting for this item.

--: You can omit this item.

#1:

You can use the Quick Guide to create historical reports and realtime reports only.

#2:

You cannot select multiple fields.

## 5.5 Creating reports by using commands

### 5.5.1 Outputting and customizing report definitions

1. Describe the report whose definition you want to output in the report definition file (XML format).

For example, to output report definitions of `report1` and `report2` stored in the `report_win` folder under **User Reports**, describe the report as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "rdef_output_params.dtd">
<pr-cli-parameters ver="0100">
<report-definitions>
<report-definition name="report1" parent-folder="/report_win"/>
<report-definition name="report2" parent-folder="/report_win"/>
</report-definitions>
</pr-cli-parameters>
```

2. Save the report definition file in step 1.

3. Execute the `jpcrdef output` command.

For example, to output the report definition described in the report definition file `rdef_input_win.xml` to the destination report definition file `rdef_output_win.xml`, the specification could be as follows:

```
jpcrdef output -o rdef_output_win.xml rdef_input_win.xml
```

For details on the `jpcrdef output` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

4. Edit the report definition file output in step 3.

For details on how to edit a definition file for a report, see the section that describes the `jpcrdef create` command in the manual *JPI/Performance Management Reference*.

5. Save the report definition file edited in step 4.

6. Register the report definition edited in step 4 by executing the `jpcrdef create` command.

For example, to use the report definition file `rdef_output_win.xml`, the specification could be as follows:

```
jpcrdef create rdef_output_win.xml
```

For details on the `jpcrdef create` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

#### Important

- You need to edit the report definition file in the prescribed format. Note that if you edit or create it in any format other than the prescribed one, it might not operate normally.
- An error occurs if you attempt to register a report with the same name as an existing report. To register the report, you need to delete the existing report by using the `jpcrdef delete` command.



## 5.5.2 Deleting an unnecessary report

1. Describe the report to be deleted in the definition file used by the command (XML format).

For example, to delete report definitions of `report1` and `report2` stored in the `report_win` folder under **User Reports** folder, describe the report as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "rdef_delete_params.dtd">
<pr-cli-parameters ver="0100">
<report-definitions>
<report-definition name="report1" parent-folder="/report_win"/>
<report-definition name="report2" parent-folder="/report_win"/>
</report-definitions>
</pr-cli-parameters>
```

For details on how to edit a definition file for a report, see the section that describes the `jpcrdef create` command in the manual *JP1/Performance Management Reference*.

2. Save the report definition file in step 1.
3. Delete the report by executing the `jpcrdef delete` command.

For example, to use the report definition file `rdef_del_win.xml`, the specification could be as follows:

```
jpcrdef delete -y rdef_del_win.xml
```

For details on the `jpcrdef delete` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

### Important

You need to edit the report definition file in the prescribed format. Note that if you edit or create it in any format other than the prescribed one, it might not operate normally.

## 5.6 Creating and editing bookmarks in the Web browser

---

### 5.6.1 Creating bookmarks

#### (1) Creating and registering a new bookmark (new registration)

##### (a) To display and register a report

1. Display the View Report window for the report to be registered with a bookmark.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).  
For details on how to display the View Report window for reports created using Quick Guide, see [5.4 Creating reports in the Web browser \(Quick Guide\)](#).
2. Click the **View Report** tab.
3. Select the **Bookmark** menu on the menu bar.  
The Bookmark window appears, and the Bookmarks tree is displayed.
4. To create a new folder for storing bookmarks, select the location where you want to create the folder, and click the **New Folder** button.  
If you do not want to create a new folder, select the location where you want to create the bookmark, and go to step 7.
5. Enter a folder name in the Bookmark(the folder name entry) window.  
**Name**  
Enter a folder name of no more than 64 single and double-byte characters. The folder name can contain a combination of single and double-byte characters.
6. Click the **OK** button.  
The created folder is added and displayed as selected in the Bookmarks tree of the Bookmark window.
7. In **Type a name of the bookmark**, enter the name of the bookmark with which you want to register the report.  
**Type a name of the bookmark**  
Enter a bookmark name of no more than 64 single and double-byte characters. The folder name can contain a combination of single and double-byte characters.
8. In **Bookmark type**, select the type of bookmark.  
To register the report with a bookmark, select **Bookmarks**. To register the report with a combination bookmark, select **Combination Bookmarks**.  
Note that you cannot register a realtime report with a combination bookmark.
9. Click the **OK** button.  
The report is registered with the bookmark you entered in step 7.

##### (b) To register a report without displaying it

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Agents** tab.

3. In the navigation frame of the Agents window, select the agent whose reports you want to display.  
The selected agent is marked with a checkmark.  
If you select **Multi select**, you can select multiple agents simultaneously.
4. In the method frame, select the **Register Bookmark** method.  
The Register Bookmark > Select Report window appears in the information frame. When you click a report definition in the reports tree, the Bookmark window appears with the Bookmarks tree displayed.
5. Go to step 4 of *5.6.1(1)(a) To display and register a report*.

## (2) Registering a report with an existing bookmark (additional registration)

### (a) To display and register a report

1. Display the View Report window for the report to be registered with a bookmark.  
For details on how to display the View Report window, see *5.7.1 Displaying reports*.
2. Click the **View Report** tab.
3. Select the **Bookmark** menu on the menu bar.
4. In the Bookmarks tree in the Bookmark window, select the bookmark where you want to register the report.  
**Click OK to add the report to the selected bookmark** appears in the Bookmark window, and the selected bookmark is marked with a checkmark.  
You cannot register the following types of report with a combination bookmark:
  - Realtime reports
  - Reports that do not display graphs
  - Reports for which a display key field is specified
5. Click the **OK** button.  
The report is registered with the bookmark you selected in step 4.

#### Note:

When you display reports from a bookmark, a number of instances of the View Report window equivalent to the number of reports is displayed. As the number of reports to display increases, it takes correspondingly longer to display the reports. For this reason, we recommend that you register no more than 10 reports in any one bookmark.

### (b) To register a report without displaying it

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Agents** tab.
3. In the navigation frame of the Agents window, select the agent whose reports you want to display.  
The selected agent is marked with a checkmark.  
If you select **Multi select**, you can select multiple agents simultaneously.
4. In the method frame, select the **Register Bookmark** method.

The Register Bookmark > Select Report window appears in the information frame. When you click a report definition in the reports tree, the Bookmark window appears with the Bookmarks tree displayed.

5. Go to step 4 of [5.6.1\(2\)\(a\) To display and register a report](#).

### (3) Updating a report registered with an existing bookmark (update registration)

#### (a) To display and register a report

1. Display the View Report window for the updated report.

For details on how to display the View Report window, see [5.7.1 Displaying reports](#).

2. Click the **View Report** tab.

3. Select the **Bookmark** menu on the menu bar.

4. In the Bookmarks tree of the Bookmark window, select the report that you want to update.

**Click OK to update the selected report** appears in the Bookmark window, and the selected bookmark is marked with a checkmark.

5. Click the **OK** button.

The registered report you selected in step 4 is updated.

#### (b) To register a report without displaying it

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Agents** tab.

3. In the navigation frame of the Agents window, select the agent whose reports you want to display.

The selected agent is marked with a checkmark.

If you select **Multi select**, you can select multiple agents simultaneously.

4. In the method frame, select the **Register Bookmark** method.

The Register Bookmark > Select Report window appears in the information frame. When you click a report definition in the reports tree, the Bookmark window appears with the Bookmarks tree displayed.

5. Go to step 4 of [5.6.1\(3\)\(a\) To display and register a report](#).

### 5.6.2 Adding a bookmark folder

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, select the **Bookmarks** tab.

3. In the navigation frame of the Bookmark window, select **Bookmarks** or one of its subfolders as the location of the new folder.

The selected folder is marked with a checkmark.

4. In the method frame, select the **New Folder** method.

5. In the New Folder window in the information frame, enter a folder name in **Name of new folder**.

**Name of new folder**

Enter a folder name of no more than 64 single and double-byte characters. The folder name can contain a combination of single and double-byte characters.

6. Click the **OK** button.

A folder is added just below the **Bookmarks** folder or the folder selected in step 3.

## 5.6.3 Renaming folders and bookmarks

### (1) Renaming a bookmark folder

To rename a folder:

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Bookmarks** tab.

3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the folder you want to rename.  
The selected folder is marked with a checkmark.

4. In the method frame, select the **Rename** method.

The Rename window appears in the information frame.

The folder name selected in step 3 is displayed in **Current folder name**.

5. In **Name of new folder**, enter a new folder name.

**Name of new folder**

Enter a folder name of no more than 64 single and double-byte characters. The folder name can contain a combination of single and double-byte characters.

6. Click the **OK** button.

The folder selected in step 3 is renamed.

### (2) Renaming a bookmark

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Bookmarks** tab.

3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the bookmark you want to rename.  
The selected bookmark is marked with a checkmark.

4. In the method frame, select the **Rename** method.

The Rename window appears in the information frame.

The name of the bookmark selected in step 3 is displayed in **Current name of the bookmark**.

5. In **New name of the bookmark**, enter a new bookmark name.

### New name of the bookmark

Enter a bookmark name of no more than 64 single and double-byte characters. The bookmark name can contain a combination of single and double-byte characters.

#### 6. Click the **OK** button.

The bookmark selected in step 3 is renamed.

#### Notes:

- When you rename a bookmark, any drilldown reports will still reference the old bookmark name. Reconfigure the drilldown reports in the Edit > Drilldown window for each report definition.
- Do not place a \ or / character at the end of the folder name for the bookmark. An error might occur when you use the `jspcrpt` command to output a report.

## 5.6.4 Deleting folders, bookmarks, and reports

You can delete unnecessary folders, bookmarks, and reports. When you delete a folder, everything under the folder is deleted. When you delete a bookmark, any reports registered under the bookmark are also deleted.

### (1) Deleting a bookmark folder

To delete a bookmark folder:

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Bookmarks** tab.
3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the folder you want to delete.  
The selected folder is marked with a checkmark.
4. In the method frame, select the **Delete** method.
5. In the confirmation dialog box, click the **OK** button.  
The folder selected in step 3 is deleted.

### (2) Deleting a bookmark

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Bookmarks** tab.
3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the bookmark you want to delete.  
The selected bookmark is marked with a checkmark.
4. In the method frame, select the **Delete** method.
5. In the confirmation dialog box, click the **OK** button.  
The bookmark selected in step 3 is deleted.

### (3) Deleting a report from a bookmark

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Bookmarks** tab.
3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the report you want to delete.  
The selected report is marked with a checkmark.
4. In the method frame, select the **Delete** method.
5. In the confirmation dialog box, click the **OK** button.  
The report selected in step 3 is deleted.

#### Supplemental information:

When you delete the last report registered with a bookmark, the bookmark is also deleted. In this case, a message appears prompting you to confirm deletion of the bookmark.

### 5.6.5 Checking the properties of a bookmark

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Bookmarks** tab.
3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the bookmark whose properties you want to check.  
The selected bookmark is marked with a checkmark.
4. In the method frame, select the **Properties** method.  
The Properties window appears in the information frame.

### 5.6.6 Tiling reports registered in bookmarks

You can display side-by-side graphs of multiple historical reports, which are managed using a bookmark, in an information frame by using the tiling display. You can also rearrange the graphs on screen or click a graph to display the View Report window for that graph.

Tiled display of graphs is only valid for historical reports that have graph display enabled. You cannot tile historical reports that have graph display disabled, or graphs associated with realtime reports.

#### Note

If report series paging is enabled, fields in the graph might be displayed over several pages. If you tile reports in which fields are displayed in this manner, the graph on the first page appears in the tile.

For details on how to configure report series paging and the parameters you can set, see the chapter describing installation and setup of Performance Management in the *JP1/Performance Management Planning and Configuration Guide*.

## (1) Tiling report display

To display graphs in tiling display:

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Bookmarks** tab.
3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the bookmark whose graphs you want to display in a tiled format.

The selected bookmark is marked with a checkmark.

4. Select the **Tiling Display** method in the method frame.

When you specify something other than **Specify when displayed** for the date range of historical reports that are registered in a bookmark, the Tiling Display window is displayed in the information frame.

If you select **Specify when displayed** when the date range for a bookmarked historical report is displayed, the Tiling Display Settings window appears. The Tiling Display Settings window can also be displayed using the Display Settings menu in the Tiling Display window.

5. Set the individual items for the Tiling Display Settings window.

Set display conditions for the following items, if necessary:

### Settings for the report display period

#### Date range

From the pull-down menu, select the date range for the data to be displayed in graphs that are displayed in tiling display. The selectable values are as follows:

- **Specify when displayed**
- **Within the past hour**
- **Within the past 24 hours**
- **Within the past 7 days**
- **Within the past month**
- **Within the past year**

The default is **Within the past 24 hours**.

When you select something other than **Specify when displayed**, the dates and times corresponding to the **Start time** and **End time** are automatically set.

#### Start time and End time

When you select **Specify when displayed** in **Date range**, set the start time and end time of the date range for graphs that are displayed in tiling display.

Specify the **Start time** and **End time** in *YYYY MM DD hh:mm* format (*YYYY* = year, *MM* = month, *DD* = day, *hh* = hour, *mm* = minute).

The range of dates and times you can specify is from 1971/01/01 00:00 to 2035/12/31 23:59. For the **End time**, specify a date and time after the **Start time** you specified.

Note that when you select something other than **Specify when displayed**, the appropriate date and time is automatically set. Additionally, if you change the date and time that are automatically displayed, settings for the **Date range** change to **Specify when displayed**.

#### Report interval

From the pull-down menu, select a report interval from the ones listed below. The default is displayed according to the date range selected in **Date range**.

- **Minute**
- **Hour**



- Day
- Week
- Month
- Year

#### Target reports

The **Apply to all reports** check box determines the target of the settings specified in the **Settings for the report display period** area. The check box is cleared by default.

If the check box is selected, the settings will be applied to all reports regardless of the report definitions.

If the check box is cleared, the settings will only be applied to reports for which **Specify when displayed** is specified for **Date range**.

#### Display the start time data and Display the end time data

These check boxes determine whether reports include the data for the times specified in **Start time** and **End time**. The check boxes are selected by default. You can specify the default state of the check boxes in the `excludeTerminalData` parameter within the `<vsa>` tag in the initialization file (`config.xml`). For details on how to enter settings in the initialization file (`config.xml`), see the section describing the initialization file in the appendixes of the manual *JPI/Performance Management Reference*.

When either check box is selected, the report includes data that matches the time specified in **Start time** or **End time**.

If a check box is cleared, data that matches the time specified in **Start time** or **End time** is excluded from the report.

#### Display layout

Specify the maximum number of graphs to be arranged next to in the Tiling Display window. The selectable values are as follows:

- Number of columns: 2
- Number of columns: 3
- Number of columns: 4

6. After you finish specifying the settings, click the **OK** button.

The Tiling Display window is displayed with the specified settings applied.

#### Note

If the value specified in **Display Layout** is changed, the default graph layout (in the order of the report names) is used.

## (2) Rearrange graphs

By using the tiling display, you can rearrange graphs that are displayed in the information frame.

1. Display the Tiling Display window.
2. In the Tiling Display window, select the **Arrange tile order** check box.  
In the Tiling Display window, a grid frame is displayed.
3. Select the display area of the source graph that is surrounded by a grid frame.  
From the selected area, the graph will be moved. You can also select an area where no graph is displayed.
4. Select the destination area enclosed with grid lines.  
The area selected as the source is replaced with the area selected as the destination. You can also select an empty area with no graph as the destination.

5. Repeat steps 3. and 4. until the desired layout is achieved, and then clear the **Arrange tile order** check box.  
The grid frame disappears from the Tiling Display window.

### (3) Saving a layout

You can save settings for the Tiling Display window specifying the maximum number of graphs to be displayed side-by-side and the sorting order of the graphs.

1. Display the Tiling Display window.
2. Change the maximum number of graphs displayed side-by-side or the layout of the graphs, as required.
3. Select the **Save Layout** menu in the Tiling Display window.  
A message appears asking you to confirm whether to save the layout. If a layout already exists, the existing layout is overwritten.

Note:

If any of the bookmarked reports is deleted or if a new report is registered with the bookmark, the saved layout becomes invalid. In this case, the value for the maximum number of graphs to be displayed side-by-side becomes the default value of three, and the graphs are displayed in the order of the report names registered with the bookmark.

### (4) Display a report

You can display the View Report window for a specific graph by clicking the graph in tiled display.

The displayed View Report window and the date range displayed in reports depend on conditions such as the tiled display settings and the settings for data ranges of reports registered in the bookmark.

Displayed View Report window

If **Specify when displayed** is selected as the data range for reports registered with the bookmark, the **Show Options** tab appears.

If **Specify when displayed** is not selected as the data range for reports registered with the bookmark, the **View Report** tab appears.





Date range for report display

For a View Report window displayed when a graph in tiled display is clicked, the data range specified in the Tiling Display Settings window supersedes the date ranges for the reports registered with the bookmark.

## 5.7 Displaying reports

### 5.7.1 Displaying reports

#### Tip





If report series paging is enabled, fields might be displayed over several pages in the View Report window. By default, 14 fields are displayed per page. You can navigate between pages by using the , , , and  buttons at the top of the lower frame.

For details on how to configure report series paging and the parameters you can set, see the chapter describing installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.





For the following reports, you can change how each period of the report is displayed.

- Report (historical report)
- Combination report (historical report)
- Event history




By using the buttons that control the report display period, you can display the next or previous set of data for a period of the same length. You can also use the Display report settings page to control the report display period even more precisely.


-  : Changes the display period to the previous time period of the same length.
-  : Moves the display period backward by half the length of the current display period.
-  : Moves the display period forward by half the length of the current display period.
-  : Changes the display period to the next time period of the same length.

For example, when a report shows data for one hour from 10:00 to 11:00, clicking each button changes the display period as follows:

-  : Displays data from 9:00 to 10:00
-  : Displays data from 9:30 to 10:30
-  : Displays data from 10:30 to 11:30
-  : Displays data from 11:00 to 12:00

If a report shows data for the 30 days from January 1st to 30th, clicking each button changes the display period as follows:

-  : Displays data from December 2nd to 31st
-  : Displays data from December 17th to January 15th
-  : Displays data from January 16th to February 14th

-  : Displays data from January 31st to March 1st

## (1) Displaying a report by specifying a specific agent

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents tree, select the agent for which you want to display a report.  
The selected agent is marked with a checkmark.



### Tip

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the object.

4. In the method frame, select the **Display Reports** method.  
In the information frame, the Reports window appears.  
The contents of the View Report > Select Report window depends on the selected tree type.  
If **Report** is selected as the tree type, see *When the tree type is Report*, described below. If **Bookmark** is selected as the tree type, see *When the tree type is Bookmark*, described below.

### Notes:

When no report is displayed:

If no historical report is displayed, check the record setting of the Store database as a target item of the report.

- The value of Log is `Yes`
- The value of Collection Interval is 1 or more

Make sure the setting is the same as above. Because historical reports use and display collected past data, if the target records are not set to be recorded in the Store database, they cannot be displayed.

If no combination report is displayed, the target registered reports might not be set. In this case, set registered reports by editing the combination bookmark.



### Note

The View Report window displays reports in the following ways:

*When the tree type is Report:*

- If a single agent is selected  
If more than one report is selected, each report is displayed in a View Report window.
- If more than one agent is selected and **Historical (single agent) report** or **Realtime (single agent) report** is selected  
A View Report window is displayed for each of the agents.
- If more than one agent is selected and **Historical (multiple agents) report** is selected  
A single View Report window is displayed for all the agents.

*When the tree type is Bookmark:*

- One or more agents selected when the bookmark was registered are used, regardless of how many agents (single or multiple) are specified.
- If a bookmark (a non-combination bookmark) is selected  
A report is displayed in a View Report window for each of the reports registered with the bookmark.

## (a) When the tree type is Report

1. Select a report from the reports tree.

The Reports tree shows the View Report window for the same product as the agent selected in the navigation frame of the Agents window.

- Viewing a single report

When you select a report in the Reports tree, the View Report window appears in a new window.

- Viewing multiple reports

You can select more than one report from the reports tree by selecting **Multi select**. This option is not available if more than one monitoring agent is selected from the navigation frame in the Agents tree window.

When you select more than one report in the Reports tree and click the **OK** button, each report appears in a new View Report window.

Supplementary note: When the Display report settings page appears in the View Report window

If you selected **Specify when displayed** as a display condition for a field when you created the report, the Display report settings page appears in the View Report window. Set the display conditions as needed, and then click the **OK** button to display the Report page.

## (b) When the tree type is Bookmark

1. Select a bookmark or registered report from the Bookmark tree.

When you select a bookmark or registered report from the Bookmark tree, the View Report window is displayed in a new window.



### Tip

To filter the contents of a bookmark or registered report, select the **Filter selected agents** check box. Only the fields that contain the name of the agent selected in the navigation frame will be displayed. Clear the check box to return the bookmark or registered report to normal.

## (2) Displaying a report associated with an alarm

You can display a report associated with an alarm and analyze the cause of the generated alarm.




1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents tree, select the agent whose report you want to display.  
The selected agent is marked with a checkmark.



## Tip

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the object.

4. In the method frame, select the **Display Alarm Status** method.

In the information frame, the Alarm Status window appears. For an alarm with an associated report, the report icon (for Agent for Platform,  or ) is displayed next to the alarm icon ().

For details on how to associate a report with an alarm, see [6.4.6 Associating a report with an alarm](#).

5. Select the report icon whose report you want to display.

The View Report window for the selected report icon is displayed in a new window.

Supplementary note: When the Display report settings page appears in the View Report window

If you selected **Specify when displayed** as a display condition for a field when you created the report, the Display report settings page appears in the View Report window. Set the display conditions as needed, and then click the **OK** button to display the Report page.

## (3) Displaying a report from the Event Monitor window

The window which displays events of Performance Management system in a list is called an *Event Monitor* window. In the Event Monitor window, you can display a report previously associated with an alarm.

For details on how to display a report in the Event Monitor window, see [7.1.2 Displaying a report associated with an alarm](#).

For details on how to associate a report with an alarm, see [6.4.6 Associating a report with an alarm](#).

## (4) Displaying a report from the Bookmarks window

You can register reports with a bookmark. For details on how to do this, see [5.6.1 Creating bookmarks](#).

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, choose the **Bookmarks** tab.
3. In the Bookmarks tree in the navigation frame of the Bookmark window, select a bookmark or registered report. The selected report is marked with a checkmark.

4. From the method frame, choose the **Display Reports** method.

The View Report window of the report selected in step 3 is displayed in a separate window.

## (5) Displaying a report from the tiling display of a bookmark

By using the tiling display in the Bookmarks window, you can display reports from the thumbnail of the historical report being displayed.

For details on how to display reports from the thumbnail in the tiling display, see [5.6.6 Tiling reports registered in bookmarks](#).

## 5.7.2 Checking the report properties (definition)

### (1) Displaying the report definition in the Properties tab of the View Report window

1. Display the View Report window for checking the properties (definition) in the window of PFM - Web Console.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).
2. Select the **Properties** tab of the View Report window.  
The report definition is displayed in the **Properties** tab.

Note:

The **Properties** tab of the View Report window displays report definition information, but not display settings information. Therefore, even if you change the display conditions in the **Report Display Settings** tab, the displayed information of the properties will not be changed.

### (2) Displaying the report definition from the Reports tree

1. In the navigation frame of the Reports tree, select the report definition that you want to display.
2. In the method frame, select the **Properties** method.  
The properties window for the selected report definition appears.

## 5.7.3 Setting the display conditions for a report

You can set the display conditions for a report in the following two ways:

- Set the display conditions when defining the report  
Set the report display conditions when defining the report by using the window of PFM - Web Console or by using the `jpcrdef create` command.  
The display conditions set when defining a report are permanently registered in the PFM - Web Console system. This will not be affected with operations such as opening or closing of the window, startup, and exit from the system. These conditions are permanently registered until deleted from the PFM - Web Console system in the window of PFM - Web Console or through the `jpcrdef delete` command.
- Set the display conditions when or while displaying the report  
Set the report display conditions in the **Show Options** tab of the View Report window when you first display the report or while it is displayed.  
The report display conditions set in the **Show Options** tab are restricted to the window where the display conditions are set or changed, and are not permanent. For example, even if the same report is displayed in a separate window at the same time, the contents set in the **Show Options** tab are applied only to the window where the operation is carried out. In addition, display conditions that are set or changed in one window are retained until the window closes.

Note that you can set the report display conditions by using the function for editing the displayed report. For details on the function for editing the displayed report, see [5.3.10 Editing a report](#).

### (1) Setting display conditions when first displaying a report

To set display conditions when you display a report:

1. Display the View Report window for the report whose display conditions you want to set.  
The View Report window appears with the Display report settings page displayed.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).
2. Set the display conditions.
3. Click the **OK** button.  
The View Report window appears subject to the display conditions you applied in step 2.

### (a) When setting the collection interval and retrieval interval of data

Report definition in the PFM - Web Console window:

Select **Specify when displayed** in the New Report > Indication Settings window.

Report definition in command input:

Specify TRUE for the `specify-when-displayed` attribute of the `indication-settings` parameter.  
Alternatively, omit the child element `date-range` of the `indication-settings` parameter.

### (b) When setting the data filter conditions

Report definition in the PFM - Web Console window:

Select **Specify when displayed** in the New Report > Filter window.

Report definition in command input:

Specify TRUE for the `specify-when-displayed` attribute of the `record - condition-expression - expression` parameter.

The hyphen (-) indicates a layer when defining the report. `record - condition-expression` means to specify `condition-expression` for a child element of the `record` parameter.

### (c) When setting the collection interval and retrieval interval of data and filter conditions

Report definition in the PFM - Web Console window:

Select **Specify when displayed** in the New Report > Indication settings window.

Also, select **Specify when displayed** in the New Report > Filter window.

Report definition in command input:

Specify TRUE for the `specify-when-displayed` attribute of `indication-settings` parameter.  
Alternatively, omit the child element `date-range` of `indication-settings` parameter.

Specify TRUE for the `specify-when-displayed` attribute of the `record - condition-expression - expression` parameter.

The hyphen (-) indicates a layer when defining the report. `record - condition-expression` means to specify `condition-expression` for a child element of the `record` parameter.

## (2) Setting display conditions while displaying a report

Use this procedure if you want to change display conditions each time you display the report.

1. Display the View Report window to set display conditions.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).
2. Click the **Show Options** tab in the View Report window.



3. Set the display conditions on the Display report settings page.

4. Click the **OK** button.

The View Report window affected by the display conditions of step 3 is displayed.

## 5.7.4 Displaying a drilldown report

This subsection describes how to display a drilldown report associated with the displayed report based on drilldown report types.

The drilldown report types are as follows:

Report-level drilldown report

This displays a report from another report.

Field-level drilldown report

This displays the details of a report.

This also displays a drilldown report that is automatically set for time item fields.

About displaying a drilldown report:

A drilldown report is displayed in a separate window from that of the parent report. You can further open another drilldown report from a parent report while displaying a drilldown report, and can open a drilldown report from the drilldown report itself. If you close the parent report window by clicking **Close**, the drilldown report window also closes. However, instances of the View Report window opened from a bookmark and instances of the combination report window opened from a combination bookmark do not close automatically. Processing other than closing the window has no effect on the other windows.

### (1) Displaying a report-level drilldown report by specifying the report name

If a report-level drilldown report is set, the pull-down menu and the **Display Reports** menu are displayed on the menu bar of the View Report window. The number of drilldown reports displayed in the pull-down menu might vary according to the parent report.

To display a report-level drilldown report, select the report from the pull-down menu and click the **Display Reports** menu. Note that the reports registered in bookmarks and combination bookmarks appear as drilldown reports in the pull-down menu.

### (2) Displaying a field-level drilldown report from the report area

Clicking the field of a table, list, or graph in the View Report window, displays the field-level drilldown report associated with that field.

#### (a) Displaying a field-level drilldown report from a table

Click a table value to display the field-level drilldown report. The available table values are displayed as linked.

#### (b) Displaying a field-level drilldown report from the item name of a list

Click an item name in a list to display the field-level drilldown report. The available item names of the list are displayed as linked.

### (c) Displaying a field-level drilldown report from a graph area

Click a graph area to display a field-level drilldown report. To display a field-level drilldown report from a graph area, when you define the report you need to define the drilldown report for a field displayed in the graph.

### (d) Information inherited from the parent to a drilldown report

When displaying the drilldown report from the report area, information inherited from the parent by a drilldown report might differ according to the combination of report types. Tables 5-2 *Inherited information (parent report consists of multiple agents)* and 5-3 *Inherited information (parent report is a single agent)* show the information a drilldown report inherits from the parent.

Table 5–2: Inherited information (parent report consists of multiple agents)

Drilldown report	When multiple agents are specified (historical reports only)	When a single agent is specified
Data collection period	<b>Date and Time</b> information of the clicked data row	Historical report: Same as shown on the left Realtime report: Does not inherit information
Agent type	Clicked row of the table, page of list, or agent of the graph area	Agent selected when displaying the parent report
Report interval	<ul style="list-style-type: none"> <li>Report definition of the drilldown report</li> <li>Changed value when changed by specify-when-displayed setting</li> </ul>	Historical report: Same as shown on the left Realtime report: Does not inherit information

Note: Information is only inherited by a drilldown report when the parent is a report. Information is not inherited by reports registered in bookmarks and combination bookmarks.

Table 5–3: Inherited information (parent report is a single agent)

Drilldown report	When multiple agents are specified (historical reports only)	When a single agent is specified
Data collection period	<b>Date and Time</b> information of the clicked data row	Historical report: Same as shown on the left Realtime report: Does not inherit information
Agent type	Agent selected when displaying the parent report <sup>#</sup>	
Report interval	<ul style="list-style-type: none"> <li>Report definition of the drilldown report</li> <li>Changed value when changed by specify-when-displayed setting</li> </ul>	Historical report: Same as shown on the left Realtime report: Does not inherit information

Note: Information is only inherited by a drilldown report when the parent is a report. Information is not inherited by reports registered in bookmarks and combination bookmarks.

#

When the drilldown report is of a single agent, even if both parent and drilldown reports are multi-instances, the instances are not automatically inherited. If the instance needs to be inherited, set the field value in the drilldown condition settings of the parent report.

### (3) Displaying a drilldown report (automatic settings) with the time item specification

When a table is displayed, the **Date and Time** field (**Record Time** field for a realtime report) is added to the first and last columns. If the report target record is a PI record and the data retrieval interval is defined other than in minutes, you can display the drilldown report (automatic settings) by selecting the time in the **Date and Time** or **Record Time** field.

The drilldown report (automatic settings) displayed by the time item specification is the same as the report definition of the parent report. However, the value of the selected **Date and Time** or **Record Time** is set for the **Start time** of the drilldown report, the **Report interval** is one step more detailed than the parent report. For example, if the **Report interval** of the parent report is **Hour**, the **Report interval** of the drilldown report is **Minute**.

Note:

Only historical reports allow you to display the drilldown report from a time item.

### (4) Displaying the conditions for a drilldown report

The drilldown report is displayed after filtering with the following display conditions:

1. Filter conditions defined in the parent report for the drilldown report display
2. Filter conditions defined in the drilldown report for the drilldown report display
3. Report display conditions defined as **Specify when displayed** (`SPECIFY_WHEN_DISPLAYED`) in the drilldown report

The first and second conditions have a different priority. Even if the second filter condition is defined with fixed value in the drilldown report, the first filter condition defined in the parent report has precedence.

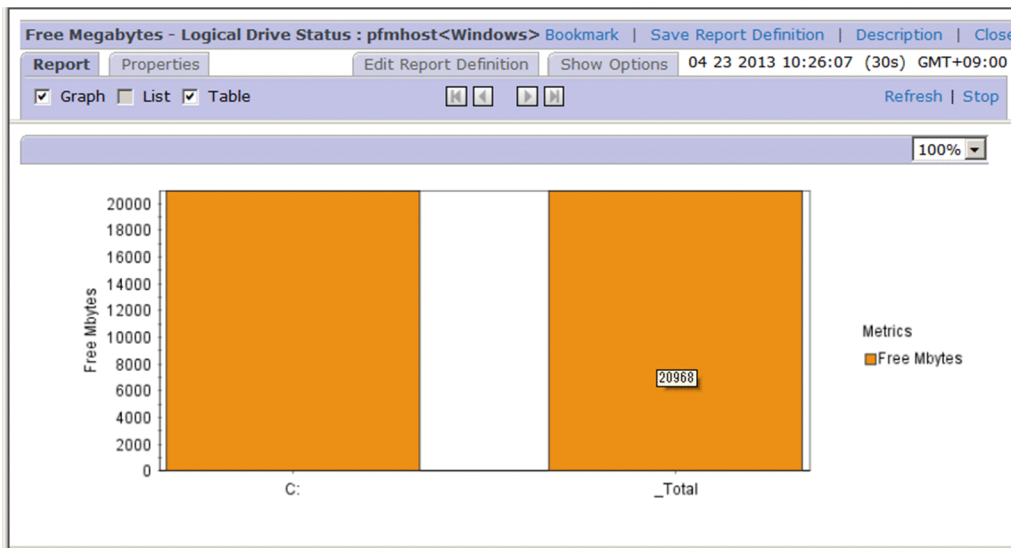
## 5.7.5 Using Autolabel to check data values

Performance Management can display tooltips that indicate the value of a graph plot when you rest your mouse pointer on the plot. This functionality is called *Autolabel*. You can enable the Autolabel functionality by selecting the **Show AutoLabel** check box on the Display report settings page of the View Report window.

To automatically enable Autolabel when you display a report, specify `true` for the `enableAutoLabelAtDefaultDisp` parameter in the initialization file (`config.xml`). For details on the initialization file (`config.xml`), see the description of the file in the manual *JPI/Performance Management Reference*.

The following figure shows an example of a View Report window in which a tooltip is displayed by the Autolabel functionality.

Figure 5–6: Example of View Report window with tooltip displayed



### Note

You cannot use the Autolabel functionality with the following graphs:

- Graphs in the print window
- Graphs in reports output in HTML format by the `jpcrpt` command
- Graphs in the Tiling Display window
- Graphs in the System Operational Status Summary window

The following describes how to set the number of digits displayed in the data in a tooltip, and describes the settings needed to use Autolabel with graphs that have a large number of plots.

## (1) Setting the number of digits in tooltips

By default, the maximum number of digits in a tooltip displayed by the Autolabel functionality is seven before the decimal point, and three after. To change these limits, set values in the `autoLabelMaxIntegerDigits` and `autoLabelMaxFractionDigits` parameters (both under the `<draw>` tag) in `config.xml`.

For details on the initialization file (`config.xml`), see the description of the file in the appendixes of the manual *JPI/Performance Management Reference*.

## (2) Using Autolabel for graphs with a large number of plots

The Autolabel functionality can display data in tooltips for a maximum of 1,440 plots. You can change the number of plots for which the Autolabel functionality can display tooltips by changing the value of the `maxAutoLabelPoints` parameter under the `<draw>` tag of `config.xml`.

For details on the initialization file (`config.xml`), see the description of the file in the appendixes of the manual *JPI/Performance Management Reference*.

## 5.7.6 Changing the color of graph series

You can change the colors in which graph series are drawn by editing the contents of the initialization file (`config.xml`). The following table describes the labels you can specify when editing the file.

Table 5–4: Labels that determine graph series colors

Item	Content
Labels	The labels <code>color1</code> , <code>color2</code> , through to <code>color16</code> in the <code>&lt;chart-symbolColors&gt;</code> tag.
Specifiable values	Specify RGB values separated by commas. You can specify each of R, G, and B in a range from 0 to 255.
Description	Graph series are drawn in the color specified in the labels, in order from <code>color1</code> . If you specify a value outside the specifiable range for any one of R, G, or B, the affected series is displayed in the default color. If you do not specify a color, the label is skipped. For example, if you omit <code>color3</code> , colors are applied in the order <code>color1</code> , <code>color2</code> , and then <code>color4</code> and so on. Any of <code>color1</code> to <code>color16</code> with valid values will determine the color of the graph series. For example, if three labels have valid values, those three colors are used as the colors of the graph series.

The following shows an example of specifying series colors in `config.xml`.






```

...
:
<chart-symbolColors>
  <param name="color1" value="255,0,0"/>
  <param name="color2" value="255,200,0"/>
  <param name="color3" value="0,0,255"/>
  <param name="color4" value="192,192,192"/>
  <param name="color5" value="255,0,255"/>
  <param name="color6" value="255,255,0"/>
  <param name="color7" value="128,128,128"/>
  <param name="color8" value="0,255,0"/>
  <param name="color9" value="64,64,64"/>
  <param name="color10" value="0,255,255"/>
  <param name="color11" value="0,0,0"/>
  <param name="color12" value="255,175,175"/>
</chart-symbolColors>
:
...

```

The following table lists common colors you can use in graphs.

Table 5–5: Common display colors and RGB values

Displayed color	RGB value (R,G,B)
 (red)	255,0,0
 (orange)	255,200,0
 (blue)	0,0,255
 (light gray)	192,192,192
 (magenta)	255,0,255

Displayed color	RGB value (R,G,B)
 (yellow)	255,255,0
 (gray)	128,128,128
 (lime green)	0,255,0
 (dark gray)	64,64,64
 (cyan)	0,255,255
 (black)	0,0,0
 (pink)	255,175,175
 (olive green)	128,128,0
 (dark blue)	0,0,128
 (purple)	128,0,128
 (teal)	0,128,128
 (maroon)	128,0,0
 (green)	0,128,0

Note that the colors of graph series have changed in PFM - Web Console version 10-00. If you want to use the color scheme from PFM - Web Console version 09-00 or earlier, use the following procedure to edit the initialization file (`config.xml`):

1. Open the sample initialization file (`config.xml`).

The sample file can be found in the following location:

In Windows:

```
installation-folder\sample\conf\
```

In UNIX:

```
/opt/jp1pcwebcon/sample/conf/
```

2. Copy the following two parts of the sample file.

- The `<chart-symbolColors>` line
- The lines from the `<!--` immediately preceding sample setting pattern, to `</chart-symbolColors>`

3. Paste the lines you copied into a text editor.

The result is as follows:

```
<chart-symbolColors>
  <!--
    sample setting pattern,
    colors are used before Web Console 0910.
```

```

        color1          : red
        ...
        color12         : pink
        not use Color Number at Graph type Circle.
        : color1
    -->
    <!--
    <param name="color1" value="255,0,0"/>
        ...
    <param name="color12" value="255,175,175"/>
    <param name="noUseCircleColor value="1"/>
    -->

</chart-symbolColors>

```

#### 4. Remove the comment tags.

From the pasted text, remove the comment tags (<!-- and -->) that enclose the lines from <param name="color1" value="255,0,0"/> to <param name="noUseCircleColor value="1"/>. Do not uncomment the preceding block that begins with the line `sample setting pattern,`.

#### 5. Apply the information you created in step 4 to the initialization settings file (`config.xml`).

Apply the information to the initialization settings file (`config.xml`) in the following location:

In Windows:

```
installation-folder\conf\
```

In UNIX:

```
/opt/jp1pcwebcon/conf/
```

The process for applying the information differs depending on whether you upgraded to PFM - Web Console 10-00 or later or performed a new installation.

In a new installation of PFM - Web Console 10-00 or later:

Replace the section from <chart-symbolColors> to </chart-symbolColors> in the initialization file (`config.xml`) with the information you edited in step 4.

In an upgraded installation:

Add the information you edited in step 4 to the initialization file (`config.xml`).

The position where you add the information depends on what appears immediately after the </vsa> tag.

- If a <draw> tag appears immediately after the </vsa> tag:  
Add the information you edited in step 4 between the <param name="maxDrilldownPoints" value="setting-value" /> line and the </draw> tag.
- If a <command> tag appears immediately after the </vsa> tag:  
Add a <draw> line and a </draw> line immediately after the </vsa> tag, and add the information you edited in step 4 between those lines.

#### 6. Restart the PFM - Web Console service.

The changes you made to the initialization file (`config.xml`) take effect, and the graph colors revert to the color scheme of PFM - Web Console version 09-00 and earlier.

For details on the initialization file (`config.xml`), see the description of the file in the appendixes of the manual *JP1/Performance Management Reference*.

## 5.8 Displaying combination reports

---

Combination reports are a feature that allows you to combine multiple historical reports in the same graph. Although normal reports allow you to display reports from multiple agents in a single graph, they must refer to the same records in a historical report. By using a combination report, you can display multiple historical reports in the same graph regardless of the agent used or the type of record in the report. You can also compare one report with another by displaying it as reference data (a *baseline*) in the graph.

The following table describes whether or not a combination report can be displayed, for each combination of graph type and graph options.

Table 5–6: Whether a combination report can be displayed

Graph type	Graph options		
	Normal	Show 3D graph	Show gridlines
Column graph	Yes	Yes	Yes
Stacked column graph	Yes	Yes	Yes
Bar graph	No	No	No
Stacked bar graph	No	No	No
Pie graph	No	No	No
Line graph	Yes	No <sup>#</sup>	Yes
Area graph	Yes	No <sup>#</sup>	Yes
Stacked area graph	Yes	No <sup>#</sup>	Yes

Legend:

Yes: Can be displayed.

No: Cannot be displayed.

#

Can be set, but the setting is ignored.

The following figures show examples of displaying a combination report.



Figure 5–7: Example of displaying a combination report (column graph)

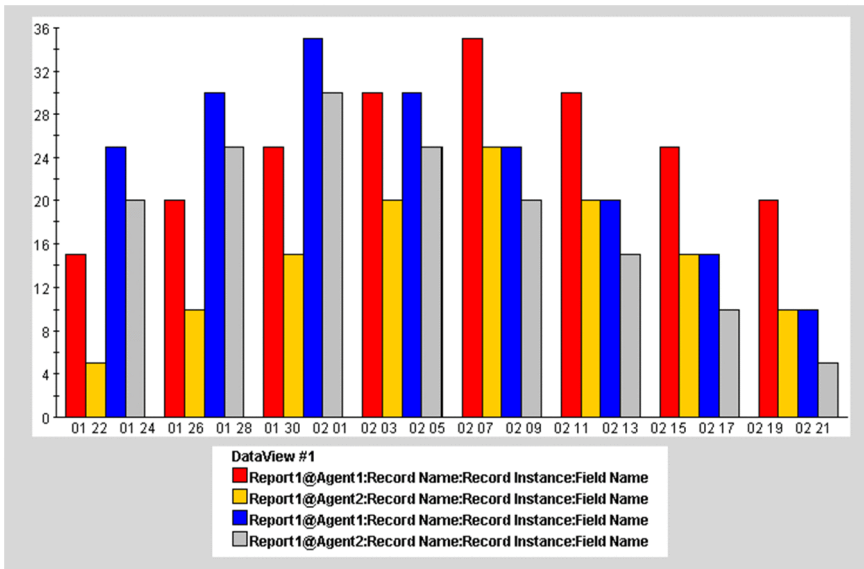


Figure 5–8: Example of displaying a combination report (stacked column graph)

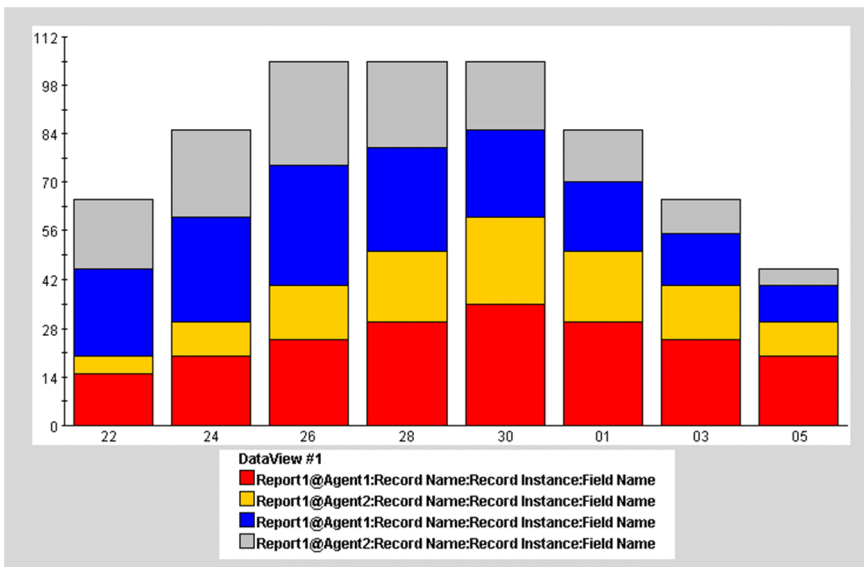


Figure 5–9: Example of displaying a combination report (line graph)

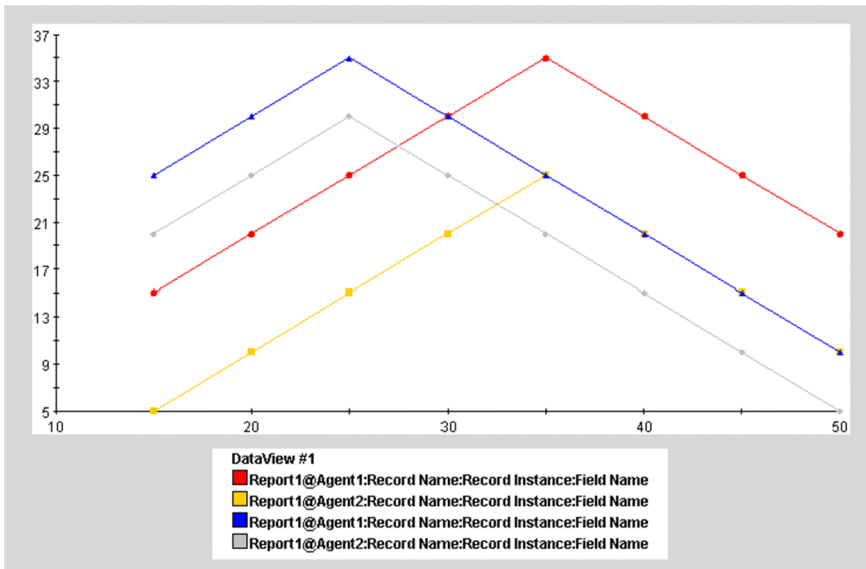


Figure 5–10: Example of displaying a combination report (area graph)

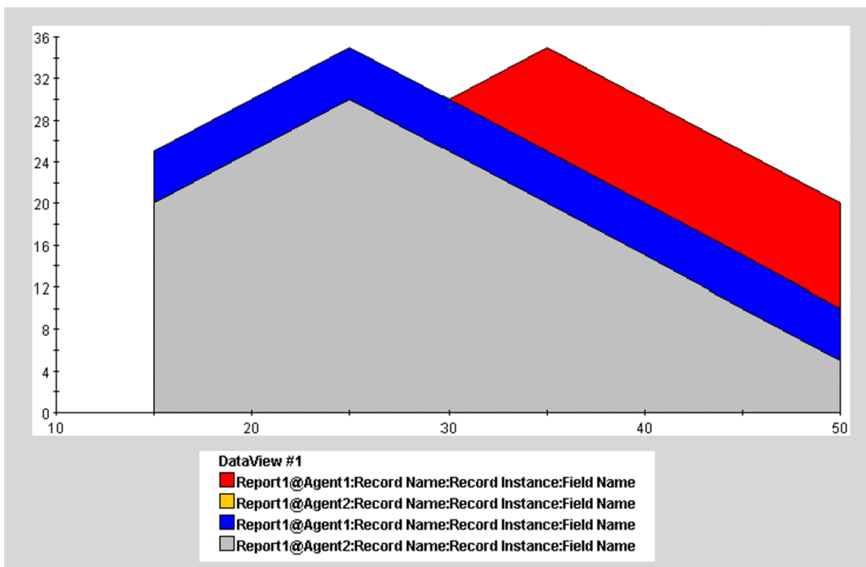
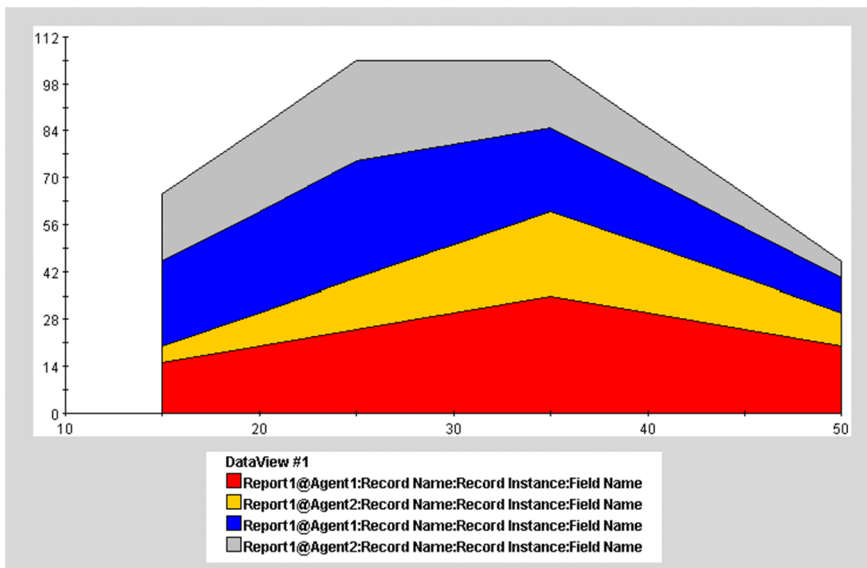


Figure 5–11: Example of displaying a combination report (stacked area graph)



## 5.8.1 Preparing to display combination reports

The following preparations are required before you can display a combination report:

- Create a report to display in a combination report.
- Register a report in a combination bookmark
- Register a baseline in a combination bookmark
- Setting the display format of a combination report

For details on how to create reports to display in a combination report, see [5.2 Overview and procedure for report creation](#). For details on how to register reports with a combination bookmark, see [5.6.1 Creating bookmarks](#).



### Note

You can register a total of 10 reports and baselines in a combination bookmark.

### (1) Registering a baseline in a combination bookmark

1. Display the View Report window for registering a baseline in a combination bookmark in the window of PFM - Web Console.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).
2. Select the **Baseline** in the View Report window.
3. From the Bookmarks tree in the Baseline window, select a combination bookmark and enter the name of the baseline in **Specify the baseline name**.

Specify the baseline name

Enter a baseline name using 1 to 64 single or double-byte characters. You can enter a combination of single and double-byte characters.

4. Click the **OK** button.

The baseline is registered in the combination bookmark.

## (2) Setting the display format of a combination report

To set the display format of a combination report, edit the display conditions for combination bookmarks:

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Bookmarks** tab.

3. From the Bookmarks tree in the navigation frame of the Bookmark window, select the combination bookmark you created.

The selected combination bookmark is marked with a checkmark.

4. From the method frame, choose the **Edit** method.

In the information frame, the Edit window appears.

5. Edit the display conditions as needed in the Edit window in the information frame.

You can group the reports of a combination report in the **Series group settings** area of the Edit window, as a *series group*. You can set and modify the following settings for each series group:

- Graph type
- Series group name
- Maximum and minimum values of the Y-axis
- Y-axis display position

6. Click the **OK** button.

The series group settings take effect as the display settings for the combination report.

## 5.8.2 Displaying combination reports

You can display the reports registered in a combination bookmark from the Agents tree or the Bookmarks tree.

Some preparation is required before you can display a combination report. The first step is creating the combination bookmark, after which you can perform such tasks as registering a baseline and editing the display conditions and other aspects of the combination bookmark. For details on how to do so, see [5.6.1 Creating bookmarks](#) and [5.8.1 Preparing to display combination reports](#).

Note:

It might take a long time to display a combination report with a large number of reports assigned, preventing you from checking the contents of the report. In this case, reduce the number of reports in the combination report.

### (1) Displaying a combination report from the Agents tree

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Agents** tab.

3. In the navigation frame of the Agents tree, select an agent.

The selected agent is marked with a checkmark.



### Tip

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the object.

4. In the method frame, select the **Display Reports** method.

By default, the reports tree appears in the information frame.

5. In the information frame, select **Bookmark** from the **Tree type** drop-down list box.

The bookmarks tree appears in the information frame.



### Tip

You can filter the bookmarks and registered reports displayed in the information frame by selecting the **Filter selected agents** check box. When you select the check box, the bookmarks and registered reports that contain the name of the agent selected in the navigation frame are displayed. To remove the filter, clear the **Filter selected agents** check box.

6. Select a combination bookmark from the bookmarks tree.

The registered reports associated with the combination bookmark appear as a combination report in a new window.

## (2) Displaying a combination report from the Bookmarks tree

1. From the monitoring console Web browser, log on to PFM - Web Console.

2. In the navigation frame of the main window, choose the **Bookmarks** tab.

3. In the Bookmarks tree in the navigation frame of the Bookmark window, select the combination bookmark you created.

The selected combination bookmark is marked with a checkmark.

4. In the method frame, select the **Display Reports** method.

The registered reports associated with the combination bookmark selected in step 4 appear as a combination report in a new window.

### 5.8.3 Checking the properties (definitions) of combination bookmarks

On the **Properties** tab of the combination report window, you can check the definition of a combination bookmark. You cannot check the definitions of the registered reports themselves.

1. In PFM - Web Console, display the reports window for the report whose properties (definition) you want to check.

For details on how to display the View Report window, see [5.7.1 Displaying reports](#).

2. Select the **Properties** tab in the View Report window.

The combination bookmark definition is displayed in the **Properties** tab.

#### Note

The information displayed on the **Properties** tab is the definition information of the combination bookmark, but not display settings information. Therefore, even if you change the display conditions in the **Show Options** tab, the displayed information of the properties will not be changed.

## 5.8.4 Examples of using combination reports in real-world situations

### (1) Displaying reports that include different fields from the same record

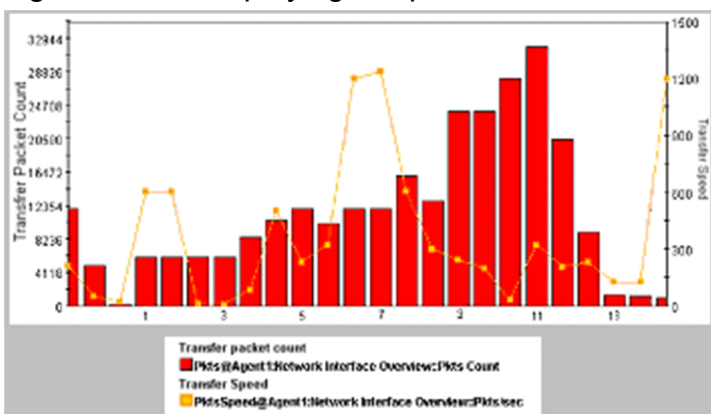
When displaying a graph that presents different fields from the same record, you need to ensure that there is not a large disparity between the fields in terms of scale or units of measurement.

Normal reports and combination reports deal with such a disparity in different ways:

- For normal reports  
The highest value among the fields is used as the maximum value of the Y axis. For this reason, displaying reports whose fields contain significantly different values might result in a graph that is difficult to comprehend.
- For combination reports  
By assigning each report to a different series group, you can adjust the following aspects of how each report is displayed:
  - The maximum value of the Y axis
  - Whether the Y axis appears at the left or right of the graph
  - The type of graph

The following figure shows an example of a graph created from a combination report. This graph plots two fields: **CPU %** (maximum value: 100%), and **Available Mbytes** (maximum value: 3,000 MB).

Figure 5–12: Displaying a report that includes different fields from the same record



To register the combination report:

1. Register multiple reports in a combination bookmark.

The reports used in this example are assumed to meet the following conditions:

- The data fields displayed in the graph (can be more than one) have the same scale
  - The data in the graph has the same collection interval
2. Edit the combination bookmark as follows:
    - Assign each report to a different series group
    - For each series group, set a suitable maximum value for the Y axis
    - Between series groups, ensure that the Y axes are displayed at opposite sides of the graph

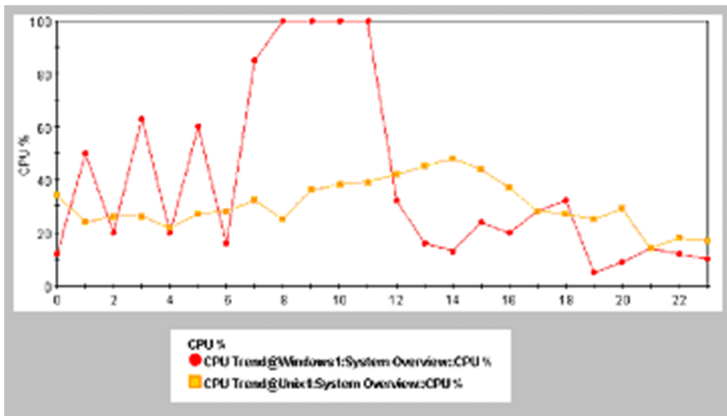
## (2) Displaying reports that gather related records from different agent types

You can compare the values of related records from different agent types by displaying them in a single graph. However, you cannot display information from different agents in a graph based on a normal report.

With combination reports, you can display information from records from different agents in the same graph by editing a combination bookmark to place the relevant reports into the same series group. By choosing stacked column or bar as the graph type, you can visually check the total of the data from the different agents.

The following figure shows an example of a graph created from a combination report. This graph displays the value of CPU usage (as a percentage) for the fields Windows1 and UNIX1 in a single graph.

Figure 5–13: Displaying a report that includes related records from different agent types



To register the combination report:

1. Register multiple reports in a combination bookmark.

The reports used in this example are assumed to contain data fields that are similar in scale and content.

2. Edit the combination bookmark to assign each report to the same series group.

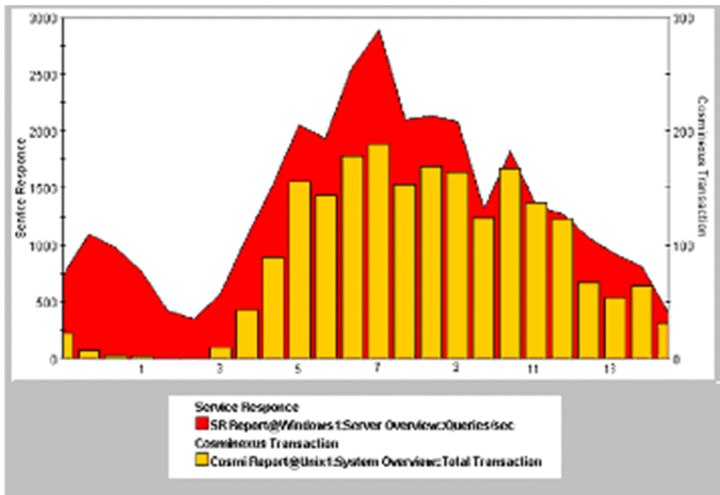
## (3) Displaying reports that gather different records from different agent types

With combination reports, you can display different records from different agents in the same graph. This is a useful feature as it allows you to visually check how changes in a given record correlate to changes in another.

The following figure shows the results of creating a graph from a combination report. In this example, the following two fields, which exhibit a correlation, are displayed in the same graph.

- Response time of HTTP service (maximum value: 3.0 seconds)
- Number of Cosminexus transactions (maximum value: 3,000)

Figure 5–14: Displaying a report that includes different records from different agents



To register the combination report:

1. Register multiple reports in a combination bookmark.

The reports used in this example are assumed to differ in scale and originate from different agents, but show a correlation.

2. Edit the combination bookmark as follows:

- Assign each report to a different series group
- For each series group, set the graph type and Y axis value according to the scale and data of the report it contains.
- Between series groups, ensure that the Y axis are displayed at opposite sides of the graph

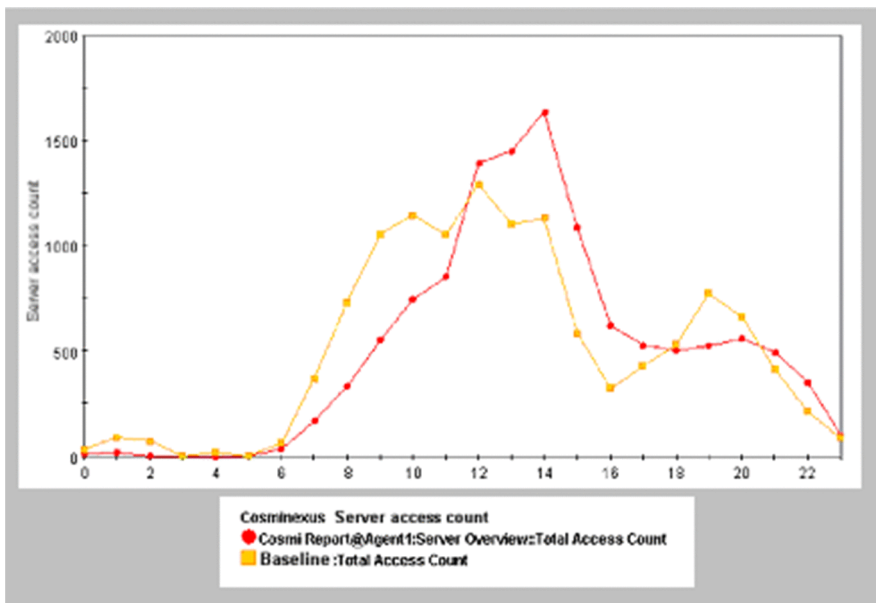
#### (4) Displaying a report together with a baseline

With combination reports, you can display past periodic data or data obtained during stable operation of the system in the graph as a baseline. By comparing this baseline with a current report, you can ascertain whether the system is operating normally and identify trends in the operation of the system.

The following figure shows the results of creating a graph showing the number of transactions over a 24-hour period (maximum value: 3,000), together with a baseline that presents the same data from a historical report.



Figure 5–15: Displaying a report together with a baseline



To register the combination report:

1. Register the report to be compared with the baseline as a combination bookmark.  
In this example, this report is configured to collect data periodically.
2. Add a baseline to the combination bookmark.  
In this example, the report registered as the baseline covers the same period or has the same collection interval as the report registered in step 1.
3. Edit the combination bookmark.  
Assign the registered report and the baseline to the same series group.

## (5) Combining various types of combination report

By applying the steps described in (1) through (4) above, you can create graphs that allow you to judge the status of the entire system from an integrated perspective. When a more detailed monitoring approach is called for, you can change perspective by drilling down to a separate report that focuses on specific data in the combination report.

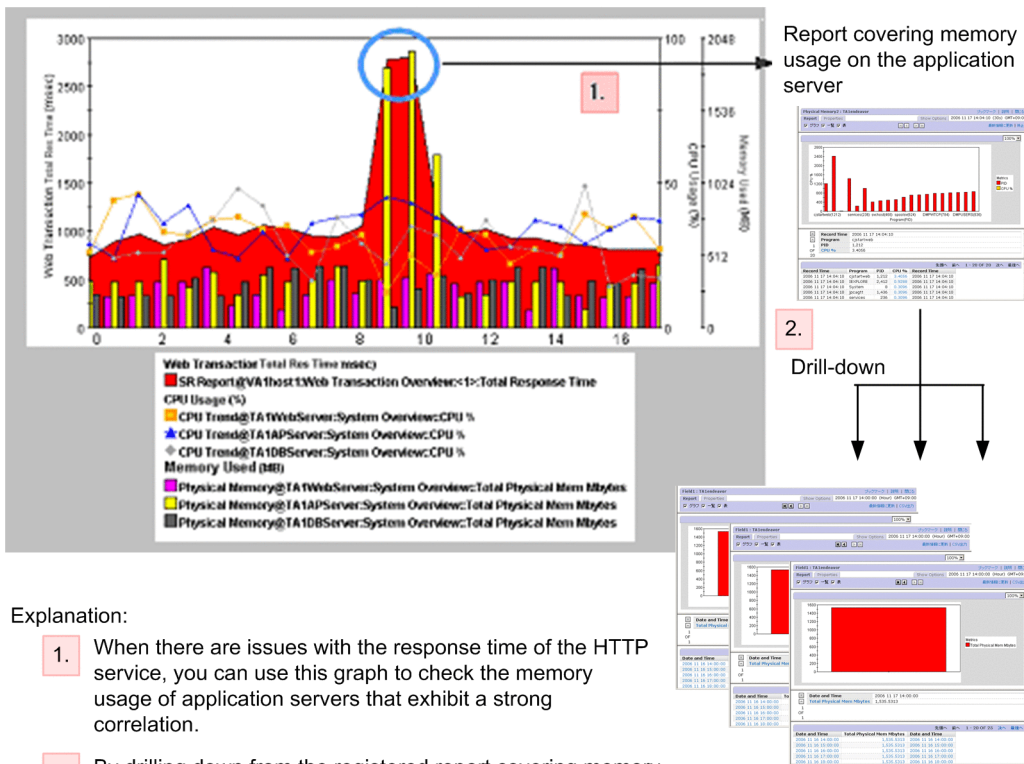
The figure below shows an example of monitoring the operation of a three-tiered Web system comprising a Web server, application server, and database server. In this example, the following aspects of the system are monitored:

- The response time of the HTTP service as collected by PFM - Agent for Service Response, giving an indication of the status of the system in its entirety
- The following two items, which can affect the response time of the HTTP service:
  - CPU usage of each server tier (percentage)
  - Memory usage (MB)

Each set of data is assigned to a series group and displayed as a combination report in a single graph. The ability to set the scale of the vertical axis individually for each series group allows trends in the operating status of the system to be compared.

The following figure shows the resulting graph.

Figure 5–16: Example combining various types of report



Explanation:

1. When there are issues with the response time of the HTTP service, you can use this graph to check the memory usage of application servers that exhibit a strong correlation.
2. By drilling down from the registered report covering memory usage on the application server you are analyzing, you can identify the underlying cause of the bottleneck.

To register the combination report:

1. Create reports featuring the following data:

- Response time of the HTTP service
- CPU usage of the Web server
- Memory used by the Web server
- CPU usage of the application server
- Memory usage of the application server
- CPU usage of the database server
- Memory usage of the database server

Associate the appropriate drilldown reports for the Web server, application server, and database server.

2. Register these reports in a combination bookmark.

Set the display conditions for the series groups as follows:

- Response time of the HTTP service: Area graph, maximum 3,000 ms
- CPU usage: Line graph, maximum 100
- Memory usage: Column graph, maximum 2,048MB

## 5.9 Outputting reports

---

### 5.9.1 Exporting reports in CSV or HTML format by using a Web browser

#### (1) Outputting reports in CSV format using a Web browser

1. Display the View Report window for the report you want to output in CSV format.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).
2. If the report you want to output is a realtime report, click the **Stop** menu on the **View Report** tab of the View Report window.  
This stops the realtime report from refreshing automatically. When you click the **Stop** menu, the **Export** menu appears.  
For historical reports, the **Export** menu appears as soon as you display the View Report window.
3. Choose the **Export** menu on the **View Report** tab of the View Report window.  
The operating system displays confirmation and Save As dialog boxes.  
Specify the file name and location and save the file.

#### Note 1

If you have enabled the report cache filing function, make sure that there are no error messages appended to the CSV file.

An error message is appended to the end of the CSV file if an error occurs during CSV file output, such as a file access error or a problem with the file contents.

#### Note 2

When you output a report in CSV format, the following field information appears in the file even if it is not selected for report output.

- In realtime reports  
The **Record Time** field and ODBC key field information are appended to the file.
- In historical reports (for a single agent)  
The **Date and Time** field and ODBC key field information are appended to the file.
- In historical reports (for multiple agents)  
The **Date and Time** field, **Agent Host** field, **Agent Instance** field and ODBC key field information are appended to the file.

For details on ODBC key fields, see the documentation for PFM - Agent.

#### (2) Outputting reports in HTML format using a Web browser

You can display the results of a report in a format suitable for printing or saving to disk.

To output a report in HTML format:

1. Display the View Report window for the report you want to output in HTML format.  
For details on how to display the View Report window, see [5.7.1 Displaying reports](#).
2. If the report you want to output is a realtime report, click the **Stop** menu on the **View Report** tab of the View Report window.

This stops the realtime report from refreshing automatically. When you click the **Stop** menu, the **Print** menu appears. For historical reports, the **Print** menu appears as soon as you display the View Report window.

3. Choose the **Print** menu on the **View Report** tab of the View Report window.

The print window opens in a new window, displaying the report in a format suitable for printing or saving to disk.

4. Print or save the report using the functionality of your Web browser.

When saving the report, use the option that saves the complete web page.

Note 1

If you intend to print the list area and table area in color, make sure that your Web browser is set up to print background colors and images.

Note 2

If the report series paging functionality is enabled, the print window shows the page displayed in the View Report window. To output all the fields in the report to a single HTML file, disable report series paging. For details on how to configure the report series paging functionality, see the chapter describing installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

## 5.9.2 Exporting reports in CSV or HTML format by using a command

By using the `jpcrpt` command, you can implement batch processing that outputs a report to a file regularly at a predetermined time, or outputs multiple reports to a file in one operation. The `jpcrpt` command outputs reports in CSV or HTML format. The report types that the `jpcrpt` command can output depend on the version of PFM - Web Console. The following table describes which report types can be output by which versions of PFM - Web Console.

Table 5–7: Report output capabilities by version

Type of output		08-00	08-11 or later
Report	CSV output	Yes	Yes
	HTML output	No	Yes
Registered report	CSV output	No	Yes
	HTML output	No	Yes
Combination report	HTML output	No	Yes

Legend:

- Yes: Can be output
- No: Cannot be output

For details on the `jpcrpt` command, see the manual *JPI/Performance Management Reference*.

Notes:

When you output a report in CSV format, the following field information appears in the file even if it is not selected for report output.

- In realtime reports  
The **Record Time** field and ODBC key field information are appended to the file.
- In historical reports (for a single agent)  
The **Date and Time** field and ODBC key field information are appended to the file.
- In historical reports (for multiple agents)

The **Date and Time** field, **Agent Host** field, **Agent Instance** field and ODBC key field information are appended to the file.

For details on ODBC key fields, see the documentation for PFM - Agent.

## 5.9.3 CSV format

### (1) CSV data output format

CSV data is output in the order of data header 1st section, data header 2nd section, and then data section.

- Data header 1st section  
One blank row + report name + one blank row are displayed.
- Data header 2nd section  
A field header is output.  
A field schema name is output as a field column header. However, if **Display name** is set for a field in definition, the **Display name** is displayed.
- Data section  
This is output as one row per record.

### (2) Character set of text used for exporting

Set as `characterCode` in `config.xml`. Available character sets are US-ASCII, windows-1252, ISO-8859-1, UTF-8, UTF-16, UTF-16BE, UTF-16LE, Shift\_JIS, EUC-JP, EUC-JP-LINUX, and MS932.

The default setting is UTF-8.

Note:

If the `characterCode` value set in `config.xml` is not one of the above character sets, or the specified value is not defined on the platform, an error is output to the log file during initialization and the default value is used.

### (3) Linefeed code

Set as `lineSeparator` in `config.xml`. The default setting is CRLF in Windows, LF in UNIX.

If the linefeed code is CRLF, 0D0A is output. If it is LF, 0A is output.

Note:

If the setting is other than CRLF or LF, an error is output to the log file during initialization, and CRLF is used as the setting value.

### (4) File end code

After the last data is output, <EOF> is output.

### (5) Delimiter between items

The delimiter between items is represented by a comma (,). If either a comma, double quotation mark ("), or linefeed is in the data value, the data value itself is surrounded with double quotation marks.

## (6) Date format

Dates are displayed in the format corresponding to the locale. For details, see the chapter describing installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

### 5.9.4 HTML format

#### (1) HTML format when output in a Web browser

A report in HTML format consists of four parts: A report header area, a graph area, a list area, and a table area.

The following table lists the information displayed in each part, and the conditions under which the part is displayed for each type of report.

Table 5–8: Content and display conditions for each part (when output from a Web browser)

Part	Output target		
	Report (bookmark)	Combination report	Event history report
Report header area	Displays the name of the report definition, the folder where the report definition is stored <sup>#1</sup> , the name of the agent <sup>#2</sup> , and the data acquisition time <sup>#4</sup> .	Displays the name of the combination bookmark, the path of the bookmark in the bookmarks tree <sup>#4</sup> , and the data acquisition time <sup>#3</sup> .	Displays the string Event History and the data acquisition time <sup>#3</sup> .
Graph area	Displays the same image of the graph as appears in the View Report window.	Displays the same image of the graph as appears in the combination report window.	Not displayed.
List area	Displays the list data and instance numbers that appear in the View Report window.	Not displayed (combination reports do not include output in list format)	Not displayed.
Table area	All data is displayed on one page in table format.	Not displayed (combination reports do not include output in list format)	All data is displayed on one page in table format.

#1

The folder where the report definition is stored appears in the format **ParentFolder** *folder-path-name*, displayed as an absolute path.

#2

Agent names appear in the format **Agents** *agent-name*. When more than one agent name is specified, the names are separated by commas. No agent name is displayed for combination reports.

#3

The data acquisition time appears in the format **Time** (*time*). This is the same information that appears in the menu bar frame of the View Report window.

#4

The path of the bookmark in the bookmarks tree is shown as an absolute path.

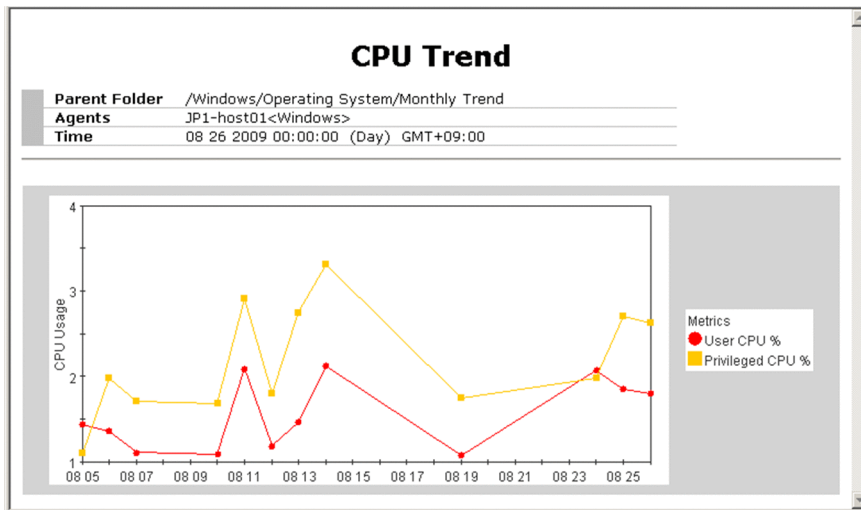
The HTML is output in UTF-8 encoding, ignoring the character set and linefeed code settings in the section of the `config.xml` file that describes the export format.

**Note**

Each time you choose the **Print** menu, a new window opens. Any print windows that have already been opened continue to display the same data. The print windows close when you close the parent window.

The following figure shows an example of outputting a report in HTML format using a Web browser.

Figure 5–17: Example of outputting a report in HTML format from the Web browser



## (2) Format when output by a command

A report in HTML format is composed of three parts: a report header area, a graph area, and a table area. The following table lists the content displayed in each part, and the conditions under which the part is displayed, for each type of report or bookmark.

Table 5–9: Content and display conditions for each part (when output by a command)

Part	Subject of output operation		
	Report	Registered report	Combination bookmark
Report header area	Displays the report name, agent name <sup>#1</sup> , date format, and command line, in a colon-separated format.	Displays the report name, agent name <sup>#1</sup> , date format, and command line, in a colon-separated format.	Displays the bookmark name, date format, and command line, in a colon-separated format.
Graph area	Displays the same image of the graph as appears in the View Report window. This part is displayed when graph display is enabled in the report definition and the show-graph tag is specified in the input file.	Displays the same image of the graph as appears in the View Report window. This part is displayed when graph display is enabled in the report definition for the registered report and the show-graph tag is specified in the input file.	Displays the same image of the graph as appears in the combination report window.
Table area	All data is displayed on one page in table format. <sup>#2</sup> This part is displayed when table display is enabled in the report definition and the show-table tag is specified in the input file.	All data is displayed on one page in table format. <sup>#2</sup> This part is displayed when table display is enabled in the report definition for the registered report and the show-table tag is specified in the input file.	Not displayed (combination reports do not include output in table format)

#1

When more than one agent name is specified, the names are separated by commas.

#2

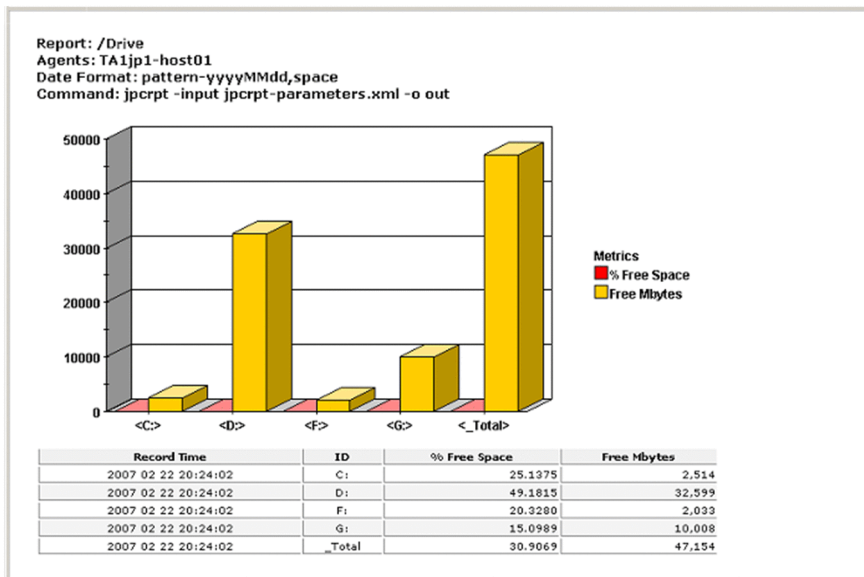
The columns appear in the table in the order in which they are defined in the report definition, with the exception of the Date and Time field. When the Date and Time field is not defined, it is added at the left of the table. When defined, the Date and Time field appears at the position defined in the report definition.

If there are 0 items of data or the agent has stopped, only the report header area is output.

The HTML is output in UTF-8 encoding, ignoring the character set and linefeed code settings in the section of the `config.xml` file that describes the export format.

The following figure shows an example of outputting a report in HTML format using a command.

Figure 5–18: Example of outputting a report in HTML format using a command





## 5.10 Notes on reports

---

### 5.10.1 Notes on creating reports

#### (1) Changing the character code

If you use double-byte characters or Japanese single-byte Katakana characters when you create reports, do not change the character code used by PFM - Manager. If you change from one character code to another, you will no longer be able to use the alarms and reports you defined before the change.

If you need to change the character code, do so by uninstalling PFM - Manager and then rebuilding the environment.

#### (2) Setting refresh intervals

If you intend to display several realtime reports simultaneously, set the refresh interval so that the windows do not automatically refresh at the same time.

#### (3) Proper use of realtime and historical reports

If you want to view long-term trends in performance data, use a historical report rather than displaying a realtime report for an extended period.

#### (4) Reports that display a large amount of data

For reports that display a large amount of data (for example, a report showing Process Detail Interval (PD\_PDI) records for PFM - Agent for Platform), use data filters or display the records by ranking so that only the necessary data is displayed.

### 5.10.2 Notes on displaying reports

#### (1) About stacked area graph

If multiple series of records are stacked in a stacked area graph, only the records that have exactly the same time will be stacked.

Therefore, if you want to display stacked records from more than one agent in a historical (multiple agents) report, set the collection interval and offset value so that they match all of the agents.

If this condition is satisfied, a collection time difference might occur due to a delay caused by collection load and the stacked area graph might not display as expected. To avoid this, you can use an optional PFM - Web Console function to adjust the record collection time for the graph display.

For details, see the description of the `<graph-time-correction>` tag of the Windows initialization file (`config.xml`) in an appendix of the manual *JP1/Performance Management Reference*.

#### (2) About pie graphs

If a report contains a large number of pie graphs, the data labels below the pie graphs might be displayed over several lines, reducing the size of the graphs themselves. In this case, take one of the following steps to resolve the issue:

- Increase the magnification of the graph
- Reduce the number of pie graphs in the report
- Reduce the number of characters displayed in data labels

The following describes how to reduce the number of characters in data labels. Perform this process in the window where you edit the report definition.

If **By row** is specified for **Series direction** in the Edit > Graph window

In the Edit > Graph window, specify a string in **Data label** that is short yet sufficient to identify the instance.

If **By column** is specified for **Series direction** in the Edit > Graph window

In the Edit > Components window, specify a short character string in **Display name**.

For example, to avoid data labels from being displayed over several lines in a report where nine pie graphs are displayed at 100% magnification, make sure that the labels contain no more than 19 single-byte or 18 double byte characters.

### (3) Maximum number of report windows displayed in the PFM - Web Console

- Display no more than four View Report windows in the PFM - Web Console.
- In one Performance Management system, display no more than 10 View Report windows that present PFM - Agent or PFM - RM information in real time. If 11 or more windows are displayed, you might fail to retrieve data.

### (4) Maximum number of data items displayed in a report

In realtime reports, data from 30 collection times can be displayed. When displaying data over 31 collection times, the data will be deleted in the order from oldest to newest data. If you want to change this maximum number, change the `maxRealtimeCache` in `config.xml`.

For historical reports, the maximum amount of displayed data of a data group is up to the maximum number of records or the maximum number set in the Windows initialization file (`config.xml`). If you want to change this maximum number, change the `maxFetchCount` (under the `<vsa>` tag).

Note that you cannot use the Web browser to change a report that has too many records to display. Use the CSV output function of the `jspcrpt` command for such a report.

### (5) About data acquisition performance

If multiple realtime reports are displayed at the same time, data acquisition performance might be degraded.

### (6) Limitation of realtime report display

If multi-instance records are collected in PFM - Agent or PFM - RM, the maximum number of instances handled by a collection is 32,767. Therefore, when displaying a realtime report of multi-instance records in the Web browser, you can display no more than 32,767 instances. You cannot display 32,768 or more instances.

### (7) Displaying a report with a large number of records

When you attempt to display a report with a large number of records in the Web browser, you might be unable to display the report if the PFM - Manager View Server service or the PFM - Web Console service has insufficient memory. Consider the following approaches to displaying reports with a large number of records.

## (a) Enabling the report cache filing function

PFM - Web Console is able to minimize the use of physical memory by temporarily storing report data in a file on disk. This function is called the *report cache filing function*, and the files it creates are called *report cache files*.

With this function enabled, PFM - Web Console references the data in report cache files when displaying reports, allowing it to keep less data in memory and reduce the likelihood of a memory shortage.

The services where a memory shortage occurs depends on whether the report being displayed contains graphs. The following describes how to avoid a memory shortage in each scenario.

- When a report contains a large amount of data and does not contain graphs  
Memory shortages occur in the View Server service of PFM - Manager, and can be avoided by enabling the report cache filing function.
- When a report contains a large amount of data and contains graphs  
Memory shortages occur in the View Server service of PFM - Manager and the PFM - Web Console service. You can avoid memory shortages in the View Server service of PFM - Manager by enabling the report cache filing function. For the PFM - Web Console service, review the contents of the report definitions with reference to [5.10.2\(8\) Taking memory requirements into consideration when planning definitions for reports that contain graphs](#).

Note:

You cannot use the report cache filing function with the baseline data used when displaying a combination report. To avoid a memory shortage, do not register a report that contains a large amount of data as a baseline.

The table below lists the types of reports that the report cache filing function supports for display in the PFM - Web Console. The function also works with reports output by the `jpcrpt` command.

Table 5–10: Reports that work with the report cache filing function

Displayed from	Report
PFM - Web Console GUI	Historical report
	Event history
	Combination report
	Print window (HTML output)
	CSV output
	Tiling display
	Realtime report (when automatic refresh is disabled or stopped)
jpcrpt command	Historical report (HTML output)
	Combination report

The report cache filing function does not apply to historical reports output in CSV format by the `jpcrpt` command. However, this scenario does not typically cause a memory shortage when outputting a report with a large number of records, because the command reads the report data as it outputs the file, not all at once.

Report cache files are stored in the following directories by default.

Type of report output	OS	Directory
Displayed in PFM - Web Console	Windows	<i>PFM-Web-Console-installation-folder</i> \reportcache\serv\
	UNIX	/opt/jplpcwebcon/reportcache/serv/
Output in HTML format by jpcrpt command	Windows	<i>PFM-Web-Console-installation-folder</i> \reportcache\cmd\
	UNIX	/opt/jplpcwebcon/reportcache/cmd/

Ordinarily, report cache files are deleted from the directory as soon as the report output process is complete. If a file could not be deleted for some reason, the system tries again with the following timing:

Directory	Timing of deletion
<ul style="list-style-type: none"> <li><i>PFM-Web-Console-installation-folder</i>\reportcache\serv\</li> <li>/opt/jplpcwebcon/reportcache/serv/</li> </ul>	The next time the PFM - Web Console service starts <sup>#1</sup>
<ul style="list-style-type: none"> <li><i>PFM-Web-Console-installation-folder</i>\reportcache\cmd\</li> <li>/opt/jplpcwebcon/reportcache/cmd/</li> </ul>	Not deleted <sup>#2</sup>

#1

Because the system deletes all files and subdirectories, do not store any files in the directory.

#2

The files will not be deleted automatically. Delete the files manually after making sure that the jpcrpt command is not running.



### Note

For details on how to estimate the disk space occupied by report cache files, see the section describing the disk space usage when using report cache files in the appendixes of the *JPI/Performance Management Planning and Configuration Guide*.

To enable the report cache filing function, specify `true` for the `useReportCacheFile` parameter in the initialization file (`config.xml`). Specify the directory in which to store report cache files in the `reportCacheFileDir` parameter of the initialization file (`config.xml`).

Note:

As the storage directory for report cache files, specify a directory on a local disk. If you specify a directory on the network, the Web browser and the jpcrpt command will operate more slowly than if the directory were on a local disk.

For details on how to configure the initialization file (`config.xml`), see the chapter describing installation and setup of Performance Management in the *JPI/Performance Management Planning and Configuration Guide*.

## (b) Outputting reports in CSV format using the jpcrpt command

When a report contains a large number of records, consider outputting the report to a CSV file instead of viewing it in PFM - Web Console.

You can use the jpcrpt command to output reports in CSV format. For details on the jpcrpt command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

## (8) Taking memory requirements into consideration when planning definitions for reports that contain graphs

When displaying reports that contain graphs, a memory shortage might occur if the amount of memory required to display the report exceeds the amount available to PFM - Web Console, preventing the report from being displayed. The memory required to display a report depends on the maximum number of records (data lines) and fields to be displayed.

You can avoid a memory shortage by keeping to the values shown below. Regardless of the graph type, a memory shortage will not occur if the data falls within these values. When displaying multiple reports simultaneously, make sure that the total data across all the reports does not exceed the values.

- Maximum number of records (data lines): 50,000
- Number of fields: 5 (when the number of records is 50,000)

Consider the above as an integrated value. That is, if the maximum number of records multiplied by the number of fields is less than  $50,000 \times 5 = 250,000$ , a memory shortage will not occur. Another example is as follows:

- Maximum number of records (data lines): 100,000
- Number of fields: 2

In this case, because  $100,000 \times 2 = 200,000$ , a memory shortage will not occur.

The following tables describe examples of report definitions that meet the criteria for avoiding a memory shortage.

Table 5–11: Report definition example 1

Definition item	Contents
Report type	Historical (single agent)
Agent	PFM - Agent for Platform (Windows)
Records	PI (single-instance record)
Selected fields	Available Mbytes
Graph fields	Cache Faults/sec Cache Mbytes Page Faults/sec Pages/sec
Graph type	Area
Report display period	Within the past month
Report interval	Minutes

Table 5–12: Report definition example 2

Definition item	Contents
Report type	Historical (single agent)
Agent	PFM - Agent for Platform (Windows)
Records	PD_PDI (multi-instance record)
Selected fields	CPU % Page File Kbytes

Definition item	Contents
Graph fields	CPU %
Graph type	Area
Report display period	Within the past day
Number of monitored processes <sup>#</sup>	30

#

This number is the number of processes (number of record instances) for which data is displayed in the report. It is not an item in the report definition.

**Table 5–13: Report definition example 3**

Definition item	Contents
Report type	Historical (multiple agents) <sup>#</sup>
Agent	PFM - Agent for Platform (Windows)
Records	PI (single-instance record)
Selected fields	Available Mbytes Cache Mbytes
Graph fields	Available Mbytes
Graph type	Line
Report display period	Within the past month
Report interval	Minutes

#

This example assumes that the report is displayed with two agents selected.

## (9) Too many graph legends to display

Although there are no restrictions on the number of fields in a report, the system might be unable to display the graph or legend in part or in its entirety if the report contains too many fields.

In PFM - Web Console 10-00 or later, you can display the fields in a graph over multiple pages. This is called *report series paging*, and allows you to view legends in their entirety. To enable this functionality, specify `true` for the `usingSeriesPagingOnTheGraph` parameter in the initialization file (`config.xml`). For details on how to configure the initialization file (`config.xml`), see the chapter describing installation and setup of Performance Management in the *JPI/Performance Management Planning and Configuration Guide*.

If you cannot see a legend in its entirety in PFM - Web Console 09-00 and earlier or in PFM - Web Console 10-00 or later with report series paging disabled, change the magnification of the graph to check whether all the legend information can be displayed. If some still cannot be displayed, add a field to the report table for each item in the legend that is not displayed. We recommended that you limit the number of fields displayed in a graph to approximately 20.

## (10) Displaying realtime reports that contain large numbers of fields

If a realtime report is split over several pages by the report series paging functionality, the number of fields might increase or decrease when the report is refreshed. This can cause different fields to be displayed on a given page.

## (11) Outputting reports with large amounts of table data to a file in HTML format

When a report output in HTML format contains a large amount of table data, displaying the tables places a considerable processing burden on the Web browser, and can sometimes cause it to hang. You can avoid this issue by limiting the number of lines of table data in reports output in HTML format.

In version 10-00 or later of PFM - Web Console, you can change the number of lines of table data in HTML-format reports by changing the value of the following parameters in the initialization file (`config.xml`).

Table 5–14: Parameters in `config.xml` that restrict the number of table data lines

Report type	Parameter in <code>config.xml</code>
Output to print window	<code>printTableMaxRowSize</code>
Output in HTML format by <code>jspcrpt</code> command	<code>cmdHtmlTableOutputMaxRowSize</code>

For details on how to configure the initialization file (`config.xml`), see the chapter describing installation and setup of Performance Management in the *JPI/Performance Management Planning and Configuration Guide*.

Even when you use these parameters to limit the number of lines of table data in a report, a report that contains a large number of fields can still exceed the tolerances of the Web browser, causing it to become unstable. To avoid this issue, review the number of fields in the report. We recommend no more than 10 fields in an environment where the default value is used for these parameters in the initialization file (`config.xml`) and Internet Explorer is used to display reports.

## (12) Displaying reports in which a large number of data items have drilldown available

When you display a field-level drilldown report, depending on the number of plots, a memory shortage might occur causing the PFM - Web Console service to shut down. You can avoid this issue by enabling the drill-down plot restriction function.

The drill-down plot restriction function restricts the number of plots (number of items of drill-down data) for fields with field-level drilldown enabled. When the number of drill-down data items exceeds a limit, field-level drilldown is disabled on the graph and clicking a field no longer displays a drilldown report. Note that this function does not disable drilldown for table and list items.

You can use the drill-down plot restriction function in version 10-00 or later of PFM - Web Console. Specify the limit in the `maxDrilldownPoints` parameter in the initialization file (`config.xml`). For details on how to configure the initialization file (`config.xml`), see the chapter describing installation and setup of Performance Management in the *JPI/Performance Management Planning and Configuration Guide*.

## (13) When reports take a long time to display

A record that has a large number of instances can take a long time to display. In this case, restrict the number of data items displayed in a graph at any one time by performing all of the following steps:

- Specify **By column** for **Series direction** in the Edit > Graph window
- Enable report series paging  
Specify `true` for the `usingSeriesPagingOnTheGraph` parameter in the initialization file (`config.xml`).
- Limit the number of fields in graph legends to 14



Specify 14 for the `displayLegendCount` parameter in the initialization file (`config.xml`).

For details on how to configure the initialization file (`config.xml`), see the chapter describing installation and setup of Performance Management in the *JP1/Performance Management Planning and Configuration Guide*.

## (14) Temporary files created when displaying or outputting a graph image

PFM - Web Console version 10-00 and later creates a temporary file approximately 10 to 100 KB in size when it displays or outputs a graph image in the following circumstances:

- A View Report window (also applies to combination report windows) containing a graph is displayed or a graph image is output
- A pie graph is displayed in the System Operational Status Summary window
- Tiling display is performed for a report registered in a bookmark

The temporary files are stored in the following directories:

In Windows

- When displaying a report in a Web browser  
The folder specified in the `TMP` system environment variable.
- When outputting a report using the `jpcrpt` command  
The folder specified in the `TMP` user environment variable for the user who executed the command.

In UNIX

The directory specified in the `TMPDIR` environment variable.  
If `TMPDIR` is not set, the directory `/var/tmp` or `/tmp`.

The temporary files are deleted after the graph image has been generated.

## 5.10.3 Notes on combination reports

### (1) Graph types and graph options

The **Show 3D graph** option can be set for any graph, but is ignored for graph types other than column or stacked column.

You can also set the **Show Grid** option for any graph, but it only applies to the graph in the foreground.

### (2) Order in which graphs are drawn

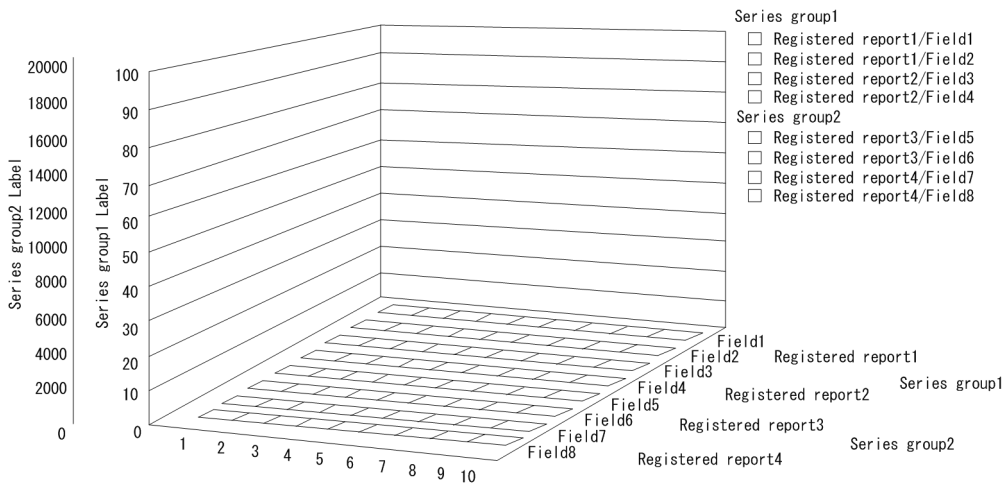
The graphs in a combination report are drawn in the following order:

1. Series groups are drawn in order from the first series group, with subsequent series groups being drawn over the earlier ones.
2. Registered reports in a series group are displayed in the order in which the report is registered in the series group, with subsequent registered reports being drawn over the top of the earlier ones.
3. Fields in a registered report are displayed in the order in which they appear in the report, with subsequent fields being drawn over the top of the earlier ones.

The following figure describes the order in which graphs are drawn.



Figure 5–19: Image showing the order in which graphs are drawn



The specific order for 1. and 2. above is determined by the series group settings you specify when defining the combination bookmark. Make sure that the settings you specify do not cause graphs to become hidden behind other graphs. The order of the fields described in 3. is determined by the settings in the window where you created or edited the report definition.

When a series group contains 3D clustered column/3D stacked column graphs or line graphs, any group can be displayed in the foreground regardless of the order of the series groups. You can specify which graph to display in the foreground in the `<foregroundCombinationGraph>` tag of the initialization file (`config.xml`).

The following table describes the order in which graphs are drawn for each value of the `<foregroundCombinationGraph>` tag.

Value of <code>&lt;foregroundCombinationGraph&gt;</code> tag	Draw order
3DBAR (default)	Graphs are drawn in the following order from front to back: <ol style="list-style-type: none"> <li>1. 3D clustered column/3D stacked column</li> <li>2. Line</li> <li>3. Clustered column/Stacked column/Area/Stacked area</li> </ol>
LINE	Graphs are drawn in the following order from front to back: <ol style="list-style-type: none"> <li>1. Line</li> <li>2. 3D clustered column/3D stacked column</li> <li>3. Clustered column/Stacked column/Area/Stacked area</li> </ol>

For details, see the section describing the `<foregroundCombinationGraph>` tag of the initialization file (`config.xml`) in the appendixes of the manual *JP1/Performance Management Reference*.

### (3) Horizontal axis (X-axis) and vertical axis (Y-axis) of graphs

- You cannot use common settings that apply across the entire combination report.  
For the Y-axis of each series group in a combination report, you can use either automatic scale adjustment (where the axis is adjusted to the maximum and minimum values of the actual data) or manual scale adjustment (where the maximum and minimum values are specified by the user). You can also choose whether to display the axis label on the left or right side of the graph.
- The X-axis for a combination report is a single fixed time series.  
Data collected over a date range or with an interval that does not match the X-axis is assumed to be missing some information and the system attempts to compensate it. This might compromise the integrity of the graph. If a

misalignment in the collection interval occurs when PD records are collected, a stacked graph might not be displayed normally. We recommend that you use a line graph when the data includes PD records.

To avoid this, you can use an optional PFM - Web Console function to adjust the record collection time for the graph display. For details, see the description of the `<graph-time-correction>` tag of the Windows configuration file (`config.xml`) in an appendix of the manual *JPI/Performance Management Reference*.

- The order of the Y axis scales for a combination report matches the order in which the graphs are drawn. Of the series groups in a combination report, the Y axis scale associated with the series group in the foreground is drawn closest to the graph. Each subsequent Y axis scale is drawn in order on the outside of the previous scale.

## (4) Number of fields in a report

- Although there are no restrictions on the number of fields in a combination report, the system might be unable to display the graph or legend in part or in its entirety when the report contains too many fields. In this case, either increase the magnification of the graph, or use the following methods to restrict the number of fields displayed in the graph (we recommend that graphs display no more than approximately 20 fields).
  - Edit the combination bookmark to remove some of the reports from the graph.
  - Edit the report definitions to contain fewer fields, and then recreate the registered reports.
  - Edit the report definitions to apply filter conditions, and then recreate the registered reports.
  - Recreate the registered reports using shorter display names for the fields than the default field names.

If the following parameters are exceeded, the system might be unable to display the graph or legend in part or in its entirety, or the legend might be displayed over two or more lines.

- 100% magnification: Legend approx. 20 lines
- 200% magnification: Legend approx. 30 lines
- 400% magnification: Legend approx. 50 lines
- 600% magnification: Legend approx. 50 lines
- 800% magnification: Legend approx. 70 lines
- When the legend for a combination report contains too many characters, part of the legend might be cut off. In this case, either increase the magnification of the graph, or use the following methods to restrict the number of characters displayed in the legend.
  - Shorten the report names and then recreate the registered reports.
  - Recreate the registered reports using shorter display names for the fields than the default field names.
  - Reduce the number of bound agents and then recreate the registered reports.

If the following parameters are exceeded, the system might be unable to display the legend in its entirety:

- 100% magnification: Legend approx. 50 double byte or 80 single byte characters
- 200% magnification: Legend approx. 80 double byte or 120 single byte characters
- 400% magnification: Legend approx. 110 double byte or 160 single byte characters
- 600% magnification: Legend approx. 140 double byte or 200 single byte characters
- 800% magnification: Legend approx. 160 double byte or 230 single byte characters

## (5) Series group settings

- At least one registered report must be assigned to a series group. No graph is displayed if none of the series groups contain any registered reports, or when the combination bookmark contains only a baseline.

- If the name of a series group in a combination report contains a large number of characters, the series group name and legend might overlap. You can resolve this issue by increasing the magnification of the graph or reducing the number of characters in the series group name.

For example, in a graph where a series group name contains approximately 25 double-byte or 30 single-byte characters and the legend contains approximately 10 lines, the series group name and legend can overlap when the magnification is at 100%. You can eliminate the overlap by increasing the magnification to 200% or more.

## (6) Date range of reports

When you set the date range of a report to a **Within the past ...** option (for example **Within the past hour**), the report is updated with the data from that time period up to the present time when you choose **Refresh** in the View Report window. The start time of the baseline remains unchanged.

If you choose **Specify when displayed** as the date range, the **Start time** and **End time** set for the report and the start time of the baseline remain unchanged when you choose **Refresh** in the View Report window.

## (7) Baseline display periods

- The **Start time** setting for the baseline display period is determined automatically based on the current time when the combination report was started and the **Date range** and **Report interval** settings for the report display period. When you change these settings, the **Start time** setting for the baseline display period is set to the **Start time** setting for the report display period.
- When you choose **Refresh** in the View Report window, the **Start time** and **End time** of the settings for the report display period might change according to the **Date range** setting. However, the **Start time** setting for the baseline display period will remain unchanged.
- Changes to the **Start time** setting for the baseline display period or the baseline data do not affect the starting points and ending points of graphs created from combination reports. However, when the report displayed with the baseline contains only one piece of data (data with the same starting point and ending point), the graph's starting point and ending point might be set to the range of the data collected as the baseline. The starting point and ending point of the actual display period for the graph is determined based on the data present in the range from the **Start time** to the **End time** in the report display period settings.
- The **Start time** setting for the baseline display period applies to the individual baseline. When a baseline contains data from multiple fields each with different start times, the field data with the earliest start time in the time series after the **Start time** setting for the baseline display period serves as the starting point. All other fields are displayed according to the start times determined when the baseline data was saved.
- When data from multiple fields with different start times is registered as a baseline, the graph is drawn with the field data earliest in the time series after the **Start time** setting for the baseline display period serving as the starting point. In this case, the relative start positions of each subsequent field are preserved.

## (8) Length of graph titles

You can display a maximum of 64 single or double byte characters in a graph title. However, when the magnification is 100%, a title that contains more than 60 double-byte characters might be displayed over two lines. The title will be displayed on one line if the characters are single byte.

## (9) Displaying PD type records

In PFM - Web Console version 10-00 or later, the following can occur when you display PD type records in a clustered column or stacked column graph:

- The column width can become narrow when there are inconsistencies in the record collection interval.

- If the record collection interval is one hour or longer, the position of the column can differ from the same graph in versions of PFM - Web Console earlier than 10-00.

For this reason, we recommend that you use a line graph when displaying PD type records in a combination report in PFM - Web Console 10-00 and later.

# 6

## Monitoring Operations with Alarms

In Performance Management, an *alarm* is used to notify the user when collected performance data has exceeded a user-defined threshold.

This chapter explains how to create alarms and use them to notify the user of problems.

## 6.1 Overview of alarms

---

Performance Management can be set up to notify the user of when performance data monitored by a monitoring agent exceeds a user-defined threshold.

A definition of how the system should behave when data reaches a threshold value is called an *alarm*. A set of alarms is called an *alarm table*. Each PFM - Agent type or PFM -RM type has a *folder* in which it stores alarm tables.

The folder is displayed on the second level of the Alarms tree. You can display the Alarms tree by selecting the **Alarms** tab from the navigation frame of the PFM - Web Console Main window.

When the data reaches a threshold value, the monitoring agent reports the information by issuing an *alarm event*. Performance Management receives the alarm event, and then performs one or more tasks, which are called *actions*. Performance Management can perform the following actions:

- Notify the system administrator via email
- Execute one or more commands, such as a restore program
- Issue a JP1 event in order to link with other JP1 products
- Send an SNMP trap

By linking an alarm table to a monitoring agent, you can detect when any thresholds are exceeded. The act of linking an alarm table to a monitoring agent is called *binding*.

In addition, each monitoring agent can have multiple alarm tables bound to it.

## 6.2 Setting up and operating alarms

---

You can use the Quick Guide to set simplified alarms. For details on the Quick Guide, see [6.5 Setting alarms using the Web browser \(Quick Guide\)](#).

### 6.2.1 How to set up and operate alarms

Alarms are set up and operated by using the Alarms window in PFM - Web Console or by using a command.

You can set up alarms in the following ways:

- Define a new alarm table or individual alarms.

Create a new alarm table for your system environment, and then define the alarms. You can add new alarms to that alarm table at a later time.

In addition, you can use the Quick Guide to set simplified alarms. Alarms set using the Quick Guide can be bound to an agent.

- Use an existing alarm table or alarms.

You can use the following methods:

- Use the monitoring template.

The monitoring template is a set of alarms, which necessary information has been preset, included with each PFM - Agent or PFM - RM. When you use the monitoring template, any active alarms in the monitoring template are enabled when PFM- Agent or PFM - RM is started.

- Customize the monitoring template.

You can copy the monitoring template and customize it to match your monitoring objectives.

- Use an existing alarm table or alarms.

You can make a copy of, and then customize one of the already user-defined alarm tables or alarms.

To use alarms, associate (or bind) the alarm table defined above with a monitoring agent.

Reference note:

- By using the `jpctool alarm` command to create an alarm definition file, you can create up to 250 alarms at once. This is a useful technique when setting up multiple alarms at the same time to run on multiple servers in a large-scale system.
- Once you have set up alarms, you can use the Alarm Application Status window or the `jpctool alarm unapplied` command to check each service's alarm application status.
- Alarm tables are displayed in a tree format that is referred to as the alarms tree. You can select either of two display formats for the alarms tree:
  - Displaying separate trees: This format displays user-created alarm tables under **User Alarms** and monitoring templates under **Template Alarms**.
  - Displaying together: This format displays user-created alarm tables and monitoring templates as a single tree under the same root **Alarms**.

To change the alarms tree display format, edit `displayAlarmTablesSeparately` in the initialization file (`config.xml`). For details about how to specify settings in the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JP1/Performance Management Reference*.

You can bind an alarm table (or alarm tables) to monitoring agents as follows:

- Define alarms and then manually bind the alarm table to monitoring agents after the start of the monitoring manager and monitoring agent service (*manual bind*).

In this case, alarm monitoring is initiated when the alarm table is bound to the monitoring agents. Any errors that occur between the start of the monitoring agent service and the binding of the alarm table do not get detected.

- Define alarms and specify the auto alarm table bind setting after the start of the monitoring manager but before the start of the monitoring agent service so that, when the monitoring agents start, the alarm table is automatically bound to them (*automatic bind*).

In this case, the alarm table is automatically bound to the monitoring agents when the monitoring agent service starts, after which alarm monitoring is initiated.



### Note

To use auto alarm bind, you have to enable the functionality for binding multiple alarm tables in advance.

## 6.2.2 Alarm evaluation

This subsection gives an explanation about alarm evaluation. The following legend applies to the contents of this subsection in general.

Legend:

--: Not issued.

Always: Whether **Always notify** is selected

All: Whether **Evaluate all data** is selected

Y: Used (selected)

N: Not used (not selected)

### (1) Differences among alarm evaluations depending on combinations of alarm conditions

The way an alarm is evaluated depends on the alarm conditions and the type of record to be evaluated. The following table describes the differences among alarm evaluations for various combinations of alarm conditions.

Table 6–1: Differences among alarm evaluations for various alarm conditions (when "Monitor whether the value exists" is not selected)

Record type	Alarm notification	Notification target	Condition	Alarm evaluation (report)
Single-instance record	Notify when the state changed is selected	State changes for the alarm is selected	Evaluate all data is not selected	<ul style="list-style-type: none"> <li>• If an Abnormal condition is met, and the previously reported alarm was other than Abnormal (red), an Abnormal (red) alarm is reported.</li> <li>• If an Abnormal condition is not met but a Warning condition is met, and the previously reported alarm was other than Warning (yellow), a Warning (yellow) alarm is reported.</li> </ul>
		State changes for each record instance is selected	--	



Record type	Alarm notification	Notification target	Condition	Alarm evaluation (report)
Single-instance record	<b>Always notify</b> is selected	--	<b>Evaluate all data</b> is not selected	If either an Abnormal or Warning condition is met, an Abnormal or Warning alarm is reported, regardless of any previously reported alarm.
		--	<b>Evaluate all data</b> is selected	
Multi-instance record	<b>Notify when the state changed</b> is selected	<b>State changes for the alarm</b> is selected	<b>Evaluate all data</b> is not selected	<ul style="list-style-type: none"> <li>If one Abnormal condition instance is found, and the previously reported alarm was other than Abnormal (red), an Abnormal (red) alarm is reported for that instance.</li> <li>If no instance is found that meets an Abnormal condition, one instance is found that meets a Warning condition, and the previously reported alarm was other than Warning (yellow), a Warning (yellow) alarm is reported for that instance.</li> <li>If none of the collected instances match the cases above, and the previously reported alarm was Abnormal (red) or Warning (yellow), a Normal (green) alarm is reported.</li> </ul> <p>Note: As soon as any instance is found that meets a condition, alarm evaluation ends. Therefore, not all of the collected instances are always evaluated.</p>
			<b>Evaluate all data</b> is selected	<ul style="list-style-type: none"> <li>If, after all of the collected instances are evaluated, one or more instances are found that meet an Abnormal condition, and the previously reported alarm was other than Abnormal (red), an Abnormal (red) alarm is reported for each of those instances.</li> <li>If, after all of the collected instances are evaluated, no instances are found that meet an Abnormal condition, one or more instances are found that meet a Warning condition, and the previously reported alarm was other than Warning (yellow), a Warning (yellow) alarm is reported for each of those instances.</li> <li>If none of the collected instances match the cases above, and the previously reported alarm was Abnormal (red) or Warning (yellow), a Normal (green) alarm is reported.</li> </ul> <p>Note: Because all of the instances are evaluated, more than one alarm can be reported in one interval.</p>
		<b>State changes for each record instance</b> is selected	--	<ul style="list-style-type: none"> <li>If, after all of the collected instances are evaluated, one or more instances are found that meet an Abnormal condition, and the alarm of the applicable instances is other than Abnormal (red), an Abnormal (red) alarm is reported for each of those instances.</li> <li>If, after all of the collected instances are evaluated, no instance is found that meets an Abnormal condition, one or more instances are found that meet a Warning condition, and the alarm of the applicable instances is other than Warning (yellow), a Warning (yellow) alarm is reported for each of the applicable instances.</li> <li>If none of the collected instances match the cases above, and the previously reported alarm of the applicable instances was Abnormal (red) or Warning (yellow), a Normal (green) alarm is reported.</li> </ul>

Record type	Alarm notification	Notification target	Condition	Alarm evaluation (report)
Multi-instance record	<b>Notify when the state changed</b> is selected	<b>State changes for each record instance</b> is selected	--	Note: Because all of the instances are evaluated, more than one alarm can be reported in one interval.
	<b>Always notify</b> is selected	--	<b>Evaluate all data</b> is not selected	<ul style="list-style-type: none"> <li>As soon as one instance is found that meets an Abnormal condition, an Abnormal alarm is reported based on that instance, regardless of any previously reported alarm.</li> <li>As soon as one instance is found that meets a Warning condition but no instance has yet been found that meets an Abnormal condition, a Warning alarm is reported based on that instance, regardless of any previously reported alarm.</li> </ul> <p>Note: As soon as any instance is found that meets a condition, alarm evaluation ends. Therefore, not all of the collected instances are always evaluated.</p>
		--	<b>Evaluate all data</b> is selected	For each instance that meets either an Abnormal or Warning condition, an Abnormal (or Warning) alarm is reported. Note: Because all of the instances are evaluated, more than one alarm might be reported in one interval.

Table 6–2: Differences among alarm evaluations for various alarm conditions (when Monitor whether the value exists is selected)

Record type	Alarm notification	Notification target	Condition	Alarm evaluation (report)	
Multi-instance record	<b>Notify when the state changed</b> is selected	<b>State changes for the alarm</b> is selected	<b>Evaluate all data</b> is not selected	All of the collected instances are checked for the values specified in the <b>New Alarm &gt; Alarm Conditions</b> window or the <b>Edit &gt; Alarm Conditions</b> window, and if no such values are found (none of the conditions are met), an Abnormal (red) alarm is reported. Note: An alarm notifying of no operation is reported only once. If no instance is collected, the alarm is not evaluated.	
			<b>Evaluate all data</b> is selected		
	<b>Always notify</b> is selected	--	<b>State changes for each record instance</b> is selected	--	--#
			--	<b>Evaluate all data</b> is selected	All of the collected instances are checked for the values specified in the <b>New Alarm &gt; Alarm Conditions</b> window or the <b>Edit &gt; Alarm Conditions</b> window, and if no such values are found (none of the conditions are met), an Abnormal (red) alarm is reported. Note: An alarm is reported every time. If no instance is collected, the alarm is not evaluated.

#

When **Monitor whether the value exists** is selected, **State changes for each record instance** cannot be selected.

The alarm evaluation method is explained for various alarm conditions below.

When you select **Monitor whether the value exists**:

All fields in records of PD and PI record types that are specified in alarm conditions are evaluated to check for the specified value. If the value is not found, the alarm is reported once per interval.

When you set alarm conditions:

When you set alarm conditions, multiple records are collected in one interval for the record of PD and PI record types to be evaluated in this alarm. If you do not select **Evaluate all data**, as soon as the first instance is found that meets the conditional expression, an alarm is reported and evaluation ends. Therefore, to evaluate all the performance data in an alarm, select **Evaluate all data** or **State changes for each record instance**.

## (2) Differences among alarm evaluations depending on whether Damping is enabled

In addition to the differences among alarm evaluations for various alarm conditions, if you set **Damping**, other differences are added to the alarm evaluation. The following table describes the differences among alarm evaluations for various alarm conditions with damping.

Table 6–3: Differences among alarm evaluations with damping

Damping	Always	All	Alarm evaluation (notification)
Y	N	N	<ul style="list-style-type: none"> <li>The alarm is reported only when the status of the alarm changes from the previously reported status.</li> <li>Based on the instance that indicates the highest severity at the time of reporting, the status of the alarm is reported.</li> </ul> <p>Note: Because the status of the alarm is determined by evaluating the damping condition, the status of the alarm might differ from the threshold of the reported instance.</p>
Y	N	Y	<ul style="list-style-type: none"> <li>The alarm is reported only when the status of the alarm changes from the previously reported status.</li> <li>If the status is Warning or Abnormal, the status of the alarm is reported based on all of the instances that meet the status condition at the time of reporting the alarm.</li> </ul> <p>Note: Because the status of the alarm is determined by evaluating the damping condition, the status of the alarm might differ from the threshold of the reported instance.</p>
Y	Y	N	The instance that indicates the highest severity at the time of reporting the alarm is reported.
Y	Y	Y	All data that meets the warning or abnormal condition at the time of reporting the alarm is reported.

The following table describes the differences when alarms are reported depending on the value set for **Damping**.

Damping	When the alarm is reported
$n/m$	<p><b>Always notify</b> is not selected:</p> <p>The alarm is reported when the threshold is exceeded <math>n</math> times during <math>m</math> evaluations of the alarm. Subsequently, the alarm is reported only if the alarm occurs the specified number of times and the status of the alarm has changed since the previous time it was reported.</p> <p><b>Always notify</b> is selected:</p> <p>The alarm is reported when the threshold is exceeded <math>n</math> times during <math>m</math> evaluations of the alarm. Subsequently, the alarm is reported every time the threshold is exceeded <math>n</math> times during <math>m</math> evaluations of the alarm.</p>
$n/n^\#$	<p><b>Always notify</b> is not selected:</p> <p>The alarm is reported when the threshold is exceeded <math>n</math> times during <math>n</math> evaluations of the alarm. Subsequently, the alarm is reported only if the alarm occurs the specified number of times and the status of the alarm has changed since the previous time it was reported.</p>

Damping	When the alarm is reported
$n/n^{\#}$	<p><b>Always notify</b> is selected:</p> <p>The alarm is reported when the threshold is exceeded <math>n</math> times during <math>n</math> evaluations of the alarm. Subsequently, the alarm is reported every time the threshold is exceeded <math>n</math> times during <math>n</math> evaluations of the alarm.</p>

#:

If **Always notify** is selected, the alarm is issued the first time the threshold is reached after the start of data collection, regardless of the occurrence frequency specified. Afterwards, the alarm is issued only when the alarm occurs for the specified number of times.

### (3) Evaluating alarms with a monitoring time range and damping conditions specified (when "State changes for each record instance" is not selected)

If you specify a monitoring time range, a normal alarm is issued at the specified end time. However, in calculating alarm damping, the system includes previous monitoring time ranges. An example of evaluating an alarm with a monitoring time range specified is given below.

#### Alarm conditions

- Monitoring time range: 9:00 to 21:00
- Damping: Threshold exceeded twice in three evaluations
- **Always notify**: Not selected
- **Evaluate all data**: Not selected

The alarm enters abnormal or warning status when the threshold is exceeded twice inside the monitoring time range for that day. When the monitoring time range is over, the alarm reverts to normal status. The following day, the status of the monitoring agent at the end of the previous day's monitoring time range (in this case *abnormal* or *warning*) is inherited at the start of the monitoring time range on the following day. Therefore, when the threshold is first exceeded in the monitoring time range of the following day, the condition of exceeding the threshold twice in three evaluations is met, and an abnormal or warning alarm is issued.

In this scenario, alarms are issued as follows:

Day	Time		Monitoring agent status	Issued alarm
First	20:58	Inside monitoring time range	Normal	--
	20:59		Abnormal	--
	21:00		Abnormal	Abnormal alarm <sup>#1</sup>
	21:01	Outside monitoring time range	Not evaluated	Normal alarm <sup>#2</sup>
	21:02		Not evaluated	--
:				
Second	8:59	Outside monitoring time range	Not evaluated	--
	9:00	Inside monitoring time range	Abnormal	Abnormal alarm <sup>#3</sup>

#1

An abnormal alarm is issued because the damping condition of *Threshold exceeded twice in three evaluations* was met.

#2

A normal alarm (Alarm expired) is issued because the monitoring end time was reached.

#3

Because the status of the monitoring agent for the previous day is inherited, the damping condition of *Threshold exceeded twice in three evaluations* is met and an abnormal alarm is issued.

#### (4) Evaluating alarms with a monitoring time range and damping conditions specified (when "State changes for each record instance" is selected)

If you specify a monitoring time range, a normal alarm is issued at the specified end time.

When **State changes for each record instance** is selected, the resultant behavior varies depending on the status of the alarm when the time falls outside the monitoring time range. If the alarm is in normal status when the time falls outside the monitoring time range, neither the occurrence frequency is cleared nor the alarm event (Alarm Expired) is reported. If, on the other hand, the alarm is in abnormal or warning status when the time falls outside the monitoring time range, the occurrence frequency is cleared and the alarm event (Alarm Expired) is reported once. When the time is in the monitoring time range, a new evaluation starts as is the case with alarm binding.

An example of evaluating an alarm with a monitoring time range specified is given below.

Alarm conditions

- Monitoring time range: 9:00 to 21:00
- Damping: Threshold exceeded twice in three evaluations
- **State changes for each record instance**: Selected
- **Evaluate all data**: Not selected

The alarm enters abnormal or warning status when the threshold is exceeded twice inside the monitoring time range for that day. When the monitoring time range is over, the alarm reverts to normal status. The following day, the status of the monitoring agent at the end of the previous day's monitoring time range (in this case *abnormal* or *warning*) is not inherited at the start of the monitoring time range. Therefore, when the threshold is exceeded twice in the monitoring time range of the following day, the condition of exceeding the threshold twice in three evaluations is met.

In this scenario, alarms are issued as follows:

Day	Time		Monitoring agent status	Issued alarm
First	20:58	Inside monitoring time range	Normal	--
	20:59		Abnormal	--
	21:00		Abnormal	Abnormal alarm <sup>#1</sup>
	21:01	Outside monitoring time range	Not evaluated	Normal alarm <sup>#2</sup>
	21:02		Not evaluated	--
	:			
Second	8:59	Outside monitoring time range	Not evaluated	--
	9:00	Inside monitoring time range	Abnormal	--#3
	9:01		Abnormal	Abnormal alarm <sup>#1</sup>

#1

An abnormal alarm is issued because the damping condition of *Threshold exceeded twice in three evaluations* was met.

#2

The damping value is cleared and a normal alarm (Alarm expired) is issued because the monitoring end time was reached.

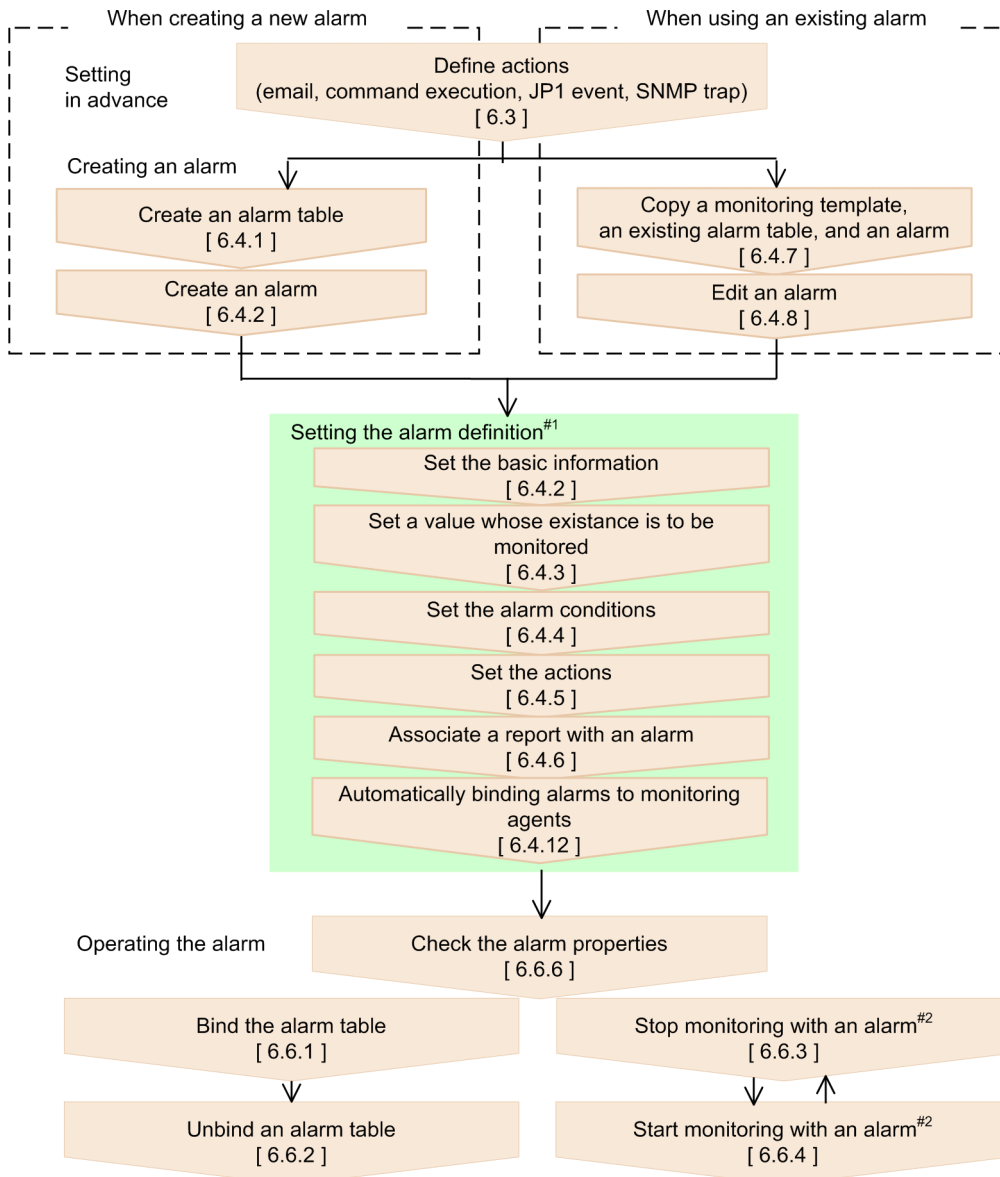
#3

Because the status of the monitoring agent for the previous day is not inherited, the damping condition of *Threshold exceeded twice in three evaluations* is not met.

## 6.2.3 Flow chart for setting up and operating alarms

The figure below is a flow chart for setting up and operating alarms. When you use the Quick Guide to set and operate alarms, perform the procedures in [6.3 Procedures before setting alarms](#) and [6.5 Setting alarms using the Web browser \(Quick Guide\)](#).

Figure 6–1: Flow chart for setting up and operating alarms



Legend: [ ] : See the indicated step.  
#1 Edit as needed when using an existing alarm.  
#2 Perform as needed.

## **(1) Detecting an error that occurs during auto alarm bind**

When an error occurs during auto alarm bind, one of the following error messages is output to the common message log:

- KAVE00559-E
- KAVE00562-E
- KAVE00563-E

If you are using log file trapping provided by JP1/IM to detect an error that occurs during auto alarm bind, set these error messages as conditions.

If you are not using log file trapping, confirm if any of these error messages have been output to the common message log of the PFM - Manager host.

## 6.3 Procedures before setting alarms

---

### 6.3.1 Configuring the email sender

If you want an email to be sent out when an alarm event occurs in PFM - Agent or PFM - RM, you need to configure the email sender.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Services** tab.
3. In the navigation frame of the Services window, click the **Machines** folder.  
This folder contains folders for the hosts where a Performance Management program is installed.
4. Select the Action Handler service on the host that will send the email.  
The name of the icon indicating the Action Handler service begins with **PH** or is the same as *host-name*<Action Handler>.
5. In the method frame, select **Properties**.  
The Properties window appears.  
Set the properties to the following:  
**Email in Capabilities:** *Yes*  
**SMTP Host in Mail:** the host name or IP address of the SMTP server that will send out emails  
**SMTP Sender in Mail:** the email address of the sender  
**Mail Subject in Mail:** the subject of the emails
6. Click the **Finish** or **Apply** button.  
The values set in step 5 are saved. For details on the settings for each alarm, see [6.4.5\(1\) Sending emails](#).

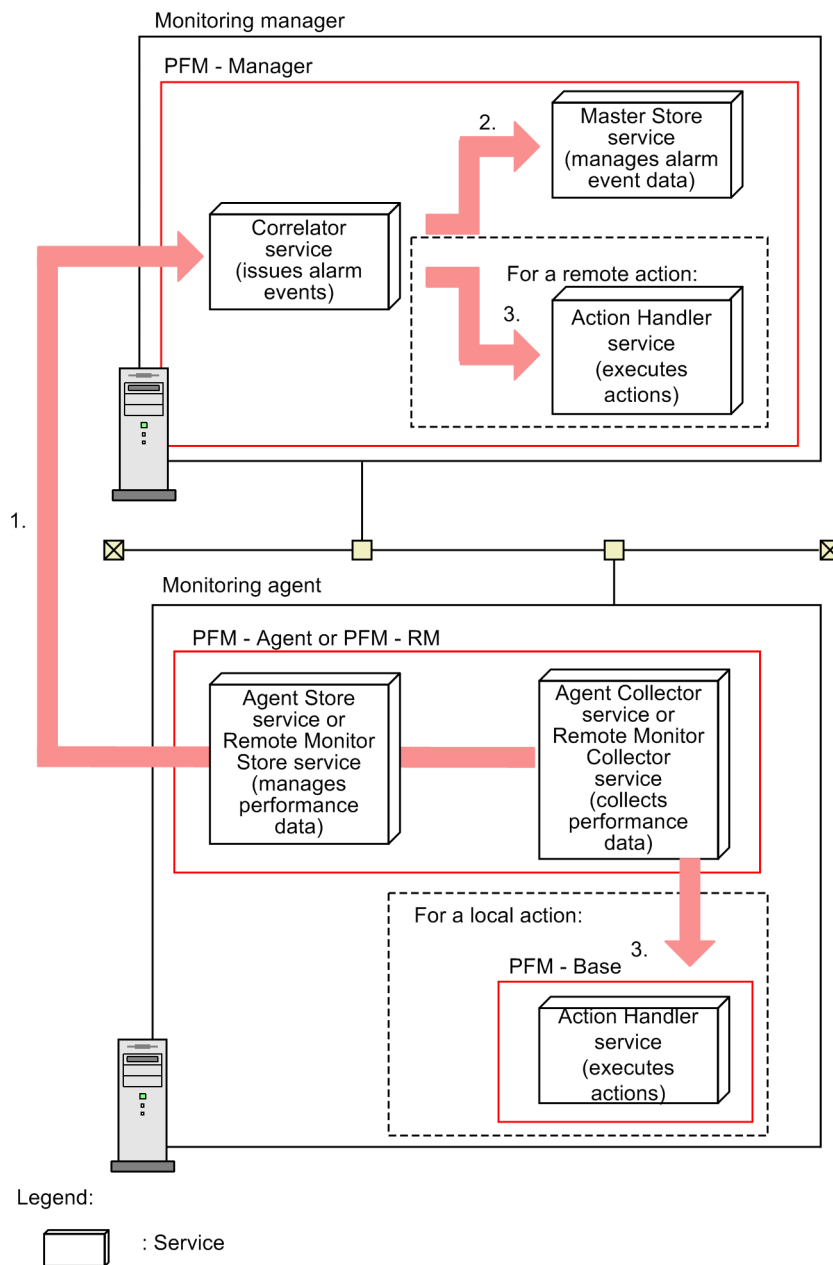
### 6.3.2 Configuring the host to automatically execute commands

If you want commands to be automatically executed when an alarm event occurs in PFM - Agent or PFM - RM, in the Service Properties window of the Services tree window in PFM - Web Console, you must set the appropriate Action Handler property on the host where the commands will be executed as follows:

- **Script in Capabilities:** *Yes*  
The action handler you select in the **Action handler** of the **Command** field in the New Alarm > Action Definitions window is used when executing the commands. By default, the Action Handler that is used is the one that resides on the same host as the agent bound to this alarm event (indicated as **LOCAL** in the **Command** tab).  
For details on the settings for each alarm, see [6.4.5\(2\) Executing commands](#).  
The actions in which a command is executed by the Action Handler on the same host as a monitoring agent bound to alarm tables are called *local actions*. The actions in which a command is executed by the Action Handler on the different host from a monitoring agent bound to alarm tables are called *remote actions*.  
The following figure shows an overview of local actions and remote actions.



Figure 6–2: Overview of local actions and remote actions



The following procedure describes the processing flow by using the numbers displayed in the above figure:

1. If the Agent Collector or Remote Monitor Collector service detects an alarm status change, an alarm event is issued to the Correlator service via the Agent Store or Remote Monitor Store service.
2. The alarm event information is stored in the Master Store service.
3. The Action Handler service receives an alarm event.

When an alarm event is received, the Action Handler service executes the specified command.

When a local action is required, the Action Handler service executes the command on the same host as the monitoring agent.

When a remote action is required, an Action Handler service (a monitoring manager or a monitoring agent) on a different host from that of the monitoring agent executes the command.

### 6.3.3 Configuration for issuing JP1 events

If you want to issue JP1 events when the alarm event occurs in PFM - Agent or PFM - RM, in the Service Properties window of the Services tree window in PFM - Web Console, you must set the appropriate Action Handler property on the host where the JP1 event-issuing command will be executed as follows:

- **Script in Capabilities:** Yes

The action handler you select in the **Action handler** of the **Command** field in the New Alarm > Action Definitions window is used when executing the commands. By default, the Action Handler that is used is the one that resides on the same host as the agent bound to this alarm event (indicated as **LOCAL** in the **Command** tab).

To issue JP1 events, you must configure the Action Handler to link with JP1/IM. For details on how to do this, see [12.3.2 Setup for linking with JP1/IM](#).

### 6.3.4 Configuration for sending SNMP traps

If you want SNMP traps to be sent when an alarm event occurs in PFM - Agent or PFM - RM, in the Service Properties window of the Services tree window in PFM - Web Console, you must set the appropriate Trap Generator property to issue the SNMP trap as follows:

- **ADD A DESTINATION in ADD OR DELETE A TRAP DESTINATION:** The host name or IP address of where the SNMP will be sent

Note that if you want to delete the location where the SNMP is sent to, select the host name or IP address in **DELETE A DESTINATION**, from the Trap Generator properties.

For details on the settings for each alarm, see [6.4.5\(4\) Sending an SNMP trap when an alarm occurs](#).

For details about SNMP traps, see the appendix that describes SNMP traps in the manual *JP1/Performance Management Reference*.

### 6.3.5 Setting the function for measurement value output at alarm recovery

Because alarms that monitor multi-instance records only enter normal status when the value of every instance is in the normal range, they do not identify the specific instance that caused the alarm to be generated. For this reason, fixed values are displayed for measured values and message text when conditions return to normal.

If you enable the function for measurement value output at alarm recovery, the instance that most recently caused the alarm to enter abnormal or warning status is assumed to be responsible for its return to normal status, and the measured values and message text are set accordingly.

The following table describes how this function affects the alarm generated when an alarm that monitors a multi-instance record returns to normal status.

Table 6–4: Differences between alarms generated at return to normal status

Item	Function for measurement value output at alarm recovery	
	Enabled	Disabled
Number of alarms generated	The number of alarms generated simultaneously when the last abnormal or warning alarm was generated	1

Item	Function for measurement value output at alarm recovery	
	Enabled	Disabled
Measured value (the variable %CVS in the alarm definition)	The current value of the instance that caused the last abnormal or warning alarm to be generated <sup>#</sup>	<OK>
The contents of the message text (the variable %MTS in the alarm definition)	The value set in the alarm definition	--

Legend:

--: Not generated.

#

If the instance has no value, (N/A) is set.

For details on how to set the function for measurement value output at alarm recovery, see the chapter describing installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

### Tip

Even with the function for measurement value output at alarm recovery enabled, the only part of the alarm message text that changes is the measured value. Therefore, if you write alarm message text that refers to the alarm being in abnormal or warning status, the message receiver might assume that the instance to which it refers is in abnormal or warning status, when in fact it indicates a return to normal status. For this reason, we recommend that you do not include references to the alarm status in alarm message text in a system with the function for measurement value output at alarm recovery enabled.

Also, some monitoring template alarms for PFM - Agent and PFM - RM might contain alarm message text that refers to the alarm status. When using such a monitoring template alarm in a system with the function for measurement value output at alarm recovery enabled, we recommend that you copy the alarm table and edit the alarm message text as needed.

## (1) Contents of alarm message text

This subsection describes the contents of alarm message text, using the Abnormal Status(A) alarm of the health check agent as an example. The Abnormal Status(A) alarm monitors the health check status of an agent. In the example below, the alarm monitors PFM - Agent for Platform (Windows) on the server `host01`.

The following table describes how the function for measurement value output at alarm recovery affects the alarm message text.

Table 6–5: Effect of the function for measurement value output at alarm recovery on alarm message text

Event	Alarm message text	
	With feature enabled	With feature disabled
A value exceeds the threshold and an abnormal or warning alarm is reported	Status of TA1host01 changed to Incomplete	Status of TA1host01 changed to Incomplete
The value enters a normal range and a normal alarm is reported	Status of TA1host01 changed to Running	--

Legend:

--: Not output.

## (2) Examples of alarm settings and generated alarms

For each of the following alarm types, this subsection describes examples of issued alarms and their message text:

- Standard alarms  
An alarm for which both **Notify when the state changed**<sup>#1</sup> and **State changes for the alarm**<sup>#1</sup> are set and **Evaluate all data**<sup>#1</sup> is not set.
- Alarms that monitor whether a value exists  
An alarm for which **Check whether the value exists**<sup>#2</sup> is set.
- Alarms that evaluate all data  
An alarm for which **Evaluate all data**<sup>#1</sup> is set.

#1

For details, see the chapter describing the New Alarm > Basic Information window or the Edit > Basic Information window in the manual *JPI/Performance Management Reference*.

#2

For details, see [6.4.3 Setting a value whose existence is to be monitored](#).

### (a) Standard alarms

The following describes an example of a standard alarm. In this example, the alarm monitors PFM - Agent for Platform (Windows). The alarm definition is as follows:



- **Message text:** Disk Busy % (%CVS1) = %CVS2
- **Check whether the value exists:** Not selected.
- **Activate alarm:** Selected.
- **Notify when the state changed:** Selected.
- **State changes for the alarm:** Selected.
- **Evaluate all data:** Not selected.
- **Evaluate regularly:** Selected.
- **Alarm when damping conditions are satisfied:** Not selected.
- **Record:** Logical Disk Overview (PI\_LOGD)
- **Abnormal:** ID <> "\_Total" AND % Disk Time >= "90.000"
- **Warning:** ID <> "\_Total" AND % Disk Time >= "50.000"

#### ■ When an instance enters abnormal or warning status after an alarm of that status has been generated

The following table describes an example in which an abnormal or warning alarm is generated for an instance, after which another instance enters the same status as the alarm.

Table 6–6: Example of alarms issued when multiple instances have the same status

Timing of alarm evaluation	Status of instance		Generated alarm
	Instance 1 (C drive)	Instance 2 (D drive)	
1st	Measurement value: 10	Measurement value: 20	..#1

Timing of alarm evaluation	Status of instance		Generated alarm
	Instance 1 (C drive)	Instance 2 (D drive)	
1st	Status: Normal	Status: Normal	--#1
2nd	Measurement value: 90 Status: Abnormal	Measurement value: 30 Status: Normal	Alarm:  (abnormal) Alarm message: Disk Busy % (C:) = 90
3rd	Measurement value: 60 Status: Warning	Measurement value: 90 Status: Abnormal	--#2
4th	Measurement value: 20 Status: Normal	Measurement value: 30 Status: Normal	Alarm:  (normal) Alarm message: Disk Busy % (C:) = 20

Legend:

--: Not generated.

#1

A normal alarm is not generated as it is the first time the alarm is evaluated.

#2

An abnormal alarm is not generated because the alarm status has not changed.



In this example, different instances enter the abnormal range the second and third time the alarm is evaluated. However, because the status of the record has not changed between the second and third evaluation, an abnormal alarm is not issued as a result of the third evaluation.


The variable %CVS in a normal alarm stores the measurement value of the instance that caused the last abnormal or warning alarm to be issued. For this reason, the normal alarm generated at the fourth evaluation uses the measurement value of instance 1, which caused the abnormal alarm to be generated at the second evaluation.

### ■ When an alarm of another status is generated after an abnormal or warning alarm

The following table describes an example in which an abnormal or warning alarm is generated, after which another alarm of a different status is generated based on a measurement value of another instance.

Table 6–7: Examples of alarms issued when multiple instances have different statuses

Timing of alarm evaluation	Instance status		Generated alarm
	Instance 1 (C drive)	Instance 2 (D drive)	
1st	Measurement value: 10 Status: Normal	Measurement value: 20 Status: Normal	--#
2nd	Measurement value: 90 Status: Abnormal	Measurement value: 30 Status: Normal	Alarm:  (abnormal) Alarm message: Disk Busy % (C:) = 90
3rd	Measurement value: 40 Status: Normal	Measurement value: 60 Status: Warning	Alarm:  (warning) Alarm message: Disk Busy % (D:) = 60

Timing of alarm evaluation	Instance status		Generated alarm
	Instance 1 (C drive)	Instance 2 (D drive)	
4th	Measurement value: 20 Status: Normal	Measurement value: 30 Status: Normal	Alarm:  (normal) Alarm message: Disk Busy % (D:) = 30

Legend:

--: Not generated.

#

A normal alarm is not generated because it is the first time the alarm is evaluated.

In this example, instance 1 enters the normal range the third time the alarm is evaluated. However, because instance 2 has entered the warning range, a warning alarm is generated.

The variable %CVS in a normal alarm stores the measurement value of the instance that caused the last abnormal or warning alarm to be issued. For this reason, the normal alarm generated at the fourth evaluation uses the measurement value of instance 2, which caused the warning alarm to be generated at the third evaluation.


## (b) Alarms that monitor whether a value exists


The following describes an example of an alarm that monitors whether a value exists. In this example, the alarm monitors PFM - Agent for Platform (Windows). The alarm definition is as follows:

- **Message text:** %CVS
- **Check whether the value exists:** Selected.
- **Activate alarm:** Selected.
- **Notify when the state changed:** Selected.
- **State changes for the alarm:** Selected.
- **Evaluate all data:** Not selected.
- **Evaluate regularly:** Selected.
- **Alarm when damping conditions are satisfied:** Not selected.
- **Record:** Process Detail Interval (PD\_PDI)
- **Field:** Program
- **Value:** process2

The following table describes an example in which this alarm is generated.

Table 6–8: Example of alarms generated when monitoring whether a value exists

Timing of alarm evaluation	Instance status		Generated alarms
	Instance 1	Instance 2	
1st	Measurement value: process1	Measurement value: process2	--#1
2nd	Measurement value: process1	Measurement value: process3	Alarm:  (abnormal)

Timing of alarm evaluation	Instance status		Generated alarms
	Instance 1	Instance 2	
2nd	Measurement value: process1	Measurement value: process3	Alarm message: (N/A)
3rd	Measurement value: process3	Measurement value: process4	--#2
4th	Measurement value: process2	Measurement value: process3	Alarm:  (normal) Alarm message: process2

Legend:

--: Not generated.

#1

A normal alarm is not generated because it is the first time the alarm is evaluated.

#2

An abnormal alarm is not generated because the alarm status has not changed.

In this example, the value `process2` whose existence is being monitored is not found when the alarm is evaluated for the second time, and an abnormal alarm is generated. However, because the value does not exist when the alarm is generated, (N/A) appears for the `%CVS` variable in the message text.

In the fourth evaluation, because the value `process2` is present again, a normal alarm is generated, and the value `process2` appears for the `%CVS` variable.





### (c) Alarms that evaluate all data

The following describes an example of an alarm that evaluates all data. In this example, the alarm monitors PFM - Agent for Platform (Windows). The alarm definition is as follows:

- **Message text:** `Disk Busy % (%CVS1) = %CVS2`
- **Check whether the value exists:** Not selected.
- **Activate alarm:** Selected.
- **Notify when the state changed:** Selected.
- **State changes for the alarm:** Selected.
- **Evaluate all data:** Selected.
- **Evaluate regularly:** Selected.
- **Alarm when damping conditions are satisfied:** Not selected.
- **Record:** Logical Disk Overview (PI\_LOGD)
- **Abnormal:** `ID <> "_Total" AND % Disk Time >= "90.000"`
- **Warning:** `ID <> "_Total" AND % Disk Time >= "50.000"`

The following table describes an example in which this alarm is generated.

Table 6–9: Example of alarms generated when evaluating all data

Timing of alarm evaluation	Instance status		Generated alarms	
	Instance 1 (C drive)	Instance 2 (D drive)	Instance 1 (C drive)	Instance 2 (D drive)
1st	Measurement value: 10 Status: Normal	Measurement value: 20 Status: Normal	--#1	--#1
2nd	Measurement value: 90 Status: Abnormal	Measurement value: 90 Status: Abnormal	Alarm:  (abnormal) Alarm message: Disk Busy % (C:) = 90	Alarm:  (abnormal) Alarm message: Disk Busy % (D:) = 90
3rd	Measurement value: 20 Status: Normal	Measurement value: 90 Status: Abnormal	--#2	--#2
4th	Measurement value: 10 Status: Normal	Measurement value: 20 Status: Normal	Alarm:  (normal) Alarm message: Disk Busy % (C:) = 10	Alarm:  (normal) Alarm message: Disk Busy % (D:) = 20

Legend:

--: Not generated.

#1

A normal alarm is not generated because it is the first time the alarm is evaluated.

#2

An abnormal alarm is not generated because the alarm status has not changed.

When an alarm evaluates all data, an alarm is generated for each instance whose data meets the alarm conditions when the alarm status changes. Therefore, the second time the alarm is evaluated, abnormal alarms are generated for instance 1 and instance 2 which have both entered the abnormal range.

When the measurement values of all instances return to the normal range, a number of normal alarms equivalent to the number of abnormal and warning alarms are issued. In this example, because two abnormal alarms were generated at the second evaluation, two normal alarms are generated at the fourth evaluation. The %CVS variable in the message text of the normal alarms is replaced with the measurement values of instance 1 and instance 2 that caused the abnormal alarms to be generated in the second evaluation.



## 6.4 Setting alarms using the Web browser (Alarms tree)

---

### 6.4.1 Creating an alarm table

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms tree, select the folder of the monitoring agent for which you want to create an alarm table.  
The selected folder is marked with a checkmark.  
You cannot create an alarm table directly under the root node in the Alarms tree. If you have enabled the separate display of alarm trees, the alarm table is created in a subfolder of **User Alarms**. If separate display is disabled, the alarm table is created in a subfolder of the root folder.
4. In the method frame, select the **New Alarm Table**.
5. In the **General Settings** area of the New Alarm Table > Main Information window displayed in the information area, select a product (data model) and enter the alarm table name.  
In this step, you can create a new alarm in the newly created alarm table by setting the basic information such as the alarm name. For details on how to create alarms, see [6.4.2 Creating an alarm \(setting the basic information\)](#).

#### Alarm table name

You can use a maximum of 64 bytes of double-byte characters and single byte alphanumeric characters, spaces, and the following single-byte symbols: % - ( ) \_ . / @ [ ]

For example, in PFM - Agent for Platform (Windows) for the inventory management system, when you want to create an alarm table with the data model version 6.0, you can specify the following settings:

**Product:** Windows (6.0)

**Alarm table name:** Inventory Control System(Win)

Note: Version of the data model to select in **Product**

Select the appropriate data model version corresponding to the agent to which you want to bind the alarm table. If two or more agents of the same type exist and each uses a different data model version, we recommend that you select the earliest data model version.

For details about how to check the data model version of an agent, see [3.4.6 Displaying agent properties](#).

### 6.4.2 Creating an alarm (setting the basic information)

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame, select the folder of the PFM - Agent product to create an alarm table.  
The selected folder is marked with a checkmark.

4. In the navigation frame, select the folder of the PFM - Agent or PFM - RM product for which you want to create an alarm table.

The selected alarm table is marked with a checkmark.

5. In the method frame, select **New Alarm**.

6. In the **General Settings** area of the New Alarm > Main Information window in the information area, set the basic information for the alarm.

#### **Alarm name**

You can use a maximum of 20 bytes of double-byte characters and single byte alphanumeric characters, spaces, and the following single-byte symbols: % - ( ) \_ . / @ [ ]

#### **Alarm Message**

You can use a maximum of 255 bytes of single and double-byte characters. The message can contain a combination of single and double-byte characters. This item can be omitted.

**Product** displays the product (data model) that you have selected in the navigation frame. **Alarm table name** displays the name of the alarm table that you have selected in the navigation frame.

For example, when you want to define an alarm to monitor the busy state of the processor, you can specify the following settings:

**Alarm name:** Usage of CPU

**Alarm message:** CPU is at %CVS% utilization

Reference note:

You can use variables such as %SCT and %HNS for the **Alarm message** setting. For further details on the variables, see the chapter describing the New Alarm > Main Information window or the Edit > Main Information window in the manual *JP1/Performance Management Reference*.

Note 1

If you have selected **Monitor whether the value exists**, the value specified in the conditional expression does not exist when the alarm is reported. In that case, a variable %CVS specified in the Message or the Mail Subject is replaced with an empty string.

Note 2

If the message text contains a multi-byte character that follows %CVS, the text might be corrupted after variable expansion. Make sure that there are no multi-byte characters following the %CVS variable.

7. In the **Advanced settings** area of the New Alarm > Main Information window, set a monitoring time and damping for the alarm.

For example, if the alarm table is defined to monitor the busy state of the processor, and you want to monitor the target 24 hours a day and be notified when the threshold has been exceeded two times over three monitoring intervals, you can specify the following settings:

**Enable alarm:** selected

**Notify when the state changed:** selected

**State changes for the alarm:** selected

**Evaluate all data:** not selected

**Always monitor:** selected

**Report alarm when the following damping condition is reached . :** Selected

2 occurrence(s) during 3 Interval(s)

#### Note 1

If you specify a monitoring time range, the monitoring period ends at the 59th second of the specified end time. For example, if you specify a monitoring time range from 9:00 to 21:00, monitoring starts at 9:00:00 and ends at 21:00:59.

#### Note 2

For details on how alarms are evaluated when a monitoring time range and damping conditions are specified, see [6.9.3 Notes on evaluating alarms](#).

#### 8. Click the **Next >** button.

The available alarm conditions depend on whether **Monitor whether the value exists** has been selected.

- When **Monitor whether the value exists** has been selected:  
You are guided to the New Alarm > Alarm Conditions window. Go to [6.4.3 Setting a value whose existence is to be monitored](#) to set the conditional expression for monitoring to check all of the fields for the value.
- When **Monitor whether the value exists** has not been selected:  
You are directed to the New Alarm > Alarm Conditions window. Go to [6.4.4 Setting the alarm conditions](#) to set the alarm conditions.

### 6.4.3 Setting a value whose existence is to be monitored

#### 1. Set the value whose existence is to be monitored.

For example, if you want to monitor whether a particular process is running for PFM - Agent for Platform (Windows), you can specify the following settings:

**Record:** Process Detail (PD)

**Field:** Program

**Value:** *name-of-the-program-to-be-monitored*<sup>#</sup>

<sup>#</sup> You can specify alphabetical characters (upper-case and lower-case). The system distinguishes between upper and lower-case characters. The specified program name does not need an extension. You cannot monitor programs whose name is a partial match to the specified character string. You can use the wildcard character to monitor programs whose name contains the specified character string. For example, by specifying *\*AAA\**, you can monitor any string that contains the substring *AAA*. To specify a backslash sign (\) immediately in front of a wildcard character in **Value**, you must specify *\\*.

#### 2. Click the **Next >** button.

You are directed to the New Alarm Table > Action window.

#### Note:

The fields of data type *time\_t*, *timeval*, and *utime* are not displayed in a **Field** because they cannot be used in the conditional expressions of the alarm.

### 6.4.4 Setting the alarm conditions

#### 1. Set the alarm conditions.

For example, if you want to monitor the busy state of a processor for the PFM - Agent for Platform (Windows), issue a Warning alarm when the usage of the processor exceeds 80% and issue an Abnormal alarm when it exceeds 90%, you can specify the following settings:

**Record:** System Overview (PI)

**Field:** CPU%

**Condition:** >

**Abnormal value:** 90

**Warning value:** 80

You can search fields for a character string by clicking the **Search Fields** button. For details on searching for fields, see [6.4.4\(1\) Searching for fields](#).

Note

The evaluation of whether an alarm is in an abnormal condition is performed only after Warning conditions are met.

Therefore, you must specify conditions for the Abnormal condition that will also be met for the Warning condition.

## 2. Click the **Add** button.

The conditional expressions are added to both **Abnormal condition** and **Warning condition**.

You can set multiple conditional expressions. Multiple conditional expressions are combined with Boolean AND operators. The alarm is issued only when all of the expressions are met.

Note that when you select a conditional expression already added to **Abnormal condition** or **Warning condition**, and then set an alarm condition, clicking the **Update** button overwrites the selected conditional expression.

Reference note:

When you create an alarm whose conditional expression contains <, <=, >=, or >, specify the conditional expression so that the abnormal condition represents a more abnormal range than the warning condition (that is, the abnormal condition encompasses the warning condition).

Examples are shown below.

Example 1:

When the value of CPU% (CPU usage) is greater than 0 and less than 100

(A larger value is considered more abnormal)

Conditional expression that is evaluated as intended:

Abnormal > 90

Warning > 80

Conditional expression not evaluated as intended:

Abnormal > 50

Warning > 80

Note: If you want to generate an alarm only for abnormal conditions, specify the same value for the abnormal and warning conditions, as follows:

Abnormal > 90

Warning > 90

Example 2:

When the value of % Free Space (free disk space) is greater than 0 and less than 100

(A smaller value is considered more abnormal)

Conditional expression that is evaluated as intended:

Abnormal < 10

Warning < 30

Conditional expression not evaluated as intended:

Abnormal < 60

Warning < 30

Note: If you want an alarm to be generated for abnormal conditions only, specify the same value for the abnormal and warning conditions, as follows:

Abnormal < 10

Warning < 10

You can use alphabetical characters (upper-case and lower-case) when you specify a string for the **Abnormal value** or **Warning value** in the conditional expression. The system distinguishes between upper and lower-case characters. You can also use the wildcard character. For example, by specifying `item name=*AAA*`, you can monitor any string that contains the substring `AAA`. Note that if you want to specify a backslash sign (`\`) just before the wildcard character, you must specify `\\`.

3. Click the **Next >** button.

You are directed to the New Alarm > Action window. Go to [6.4.5 Setting the actions](#).



### Important

If you set alarm conditions consisting of different records (such as field 1 of record A, field 2 of record B, and so on)<sup>#</sup>, the measurement value output function does not work properly when the alarm is restored to a normal state. In addition, the issues described below can arise. For these reasons, we recommend that you consider configuring the intended alarm monitoring by using a single record consisting of multiple fields.

- Alarms do not occur as intended because the collection intervals differ between records A and B.
- Management becomes complex because, for example, multiple records must be checked to identify a value that satisfies an alarm condition.

#

This is not supported when **State changes for each record instance** is selected as an alarm setting.

## (1) Searching for fields

1. Click the **Search fields** button in the New Alarm > Alarm Conditions window.

2. In the New Alarm > Alarm Conditions > Search Fields window, select the target records from the **Records to search** pull-down menu.

The items of the pull-down menu are as follows:

- **--All records--**

Select this option to search for all records.

- A list of record names of the selected agent

A list of record names of the selected agent is displayed in alphabetical order.

3. Enter a character string for the field search into **Keywords to find** and click the **Search** button.

The search results appear in the information frame.

- When **--All records--** is selected as the target record

The search results are listed for each record in the Search results record(s) window.

If you click the menu part of the relevant record, the search results are listed for each field in the New Alarm > Alarm Conditions > Search Fields window.

- When a record name is selected as the target record

The searched fields are listed in the New Alarm > Alarm Conditions > Search Fields window.

4. Select the radio button of the field that you want to select, and then click the **OK** button.

The original New Alarm > Alarm Conditions window appears and the selected fields are included in the **Field** pull-down menu.

## 6.4.5 Setting the actions

Set the actions to be performed by the system when the status of the alarm changes. The possible actions are as follows:

- Send emails
- Execute commands
- Issue JP1 events
- Send an SNMP trap

Notes:

- You cannot select **Warning** if you select **Monitor whether the value exists** in the **General Setting** area of the New Alarm > Main Information window.
- You cannot select **Normal** if you select **Always notify** in the **Advanced settings** area of the New Alarm > Main Information window.
- You can combine multiple actions. However, you cannot combine the actions of executing commands with issuing JP1 events.

### (1) Sending emails

1. In the New Alarm > Action window, select **Email**.
2. Select a trigger for sending an email among **Abnormal**, **Warning**, or **Normal**.
3. Click the **Next >** button.
4. In the **Email settings area**, enter the email address, email body, and other information.

For example, suppose you want to send the email under the following conditions:

- Email address: Send the email to T.Hitachi@Dept01.Hitachi.com
- Action handler: Send the email through the Action Handler service with the host name WebAP
- Email body: Send an email that says "date/time, host name, product name"

In this case, specify the following settings:

**Email address:** T.Hitachi@Dept01.Hitachi.com

**Action handler:** PH1WebAP

**Email body:** Date:%SCT Host:%HNS Product:%PTS



#### Tip

You can search for an action handler by entering a search string in the text box and clicking **Filter**.

Reference note:

You can use variables such as `%SCT` and `%MTS` for the **Email body** setting. For details on variables, see the description of the New Alarm > Action Definition or Edit > Action Definition window in the manual *JP1/Performance Management Reference*.

If you want to specify multiple email addresses for **Email address**, use a comma to separate them. You can enter a maximum of 127 characters for this setting.

5. Click the **Finish** button.

The settings are applied.

## (2) Executing commands

1. In the New Alarm > Action window, select **Command**.

2. Select a trigger for executing the command among **Abnormal**, **Warning**, or **Normal**.

3. Click the **Next >** button.

The **Command Definition** area appears.

Set the command name, command arguments, and so on.

For example, suppose you want to execute the command under the following conditions:

- To execute the `/usr/bin/LogOutput` command that outputs log data
- To execute the command through the Action Handler of the WebAP host
- To pass in the date/time, host name, and message text as the command parameters

In this case, specify the following settings:

**Command name:** `/usr/bin/LogOutput`

**Action handler:** PH1WebAP

**Command arguments:** `Date:%SCT Host:%HNS %MTS`

The following figure shows an example of these settings.

Figure 6–3: Example of settings in the New Alarm > Action Definition window

The screenshot shows a window titled "New Alarm Table > Action Definitions" with "Cancel", "< Back", and "Finish" buttons at the top right. The main area is titled "Command definition" and contains the following fields:

- Command name:** `/usr/bin/LogOutput`
- Action handler:** `PH1WebAP` (selected from a dropdown menu)
- Command arguments:** `Date:%SCT Host:%HNS %MTS`
- Variables:** A list of variables: `Date/Time (%SCT)`, `Agent name (%ANS)`, `Host name (%HNS)`, and `Status (%SCS)`. An "Add Variable" button is next to the list.

At the bottom right of the window, there are "Cancel", "< Back", and "Finish" buttons.

Notes:

- You cannot use the following symbols in a character string that is passed to a command as a parameter:

<>

When these symbols are included in a character string, characters that appear before or after these symbols are sometimes truncated.

- You cannot redirect the standard output of a command to a file or other destination.

Reference note:

You can use some variables such as `%SCT` and `%MTS` in the setting of **Command arguments**. For further details on the variables, see the description of the New Alarm > Action Definition or Edit > Action Definition window in the manual *JP1/Performance Management Reference*.

In addition, the setting of **Command name** can contain an argument. However, if the command path or command name contains a single-byte space character, enclose the command path or command name with double quotations (" ").

4. Click the **Finish** button.  
The settings are applied.

### (3) Issuing a JP1 event

For details on how to issue a JP1 event when an alarm event occurs, see [12.3.2\(3\) Associating alarms with JP1 events and reports](#).

### (4) Sending an SNMP trap when an alarm occurs

1. In the New Alarm > Action window, select **SNMP**.
2. Select a trigger for sending the SNMP trap among **Abnormal**, **Warning**, or **Normal**.
3. Click the **Finish** button.  
The settings are applied.

### (5) Notes on executing actions

#### (a) Program required to send emails

A mail server that conforms to SMTP is required for sending emails. However, you cannot send emails if the SMTP server requires authentication or only accepts Extended SMTP requests.

#### (b) Executable files for executing commands

- In Windows:

To execute commands, you can run files with the following extensions:

- EXE: Executable files
- COM: Executable (command) files
- BAT: Batch files

If you want to execute internal commands such as DEL or DIR, you must make a batch file and execute such commands in the batch file.

Note that you can only specify program files that are accessible from the system account when the commands are executed. You cannot run files that are located in a network folder.

- In UNIX:

To execute commands, you can run the files listed below. Note that these files must have the execute attributes added to them.



- Executable files
- Shell script files

Note that you can only specify program files that are accessible by users with the root user permission when the commands are executed. To run files that are located in an NFS-mounted directory, those files must be made accessible by users with the root user permission on that host.

### (c) Account for command execution

- In Windows:  
You must use the system account for executing commands (for the Action Handler service, as well). Therefore, any resources that are viewed or updated from the program must be accessible from the system account.
- In UNIX:  
You must use an account with the root user permission for executing commands (note that the account for the Action Handler service has the root user permission). Therefore, any resources that are viewed or updated from the program must be accessible from an account with the root user permission.

### (d) The values of the environment variables available when a command is executed

- In Windows:  
The environment variables used when a command is executed are the system environment variables that were in effect when the Performance Management program service started. The profile information is not loaded when a command is executed.
- In UNIX:  
The environment variables used when a command is executed are the environment variables associated with the root user permission when the Performance Management program service started. The profile information is not loaded when a command is executed. For details on *umask*, see [\(f\) umask for the files generated when a command is executed](#) below.

### (e) Current directory during the execution of commands

- In Windows:  
The current folder during the execution of commands is the folder of the Action Handler service (*installation-folder* \bin\action\).  
For logical hosts, the current folder during executing of commands is *environment-directory*\jplpc\bin\action\.
- In UNIX:  
The current directory during the execution of commands is the directory of the Action Handler service (/opt/jplpc/bin/action/).  
For logical hosts, the current directory during executing of commands is *environment-directory*/jplpc/bin/action/.

### (f) umask for the files generated when a command is executed

- In Windows:  
umask is not applicable to the Windows environment.
- In UNIX:  
When a command is executed, umask is set to 000 (the file permissions become 777). When you want to modify umask, you must reset umask in the script file you execute or in the program.

## (g) Other notes on executing commands

- In Windows:
  - You cannot run a Win16-bit application.
  - You cannot run an application that displays a window or a dialog box.  
However, you can execute the `net send` command to display a dialog box. This is because the dialog box is displayed by the Messenger service of Windows, and not by the `net send` command.
  - You cannot run an application that utilizes the Windows messaging mechanism, DDE.
  - You cannot run an application that requires interactive operations.
  - You cannot run a resident program that does not terminate.
  - You cannot run a file with an extension that is associated with an application.
  - You cannot run programs that are located in a network folder.
  - Do not set up a program on a removable disk that is not ready for use.
  - Do not allow services to interact with the desktop in the startup settings of the Windows services.
  - You cannot retrieve information from the standard output or standard error of the executed program.
  - If a command name or a path in a command line contains spaces, you must enclose it in double quotation marks ("").
- In UNIX:
  - You cannot run an application that requires interactive operations.
  - You cannot run a program that involves a `stty`, `tty`, `tset`, or `script` command and requires an interactive operation environment.
  - You cannot run a resident program, which does not terminate.
  - You cannot run a program that does not have the execute attributes added to it.
  - Do not set up a program on a removable disk that is not ready for use.
  - You cannot retrieve the information from the standard output or standard error of the executed program.

## (h) Notes on Action Handler labels

If you set an action for an alarm and select something other than **LOCAL** for **Action handler** in the **Command** field on the New Alarm > Action Definitions window of the PFM - Web Console, the load on PFM - Manager increases. When an alarm triggers an action in a large system, select **LOCAL** for **Action handler** in the **Command** field on the New Alarm > Action Definitions window to prevent the load from centralizing on the PFM - Manager host.

### 6.4.6 Associating a report with an alarm

To display a report when a defined alarm occurs, associate the report with the alarm in the New Alarm > Action window.

Settings prior to setting associated reports

You need to create the desired report in the Reports window prior to setting it up as an associated report. For details on how to create reports, see [5. Creation of Reports for Operation Analysis](#).

1. In the **Report to be displayed** area of the New Alarm > Action window, click the **Browse** button.

2. From the Reports tree in the New Alarm > Action > Select a report window, select a report to associate with the alarm.  
The selected report is marked with a checkmark.  
Only reports that are for the same product and for the same or lesser version of the data model as the alarm you are creating are displayed.
3. Click the **OK** button.  
The report is associated with the alarm.
4. Click the **Finish** button.

For details on how to display a report associated with an alarm, see [5.7.1\(2\) Displaying a report associated with an alarm](#).

## 6.4.7 Copying an alarm table or alarm

### (1) Copying an alarm table

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms tree, select the alarm table that you want to copy.  
The selected report is marked with a checkmark.
4. In the method frame, select **Copy**.
5. In the Copy > Input Name [Alarm Table] window in the information frame, enter the new alarm table name.

#### **New alarm table name**

You can use a maximum of 64 bytes of double-byte characters, single byte alphanumeric characters, spaces, and the following single-byte symbols: % - ( ) \_ . / @ [ ]. Note that you cannot specify an alarm table name that begins with PFM.

6. Click the **OK** button.

When displaying alarms separately in the Alarms tree

The alarm table selected in step 3 is copied into the corresponding alarm folder under **User Alarms**.

When not displaying alarms separately in the Alarms tree

The alarm table selected in step 3 is copied into the same location as the original alarm table.

Supplemental information:

When alarm tables are displayed separately in the alarm tree, the alarm table cannot be copied into any folder other than the appropriate alarm folder under **User Alarms**.

When alarm tables are not displayed separately, the alarm table cannot be copied into a folder different from the folder of the original alarm table.

### (2) Copying an alarm

When you want to add an alarm to the alarm table, you can copy an existing alarm.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms tree, select the alarm you want to copy.  
The selected alarm is marked with a checkmark.
4. In the method frame, select **Copy**.
5. In the Copy > Input Name [Alarm] window in the information frame, enter the new alarm name.

#### **New alarm name**

You can use a maximum of 20 bytes of double-byte characters, single byte alphanumeric characters, spaces, and the following single-byte symbols: % - ( ) \_ . / @ [ ]

6. Click the **OK** button.  
The alarm selected in step 3 is added.  
Supplemental information:  
The alarm can only be copied into the alarm table where the original alarm is.

## **6.4.8 Editing an alarm**

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms tree, select the alarm you want to edit.  
The selected alarm is marked with a checkmark.
4. In the method frame, select **Edit**.
5. In the Edit > Main Information window in the information frame, edit the alarm definition.  
The subsequent steps are similar to those when creating a new alarm. For details on those procedures, see the sections from [6.4.2 Creating an alarm \(setting the basic information\)](#) to [6.4.5 Setting the actions](#).  
Supplemental information:  
When you edit an existing alarm, you cannot modify **Product**, **Alarm table name**, or **Alarm name**.

## **6.4.9 Deleting an alarm table or alarm**

### **(1) Deleting an alarm table**

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.

3. In the navigation frame of the Alarms tree, select the alarm table to be deleted from the folder of the monitoring agent.  
The selected alarm table is marked with a checkmark.
4. In the method frame, select **Delete**.
5. Click the **OK** button in the confirmation dialog box.  
The alarm table selected in step 3 is deleted.

Supplemental information:

You can delete alarm tables even when they are active (bound to the monitoring agent).  
Note that you cannot delete any alarm tables that begin with PFM.

## (2) Deleting an alarm

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms tree, select the alarm you want to delete from the folder of the monitoring agent.  
The selected alarm is marked with a checkmark.
4. In the method frame, select **Delete**.
5. Click the **OK** button in the confirmation dialog box.  
The alarm selected in step 3 is deleted.

Supplemental information:

You can delete alarm tables even when they are active (bound to the monitoring agent). When you delete all of the alarms in an alarm table, the alarm table itself is also deleted.

## 6.4.10 Exporting alarm tables

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the Alarms tree in the navigation frame of the Alarms window, select the items to be exported.  
The report is exported according to the selected target as follows:
  - When a root is selected:  
All folders and alarm tables under the selected root are exported.
  - When a folder is selected:  
The selected folder and alarm tables under it are exported.
  - When an alarm table is selected:  
The selected alarm table is exported.

4. In the method frame, select **Export**.

The operating system displays a confirmation dialog box and a Save As dialog box. Specify the file name and location, and save the file. The selected alarm tables are exported.

Note

- You can export alarm definition files from the PFM - Web Console window in binary format.
- Exported data cannot be imported to PFM - Web Console version 10-00 or earlier.

## 6.4.11 Importing alarm tables

1. Log on to PFM - Web Console from the Web browser of the monitoring console.

2. In the navigation frame of the main window, select the **Alarms** tab.

3. In the method frame of the Alarms window, select the **Import** method.

4. In the Import window, click the **Browse** button beside **Import file name**.

The operating system displays a dialog box in which you can choose a file. Select the definition file of the alarm to be imported. The root, folders, and alarm tables described in the definition file to be selected here are imported. When you select a file, a confirmation message box appears.

5. If you want to replace the definition file of the alarm table, click the **OK** button in the message box.

The alarm tables are imported.

Note:

- If importing an alarm table causes one of the already bound alarm tables to be overwritten, the alarm table is unbound. You must rebind the alarm table, if necessary.
- When you import an alarm table to PFM - Manager which does not support monitoring of operating status for each instance, the alarms in alarm table are imported as alarms for which **State changes for the alarm** is selected.

## 6.4.12 Automatically binding alarms to monitoring agents

You can configure auto alarm table bind by following the procedure described below. This procedure is not necessary if you are manually binding an alarm table (or alarm tables) to monitoring agents.

1. Click **Set Automatic Binding** in the window that is displayed when you are finished setting an alarm table.

2. If the business group function is enabled, you can select the business groups for which you want to set auto alarm bind in the window that is displayed when you are finished setting an alarm table.

3. If you want to set the alarms to be bound to specific business groups, select the **Set a Limit on Business Groups** check box, select the business groups for which you want to set auto alarm bind, and then click the **Execute** button.

4. In the Automatic Bind Settings window, select the alarms to be automatically bound to monitoring agents, and then click the **Next >** button.

If the business group function is enabled, you can select the business groups for which you want to set auto alarm bind.

If you want to set the alarms to be bound to specific business groups, select the **Set a Limit on Business Groups** check box, and then select the business groups for which you want to set auto alarm bind.

5. In the Confirm Changes window, the alarms to be automatically bound to monitoring agents are displayed. If the information displayed in the window is correct, click the **Execute** button.

The auto alarm bind setting is applied.

If the business group function is enabled, the business groups for which to set auto alarm bind are also displayed.

Note:

- When auto alarm bind is to be applied to PFM - RM products, bind alarms to only the remote agents.
- Auto alarm bind is executed according to the auto alarm bind setting only the first time the monitoring manager becomes connected with agents<sup>#</sup>.

#

This refers to the process during which, when the monitoring manager first becomes connected with agents after a system is built, agent information is registered in the monitoring manager.

## 6.5 Setting alarms using the Web browser (Quick Guide)

---

You can use the Quick Guide to create simplified alarm definitions by setting the minimum items.

### 6.5.1 Creating an alarm using Quick Guide

For details on how to create a report, see [5.4 Creating reports in the Web browser \(Quick Guide\)](#).

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents window, select the display format for the Agents tree from the **Display Style** pull-down menu.
  - When **User Agents** is selected:  
The Agents tree that has **User Agents** (*logged-on-user-name*) as the root appears.
  - When **Products** is selected:  
The Agents tree that has **Products** as the root appears.
4. From the **Agents** tree in the navigation frame, select the agent for which you want to create an alarm.  
The selected agent is marked with a checkmark.
5. Choose the **Quick Guide** button in the method frame.
6. In the Quick Guide window, display the fields you want to use to create the alarm.  
You can use one of the following ways to display a field:
  - Click and expand the appropriate record name menu and select fields from the displayed list.
  - Search fields for a specific character string and select fields from the search results.  
You can search fields by entering a search string into **Keyword** and clicking the **Search Fields** button. For details on searching for fields, see [5.4.2 Searching for fields](#).
7. Click an alarm icon that is displayed in the field.
8. In the Quick Guide > Create Alarm window, enter values for **Abnormal condition** and **Warning condition**.
9. If necessary, enter a value for **Alarm table name**, **Alarm name**, and **Alarm message**.  
The default alarm table name, alarm name and alarm message are preset. You can change these items as required.
10. Click the **Finish** button.  
The KAVJJ8554-Q message appears.
11. Choose **Yes** or **No**.  
The alarm will be created. If you choose **Yes**, the created alarm table is bound to the agent selected in step 4. If you choose **No**, the alarm table is not bound to an agent.



## 6.5.2 The default values of an alarm created by using the Quick Guide

Table 6–10: Default values of an alarm created by using the Quick Guide

Item			Default value	Edit
Main Information	General	Product	The earliest version of the data models used by the agent products or agents selected by the user	--
		Alarm table name	The value entered in the Quick Guide > Create Alarm window	Y
		Alarm name	The value entered in the Quick Guide > Create Alarm window	Y
		Alarm message	The value entered in the Quick Guide > Create Alarm window	Y
		Monitor whether the value exists	Off	--#1
	Advanced settings	Enable alarm	On	--
		Notify when the state changed	On	
		State changes for the alarm	On	
		Evaluate all data	Off	
		State changes for each record instance	Off	
		Always notify	Off	
		Evaluate all data	Off	
		Monitoring time range	Always monitor: On	
	Damping	Report alarm when the following damping condition is met: Off		
Alarm Conditions		Record	Records associated with the field selected in the Quick Guide window or the Search results: <i>record-name</i> record window	Y#2
		Field	The field selected in the Quick Guide window or the Search results: List of field(s) found in record <i>record-name</i> window	
		Abnormal condition	The value entered in the Quick Guide > Create Alarm window	Y#3
		Warning condition	The value entered in the Quick Guide > Create Alarm window	
Actions		Actions	All off	--
		Report to be displayed	None	--#4

Legend:

Y: You can edit the setting.

--: You cannot edit the setting.

#1

You cannot create an alarm that monitors whether a value exists.

#2

You cannot edit the settings in the Quick Guide > Create Alarm window. Use the Quick Guide window or the Search results: List of field(s) found in record *record-name* window.

#3

You can only specify one condition for the alarm condition.

#4

You cannot associate a report to be displayed with an alarm. However, you can display a report of an alarm for which a report is not associated.

## 6.6 Operating alarms by using the Web browser

---

### 6.6.1 Changing the association between an alarm table and a monitoring agent

An alarm table is a collection of several alarms. For Performance Management to monitor with alarms, you must associate one or more alarm tables with a monitoring agent. This association is known as *binding*. Canceling a bound alarm table is called *unbinding*. You can bind an alarm table to multiple monitoring agents, or bind one or more alarm tables to a monitoring agent. To bind more than one alarm table to a single monitoring agent, you must enable the functionality for binding multiple alarm tables using PFM - Manager, beforehand. For details on how to set this functionality, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

#### (1) When the functionality for binding multiple alarm tables is enabled

If the functionality for binding multiple alarm tables is enabled, you can both bind and unbind alarm tables in a single window.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents window, select **Products** from the **Display Style** pull-down menu.
4. In the navigation frame, select the monitoring agent to bind to the alarm table.  
The selected agent is marked with a checkmark.  
If you select **Multi select**, you can select multiple agents.



#### Tip

To bind an agent monitored by PFM - RM, select the appropriate remote or group agent as the monitored agent.

5. In the method frame, select the **Alarm Table Bind Settings** method.  
In the information frame, the Alarm Table Bind Settings [Select Alarm Tables] window appears.  
*For binding:*  
Select one or more alarm tables to bind. After you select alarm tables, the selected alarm tables are marked with a checkmark. You can select no more than 50 alarm tables.  
*For unbinding:*  
Clear the selection for the alarm table to unbind it.

Reference note:

You can only bind or unbind alarms on an alarm table basis. Therefore, you cannot bind or unbind individual alarms separately.



#### Tip

You can search for an alarm table by entering a search string in the text box and clicking **Filter**. You cannot use the **Show User Alarms** or **Show Template Alarms** options while a filter is applied.

You cannot apply filter conditions in PFM - Manager version 09-00 or earlier.

6. Click the **OK** button.

The alarm table selected in step 5 is bound to or unbound from the agent selected in step 4.

Reference note:

When an alarm table is bound or unbound, all the alarms bound to the monitoring agent are reset to **Normal Status**. If an alarm table is bound to a monitoring agent that has one or more alarm tables already bound to it, all the alarms in the alarm tables including the existing alarm tables are reset to **Normal**. These alarms are then set to their actual state the next time they are evaluated.

## (2) When the functionality for binding multiple alarm tables is disabled

### (a) Associating an alarm table with a monitoring agent

Note

Each agent can only have one alarm table bound to it. If you bind an alarm table to an agent already bound to another alarm table, the existing alarm table is unbound automatically and the new alarm table is bound.

When the functionality for binding multiple alarm tables is disabled, you can only bind one alarm table to an agent. Alternately, you can use the Quick Guide to set simplified alarms. For details on the Quick Guide, see [6.5 Setting alarms using the Web browser \(Quick Guide\)](#).

To bind an alarm table when the functionality for binding multiple alarm tables is disabled:

1. From the monitoring console Web browser, log on to PFM - Web Console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents window, select **Products** from the **Display Style** pull-down menu.
4. In the navigation frame, select the monitoring agent to bind to the alarm table  
The selected agent is marked with a checkmark.  
If you select **Multi select**, you can select multiple agents.



**Tip**

To bind an agent monitored by PFM - RM, select the appropriate remote or group agent as the monitored agent.

5. In the method frame, select the **Bind Alarm Table**.
6. In the Bind Alarm Table to Agents [Select Alarm Table] window in the information frame, select the alarm table to which to bind the monitoring agent.  
The selected alarm table is marked with a checkmark.  
You cannot select multiple alarm tables.

Reference note:

You can bind alarms only on an alarm table basis. You cannot bind individual alarms separately.



### Tip

You can search for an alarm table by entering a search string in the text box and clicking **Filter**.

You cannot apply filter conditions in PFM - Manager version 09-00 or earlier.

7. Click the **OK** button.

The alarm table selected in step 6 is bound to the agent selected in step 4.

## (b) Unbinding an alarm table bound to a monitoring agent

1. Log on to PFM - Web Console from the Web browser of the monitoring console.

You must log on as a user with administrator user permissions.

2. In the navigation frame of the main window, select the **Agents** tab.

3. In the navigation frame of the Agents window, select **Products** from the **Display Style** pull-down menu.

4. In the navigation frame, select the monitoring agent to unbind the alarm table from.

The selected agent is marked with a checkmark. If you select **Multi select**, you can select multiple agents.



### Tip

To unbind an agent monitored by PFM - RM, select the appropriate remote or group agent as the monitored agent.

5. In the method frame, select the **UnBind Alarm Table**.

6. To unbind the alarm table, click the **OK** button in the confirmation message box.

The alarm table is unbound from the monitoring agent selected in step 4.

## (3) Notes on the limit on the number of alarms and alarm tables

You can create up to 250 alarms in one alarm table. In addition, you can bind up to 50 alarm tables to one agent.

Binding a large number of alarms to PFM - Agent or PFM - RM in the Performance Management system might delay the processing of PFM - Manager, PFM - Agent, or PFM - RM. We recommend that you keep the number of bound alarms within the following limits:

- 250 alarms per agent.
- 20,000 alarms across the entire Performance Management system.

### 6.6.2 Displaying the monitoring agents bound to an alarm table

You can check which monitoring agents are bound to an alarm table.

1. In the navigation frame of the Alarms window, select the alarm table for which you want to display bound monitoring agents.
2. In the method frame, select the **Show Bound Agents** method.

A list of the agents bound to the selected alarm table appears in the information frame.

### 6.6.3 Stopping monitoring with an alarm

You can temporarily stop and then start monitoring with an alarm without unbinding the alarm from the monitoring agent.

If you want to not only stop monitoring but also unbind the alarm definition from the monitoring agent, see [6.6.1\(2\)\(b\) Unbinding an alarm table bound to a monitoring agent](#).

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms window, select the alarm tables to stop monitoring from the monitoring agent folder.  
The selected alarm table is marked with a checkmark.
4. In the method frame, select **Activate**.
5. Change the **Activate** setting in the Activate window.  
Deselect **Activate** for the alarm for which monitoring is to stop.



#### Tip

You can search for an alarm by entering a search string in the text box and clicking **Filter**. By clicking **Select all** or **Unselect all**, you can select or clear the **Activate** check boxes for every alarm table.

6. Click the **OK** button.  
The monitoring with the alarm stops.

### 6.6.4 Starting monitoring with an alarm

You can temporarily stop, and then start monitoring with an alarm without unbinding the alarm from the monitoring agent.

1. Log on to PFM - Web Console from the Web browser of the monitoring console.  
You must log on as a user with administrator user permissions.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms window, select the alarm tables to start monitoring from the folder of the monitoring agent.  
The selected alarm table is marked with a checkmark.
4. In the method frame, select **Activate**.
5. Change the **Activate** setting in the Activate window.  
Check **Activate** for the alarm for which monitoring is to start.

6. Click the **OK** button.

The monitoring with the alarm starts.

## 6.6.5 Checking alarm application status

In the message area of the Agents tree and in the Alarm Application Status window, you can determine if alarm information has been applied to monitoring agents. If no alarm information has been applied, it is possible that the targets are not being monitored correctly. In such a case, re-apply the alarm information from the Alarm Application Status window.

The alarm information discussed here includes the results of alarm-related operations, such as binding and unbinding monitoring agents, updating bound alarm definitions, and updating action definitions. If you have performed these operations, we recommend that you check the alarm application status. For details, see [6.6.5\(1\) Timing of checking alarm application status](#).

You can also use the following commands to check alarm application status and apply alarm information:

- `jpctool alarm unapplied` command (for checking alarm application status)
- `jpctool config alarmsync` command (for re-applying alarm information)

1. Log on to PFM - Web Console from the monitoring console web browser.

You must log on as a user with administrator user permissions.

In a multiple-monitoring configuration, log on to the primary system.

2. In the navigation frame of the main window, select the **Agents** tab.

3. Check if the message `Application of alarm information is not complete` is displayed in the navigation frame of the Agents window.

- If this message is not displayed

Alarm information has been applied. There is no need to proceed to the steps described below.

- If this message is displayed

Wait a while, and then click **Refresh**. If the message is still displayed, perform the steps below.

4. Click the message to display the Alarm Application Status window.

You can also display this window by clicking **Alarm Application Status** in the method frame.

5. If there are services awaiting application of alarm information, wait about five minutes, and then click **Refresh** to see if the message `Services waiting for application do not exist` is displayed.

6. Check the **Application status**, **Incompatible**, and **Inactive** tabs.

The monitoring agent's services to which the results of alarm-related operations have not been applied are displayed. Take the corrective action according to the status of the service as described in the following table.

Table 6–11: Corrective action according to alarm application status (web browser)

Tab	Application status	Description	Corrective action
<b>Application status</b>	Failed	Application of alarm information has failed or the application processing timed out.	Click the <b>Apply to All</b> or <b>Apply</b> button to re-apply alarm information.#

Tab	Application status	Description	Corrective action
<b>Application status</b>	Uncertain	Alarm information application status is unknown.	Take the appropriate corrective action according to the cause of the error. For details, see <i>6.9.4(4) Scenarios where application status becomes Uncertain</i> .
<b>Incompatible</b>	Incompatible	Application of alarm information has failed or the application processing timed out. In addition, the version of the service does not support the application processing on the <b>Application status</b> tab.	Restart the displayed Action Handler service.
<b>Inactive</b>	Inactive	Alarm information cannot be applied because the service is stopped.	Take the corrective action according to the displayed message. If the service's inactivity is not a problem, no action is needed.

#  
If alarm information is being applied to many services at the same time, the monitoring manager's processing speed might become slow. Note that alarm information cannot be applied while the `jpctool config sync` or `jpctool config alarmsync` command is running.

If alarm information is still not being applied after taking these corrective actions, check the following:

- A target service is not running in standalone mode.
- A target service is busy.
- A connection-target PFM - Manager's host name is invalid.
- In a multiple-monitoring environment, the primary and secondary systems are reversed.

7. Re-display the Alarm Application Status window or click **Refresh** to display the most recent alarm application status and verify that no more services are displayed in the window.

## (1) Timing of checking alarm application status

When an alarm-related operation is performed, its results (alarm information) are applied to monitoring agents. If application of alarm information has not been completed, the target might not be being monitored correctly. Therefore, we recommend that you check the alarm application status after you have performed operations.

The following table describes the operations that should trigger checking of alarm application status.

Table 6–12: Timing of checking alarm application status

No.	Classification	Operation
1	Updating binding information	The following operations are performed on monitoring agents: <ul style="list-style-type: none"> <li>• Binding</li> <li>• Unbinding</li> </ul>
2	Updating alarm definitions	The following operations are performed on the alarms contained in bound alarm tables: <ul style="list-style-type: none"> <li>• Addition</li> <li>• Editing</li> <li>• Deletion</li> <li>• Changing active settings</li> </ul>
3	Updating action definitions	LOCAL is specified for the action handler and the following operations are performed: <ul style="list-style-type: none"> <li>• Binding to monitoring agents</li> <li>• Unbinding from monitoring agents</li> </ul>



No.	Classification	Operation
3	Updating action definitions	<ul style="list-style-type: none"> <li>Changing action definitions for the alarms that are contained in bound alarm tables</li> </ul> A remote action is set for the action handler and the following operation is performed: <ul style="list-style-type: none"> <li>Updating of action definitions (including when alarms are not bound to monitoring agents)</li> </ul>
4	Manually applying alarm information	The following operations are performed on a monitoring agent or handler subject to operations described in 1 to 3: <ul style="list-style-type: none"> <li>Executing the <code>jpctool config sync</code> command</li> <li>Executing the <code>jpctool config alarmsync</code> command</li> <li>Applying alarm information in the Alarm Application Status window</li> </ul>
5	Starting a monitoring agent or action handler to which alarms are to be applied	The following operations are performed on a monitoring agent or handler subject to operations described in 1 to 4: <ul style="list-style-type: none"> <li>Starting services</li> <li>Restoring from standalone mode to normal mode</li> </ul>

## 6.6.6 Displaying alarm properties (definitions)

You can check alarm properties from one of the following windows:

- The Alarms window  
Here you can check the properties of all the alarms.
- The Agents window  
Here you can check the properties of the alarms contained in the alarm table bound to an agent.
- The Event Monitor window  
Here you can check the properties of the alarms that have issued alarm events.

Only management users can display alarm properties from the Alarms window.

### (1) Checking from the Alarms window

1. Log on to PFM - Web Console from the Web browser of the monitoring console.
2. In the navigation frame of the main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms window, select the alarm whose properties you want to display in the folder of the monitoring agent.
4. In the method frame, select **Properties**.  
The Properties window appears.  
Click **Main Information**, **Alarm Conditions**, **Action**, and **Action Definitions** on the menu-bar to jump to the corresponding information.

### (2) Checking from the Agents window

1. Log on to PFM - Web Console from the Web browser of the monitoring console.
2. In the navigation frame of the main window, select the **Agents** tab.

3. In the Agents tree in the navigation frame of the Agents window, select the agent whose properties you want to check.
4. In the method frame, select the **Display Alarm Status** method.  
The Display Alarm Status window appears.

### **(3) Checking from the Event Monitor window**

1. Log on to PFM - Web Console from the Web browser of the monitoring console.
2. In the toolbar frame of the main window, select the **Event Monitor** menu.
3. In the Event Monitor window, from the **View** pull-down menu, choose **Alarm Events**.
4. From the list of alarm events, select the icon of the alarm whose properties you want to display.  
The Properties window for the alarm appears in a new window.

## 6.7 Setting alarms by using commands

---

### 6.7.1 Creating an alarm definition file

#### (1) Outputting the template file for the alarm definition file

To create an alarm definition file, first output the template file that includes all of the labels that need to be defined in the alarm definition file.

For example, we will output the template file called `/tmp/alarmtmp01.cfg`.

1. Output the template file.

To output the template file, you can use the `jpctool alarm export` command. Execute the command with the `-template` option, as follows:

```
jpctool alarm export -f /tmp/alarmtmp01.cfg -template
```

The output is shown below.

```
#Alarm Definition File Version=0002
#Alarm Definition File Code=

#[Alarm Data]
#[[General]]
#Product=
#Alarm Table Name=
#Alarm Name=
#Message Text=
#Check Value Exist=N

#[[Advanced Setting]]
#Active Alarm=Y
#Regularly Alarm=Y
#Evaluate All Data=N
#Notify State=Alarm
#Monitoring Regularly=N
#Monitoring Time=
#Damping=N
#Damping Count=

#[[Check Value Exist]]
#Record=
#Field=
#Value=

#[[Alarm Condition Expressions]]
#Condition=

#[[Actions]]
#Report=
#E-mail=Abnormal,Warning,Normal
#Command=Abnormal,Warning,Normal
#SNMP=Abnormal,Warning,Normal
#JP1 Event=N
```

```

#[[Action Definition E-mail]]
#E-mail Address=
#Action Handler=

#[[Message Text]]
#Date: %SCT
#Host: %HNS
#
#Product: %PTS
#Agent: %ANS
#
#Alarm: %AIS (%ATS)
#State: %SCS
#
#Message: %MTS

#[[Action Definition Command]]
#Command Name=
#Action Handler=

#[[Message Text]]
#
#[[Action Definition JP1 Event]]
#Event ID=
#Message=%MTS
#Switch Alarm Level=Y
#Action Handler=
#Exec Logical Host=

```

Note that each line in the template file begins with a sharp (#). Lines that begin with a sharp are comment lines.

For details on the `jpctool alarm export` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

## (2) Creating the alarm definition file

Edit the output template file `/tmp/alarmtmp01.cfg` into an alarm definition file.

1. Open the `/tmp/alarmtmp01.cfg` file with a text editor or other tool.
2. Define the header part of the alarm definition file.

In the header part, define the syntax version of the alarm definition file and the character set to use to write the file. These values are defined in the following portion:

```

#Alarm Definition File Version=0002
#Alarm Definition File Code=
:

```

Delete the sharps (#) at the beginning of these lines, and edit the lines as follows:

```

Alarm Definition File Version=0002
Alarm Definition File Code=C
:

```

- Alarm Definition File Version label  
This is the syntax version of the alarm definition file.

You can specify 0001 or 0002.

You cannot omit this item.

- Alarm Definition File Code label

This is the character code used to create the alarm definition file. You can specify Shift\_JIS, EUC-JP, C, UTF-8, or GB18030.

You cannot omit this item.

### 3. Define the PFM - Agent or PFM - RM type, the version of the data model, the alarm table name, and the alarm name.

The definition of an alarm is coded in the Alarm Data section. For each alarm definition, you must create an Alarm Data section.

Each Alarm Data section consists of different subsections.

The following values are defined in the General subsection.

- PFM - Agent or PFM - RM type
- Version of the data model
- Alarm table name
- Alarm name

These values are defined in the following portion:

```
:
#[Alarm Data]
#[[General]]
#Product=
#Alarm Table Name=
#Alarm Name=
#Message Text=
#Check Value Exist=N
```

In this example, we define the alarm Free Space (hda3) that monitors the free space of the disk /dev/hda3.

Delete the sharps (#) at the beginning of these lines, and edit the lines as follows:

```
[Alarm Data]
[[General]]
Product=U4.0
Alarm Table Name=Disk Monitoring
Alarm Name=Free Space (hda3)
Message Text=Free Space (%CVS%)
Check Value Exist=N
:
```

If the content of Alarm Table Name, Alarm Name, or Message Text includes space(s), you must enclose the item in double quotation marks ("").

For the Alarm Table Name label, you cannot specify a name that begins with PFM.

- Product label

Defines the PFM - Agent or PFM - RM type and the data model version. With this label, both the product ID of PFM - Agent or PFM - RM and the version of the data model are defined.

You cannot omit this item.

- Alarm Table Name label

Defines the alarm table name in 1 to 64 bytes.

You cannot omit this item.

- Alarm Name label

Defines the alarm name in 1 to 20 bytes.

You cannot omit this item.

- Message Text label

Defines (in 0 to 255) bytes the content of the variable `%MTS`, which is used in the message text sent by the email or the JPI event.

An empty string is used by default.

- Check Value Exist label

Defines whether the alarm monitors whether a value exists.

- To define the alarm as monitoring whether a value exists: Y

In this case, you must define the record and the value to be monitored in the Check Value Exist subsection.

Note that you cannot specify Warning for the E-mail, Command, or SNMP label in the Actions subsection.

- To define an ordinary alarm: N

In this case, you must define the alarm conditions in the Alarm Condition Expressions subsection.

N is the default value.

Note: Version of the data model to be specified for the Product label

Select the data model version that corresponds to the agent to which you want to bind the alarm table. If two or more agents of the same type exist and each uses a different data model version, we recommend that you select the earliest data model version.

For details about how to check the data model version of an agent, see [3.4.6 Displaying agent properties](#).

#### 4. Define the conditions for the alarm.

When you create an alarm whose conditional expression contains `<`, `<=`, `>=`, or `>`, specify the conditional expression so that the abnormal condition represents a more abnormal range than the warning condition (that is, the abnormal condition encompasses the warning condition).

Examples are shown below.

Example 1:

When the value of `CPU%` (CPU usage) is greater than 0 and less than 100

(A larger value is considered more abnormal)

Conditional expression that is evaluated as intended:

Abnormal > 90

Warning > 80

Conditional expression not evaluated as intended:

Abnormal > 50

Warning > 80

Note: If you want an alarm to only be generated for abnormal conditions, specify the same value for the abnormal and warning conditions, as follows:

Abnormal > 90

Warning > 90

Example 2:

When the value of `% Free Space` (free disk space) is greater than 0 and less than 100

(A smaller value is considered more abnormal)

Conditional expression that is evaluated as intended:

Abnormal < 10

Warning < 30

Conditional expression not evaluated as intended:

Abnormal < 60

Warning < 30

Note: If you want an alarm to be generated only for abnormal conditions, specify the same value for the abnormal and warning conditions, as follows:

Abnormal < 10

Warning < 10

Note:

The evaluation of whether an alarm is in an abnormal condition is performed only after Warning conditions are met.

Therefore, you must specify conditions for the Abnormal condition that will also be met for the Warning condition.

When defining an ordinary alarm (when you specify `Check Value Exist=N` in the General subsection), define the conditions for the alarm.

You can define the conditions for the alarm in the `Alarm Condition Expressions` subsection.

If you define an ordinary alarm, you cannot omit this subsection.

The conditions for the alarm are defined in the following portion:

```
      :  
# [[Alarm Condition Expressions]]  
#Condition=  
      :
```

For the `Condition` label, code the conditional expressions for the alarm using the record name and the field name to be monitored.

In this example, we will monitor two items, the disk name and the free space, so we need to define two conditional expressions.

- The conditional expression to determine the disk to be monitored  
The disk name is stored in the File System (`FILESYSTEM_NAME`) field of the File System Detail - Local (`PD_FSL`) record. The value of this field is used for the judgment condition.

```
PD_FSL_FILESYSTEM_NAME="/dev/hda3", "/dev/hda3"
```

The left side of the conditional expression specifies the field name of the record to be used for the judgment in the form of the PFM - Manager name.

The right side of the conditional expression specifies the judgment conditions for Abnormal and Warning, separated by a comma.

In this example, we specify the same values to monitor the same disk for both Abnormal and Warning.

- The conditional expression to judge the free space ratio  
The free space is stored in the Mbytes Free % (`TOTAL_MBYTES_FREE_PERCENT`) field of the File System Detail - Local (`PD_FSL`) record. The value of this field is used for the judgment condition.

```
PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20
```

In this example, we will define a free space ratio lower than 10% as Abnormal and one lower than 20% as Warning.

Delete the sharps (#) at the beginning of the appropriate lines, and code these conditional expressions combined with an AND operator in the alarm definition file.

```

:
[[Alarm Condition Expressions]]
Condition=PD_FSL_FILESYSTEM_NAME="/dev/hda3", "/dev/hda3" AND
PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20
:

```

If you specify strings on the right side of the conditional expression (the Abnormal and Warning values), you must enclose them in double quotation marks (").

To specify a hash mark (#) to the right of a conditional expression, you must specify \#.

The right side of a conditional expression must not contain (, ), [, ], <, >, =, or ". To use these characters, use the wildcard character to specify a conditional expression. To specify a backslash sign (\) immediately before the wildcard character to the right of a conditional expression, you must specify \\.

## 5. Define the actions to be taken when the alarm occurs.

You can define the actions to be taken when the alarm occurs in the `Actions` subsection. The actions to be taken when the alarm occurs are defined in the following portion:

```

:
#[Actions]
#Report=
#E-mail=Abnormal,Warning,Normal
#Command=Abnormal,Warning,Normal
#SNMP=Abnormal,Warning,Normal
#JP1 Event=N
:

```

Code the following to have an email sent when the Abnormal alarm status is reached and a JP1 event issued when the Abnormal or Warning status is reached:

```

:
[[Actions]]
#Report=
E-mail=Abnormal
Command=Abnormal,Warning
#SNMP=Abnormal,Warning,Normal
JP1 Event=Y
:

```

- E-mail label

Defines the alarm status that triggers an email to be sent.

- To have emails sent in the Abnormal status: `Abnormal`
- To have emails sent in the Warning status: `Warning`
- To have emails sent in the Normal status: `Normal`

If you want to specify multiple statuses for the action, separate them with commas.

If you specify a status here, you must define the details of the emails in the `Action Definition E-mail` subsection.

You can omit this item.

- Command label

Defines the alarm status for which actions are to be performed, when the action is to issue a JP1 event or to execute a command.

- To perform the action when the status is Abnormal: `Abnormal`
- To perform the action when the status is Warning: `Warning`



- To perform the action when the status is Normal: Normal

If you want to specify multiple statuses for the actions, separate them with commas.

You can omit this item.

- JP1 Event label

Defines whether to issue JP1 events or to execute commands as the actions defined for the Command label.

- To issue JP1 events: Y

In this case, you must define the details for issuing JP1 events in the Action Definition JP1 Event subsection.

- To execute commands: N

In this case, you must define the details for executing commands in the Action Definition Command subsection.

N is the default value.

## 6. Define the destination and message text of the email.

You can define the destination and message text of the email in the Action Definition E-mail subsection.

If you define the action of sending an email, you cannot omit this subsection.

The destination and message text of the email are defined in the following portion:

```
      :
#[[Action Definition E-mail]]
#E-mail Address=
#Action Handler=

#[[Message Text]]
#Date: %SCT
#Host: %HNS
#
#Product: %PTS
#Agent: %ANS
#
#Alarm: %AIS (%ATS)
#State: %SCS
#
#Message: %MTS
      :
```

For the following example, suppose we want to specify the email destination as `operatorA@aaa.com` and the message text with some variables. Delete the sharps (#) at the beginning of the appropriate lines, and edit those lines as follows:

```
      :
[[Action Definition E-mail]]
E-mail Address=operatorA@aaa.com
Action Handler=PH1host01
      :
[[Message Text]]
Date: %SCT
Host: %HNS

Product: %PTS
Agent: %ANS

Alarm: %AIS (%ATS)
```

```
State: %SCS
Message: %MTS
:
```

- **E-mail Address label**

Defines the destination of the email in 1 to 127 bytes of characters. If you want to specify multiple destinations, separate them with commas.

You cannot omit this item.

- **Action Handler label**

Defines the service ID of the Action Handler service to send the email from.

You cannot omit this item.

- **Message Text sub-subsection**

Defines the message text in 0 to 1,000 bytes.

All characters including any linefeeds that appear before the line where the next section or subsection begins, or just before the end of the file, are considered valid text strings. As an exception, any comment lines in this sub-subsection are excluded. Also, the linefeed character in the last line is excluded.

If this value is omitted, an empty string is assumed.

The variables used in the example above are defined as:

- Date and time when the alarm occurred
- Host name of the agent where the alarm occurred
- Agent type and version of the data model
- Name of the agent where the alarm occurred
- Alarm name
- Alarm table name
- Status of the alarm
- Free space (the value defined for the Message Text label in the General subsection)

For details on variables used in the definitions for the Message Text subsection, and their meanings, see the chapter explaining the Alarms window in the manual *JP1/Performance Management Reference*.

## 7. Define the details for issuing the JP1 events.

You can define the details for issuing the JP1 events in the Action Definition JP1 Event subsection.

If you define the actions to issue JP1 events, you cannot omit this subsection.

The details for issuing the JP1 events are defined in the following portion:

```
:
#[[Action Definition JP1 Event]]
#Event ID=
#Message=%MTS
#Switch Alarm Level=Y
#Action Handler=
#Exec Logical Host=
:
```

Delete the sharps (#) at the beginning of the appropriate lines, and edit those lines as follows:

```
:
[[Action Definition JP1 Event]]
Event ID=1234
Message=%MTS
```

```
Switch Alarm Level=Y
Action Handler=PH1host01
#Exec Logical Host=
:
```

- Event ID label

Defines the event ID of the JP1 event in hexadecimal. For a JP1 system event, the information set for this option is identified as an event ID (JPC\_USER\_EVENTID) with an extended JP1 event attribute when output. For a JP1 user event, it is identified as an event ID (JPC\_USER\_EVENTID) with a basic JP1 event attribute when output. For details on the JP1 event types, see *12.2 JP1 events issued from Performance Management to JP1/IM*. You cannot omit this item.

- Message label

Defines the message to send with the JP1 event in 0 to 1,023 bytes. When using version 09-00 or earlier of the Action Handler service to send the JP1 event, define the message in 0 to 128 bytes.

If a label contains a space, you must enclose the value with double quotation marks (").

An empty string is used by default.

- Switch Alarm Level label

Defines whether to convert the alarm level to the severity level.

- To convert the alarm level to the severity level: Y

- To not convert the alarm level to the severity level: N

Y is the default.

- Action Handler label

Defines the service ID of the Action Handler service to issue the JP1 event from.

You cannot omit this item.

## 8. Define the alarm Free Space (hda4) in the same way.

By following steps 3-7, define the alarm Free Space (hda4) that monitors the free space of the disk /dev/hda4.

The completed alarm definition file is shown below:

```
Alarm Definition File Version=0002
Alarm Definition File Code=C

[Alarm Data]
[[General]]
Product=U4.0
Alarm Table Name=Disk Monitoring
Alarm Name=Free Space (hda3)
Message Text=Free Space (%CVS%)
Check Value Exist=N

#[[Advanced Setting]]
#Active Alarm=Y
#Regularly Alarm=Y
#Evaluate All Data=N
#Notify State=Alarm
#Monitoring Regularly=N
#Monitoring Time=
#Damping=N
#Damping Count=
```

```

#[[Check Value Exist]]
#Record=
#Field=
#Value=

[[Alarm Condition Expressions]]
Condition=PD_FSL_FILESYSTEM_NAME="/dev/hda3", "/dev/hda3" AND
PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20

[[Actions]]
#Report=
E-mail=Abnormal
Command=Abnormal,Warning
#SNMP=Abnormal,Warning,Normal
JP1 Event=Y

[[Action Definition E-mail]]
E-mail Address=operatorA@aaa.com
Action Handler=PH1host01

[[[Message Text]]]
Date: %SCT
Host: %HNS

Product: %PTS
Agent: %ANS

Alarm: %AIS (%ATS)
State: %SCS

Message: %MTS

#[[Action Definition Command]]
#Command Name=
#Action Handler=

#[[[Message Text]]]
#
[[Action Definition JP1 Event]]
Event ID=1234
Message=%MTS
Switch Alarm Level=Y
Action Handler=PH1host01
#Exec Logical Host=

[Alarm Data]
[[General]]
Product=U4.0
Alarm Table Name=Disk Monitoring
Alarm Name=Free Space (hda4)
Message Text=Free Space (%CVS%)
Check Value Exist=N

#[[Advanced Setting]]
#Active Alarm=Y
#Regularly Alarm=Y
#Evaluate All Data=N
#Notify State=Alarm

```

```

#Monitoring Regularly=N
#Monitoring Time=
#Damping=N
#Damping Count=

#[[Check Value Exist]]
#Record=
#Field=
#Value=

[[Alarm Condition Expressions]]
Condition=PD_FSL_FILESYSTEM_NAME="/dev/hda4", "/dev/hda4" AND
PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20

[[Actions]]
#Report=
E-mail=Abnormal
Command=Abnormal,Warning
#SNMP=Abnormal,Warning,Normal
JP1 Event=Y

[[Action Definition E-mail]]
E-mail Address=operatorA@aaa.com
Action Handler=PH1host01

[[[Message Text]]]
Date: %SCT
Host: %HNS

Product: %PTS
Agent: %ANS

Alarm: %AIS (%ATS)
State: %SCS

Message: %MTS

#[[Action Definition Command]]
#Command Name=
#Action Handler=

#[[[Message Text]]]
#
[[Action Definition JP1 Event]]
Event ID=1234
Message=%MTS
Switch Alarm Level=Y
Action Handler=PH1host01
#Exec Logical Host=

```

9. When you have finished making the necessary changes, save the `/tmp/alarmtmp01.cfg` file.

For details on the items that are not specified in above example, see the description of the `jpctool alarm import` command in the manual *JP1/Performance Management Reference*.

## 6.7.2 Checking the alarm definition file

You can use the `jpctool alarm check` command to check the alarm definition file.

In the following example, we check not only the syntax of the alarm definition file but also the details of the definition, such as whether PFM - Agent or PFM - RM defined in the file is set up, whether the record and field are supported, and so on.

1. Verify that the Name Server, Master Manager, and View Server services are running.

You can use the `jpctool service list` command to verify that the services of the Performance Management programs are running.

For example, execute the following command when you want to list the services running on the host `host01`:

```
jpctool service list -id "*" -host host01
```

When PFM - Manager is running on the `host01`, the output is as follows:

Host Name	ServiceID	Service Name	PID	Port	Status
host01	PC1host01	Trap Generator	1468	1134	Active
host01	PE1001	Correlator	1420	1114	Active
host01	PH1host01	Action Handler	872	1116	Active
host01	PM1001	Master Manager	1388	1104	Active
host01	PP1host01	View Server	1504	1155	Active
host01	PS1001	Master Store	632	1109	Active
host01	PN1001	Name Server	484	8204	Active

In this example, the Name Server, Master Manager, and View Server services are all running.

For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

2. Execute the `jpctool alarm check` command.

Execute the command as follows:

```
jpctool alarm check -f /tmp/alarmtmp01.cfg
```

If any errors are found in the alarm definition file, an error message is generated for each error, indicating the detail of the error and the line number in the file.

You must check the messages, and then resolve the errors.

For further details on the `jpctool alarm check` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.7.3 Modifying an alarm definition

You can modify an alarm definition by exporting the alarm definition information to a file, editing the file, and then importing the file again.

In this procedure, use the following commands:

- To export the alarm definition:  
`jpctool alarm export command`
- To import the alarm definition:

```
jpctool alarm import command
```

Note:

You cannot modify alarms that are defined in a monitoring template (the alarm tables that begin with PFM). If you want to edit them, you must first export the monitoring template, rename the alarm tables in the alarm definition file, and then import them.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table whose definition you want to edit.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

3. Execute the `jpctool alarm list` command to view the name of the alarm to edit the definition for. For example, execute the following command when you want to view the alarm names defined in the alarm table named `alarmtable1` of the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX -table alarmtable1
```

The output is shown below.

```
Product ID:U
DataModelVersion:4.0
Alarm Table Name:alarmtable1
Alarm Name:
  Kernel CPU 01      [active]
  Kernel CPU 02      [active]
  User CPU 01        [active]

The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

4. Execute the `jpctool alarm export` command. For example, execute the following command when you want to export the definition information for all alarms defined in the alarm table `alarmtable1` of PFM - Agent for Platform (UNIX):

```
jpctool alarm export -f /tmp/alarmtable1.cfg -key UNIX -table alarmtable1
```

For further details on the `jpctool alarm export` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

5. Open the `/tmp/alarmtable1.cfg` file with a text editor or other tool.

6. Edit the `/tmp/alarmtable1.cfg` file.

For details on how to edit individual definitions in the alarm definition file, see [6.7.1 Creating an alarm definition file](#).

7. Save the `/tmp/alarmtable1.cfg` file.

8. Execute the `jpctool alarm import` command.

For example, execute the following command when you want to import the definition information from the alarm definition file `/tmp/alarmtable1.cfg`:

```
jpctool alarm import -f /tmp/alarmtable1.cfg
```

For further details on the `jpctool alarm import` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.7.4 Copying an alarm table

To copy an alarm table, you can use the `jpctool alarm copy` command.

Notes:

- When you make a copy of an alarm table, the copy belongs to the same PFM - Agent or PFM - RM as the original. You cannot make a copy of an alarm table as an alarm table belonging to another PFM - Agent or PFM - RM.
- For the destination alarm table name, you cannot specify a name that begins with PFM.

1. Log on to a host where PFM - Manager is installed.

2. Execute the `jpctool alarm list` command to view the name of the alarm table to copy.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that only the monitoring template is defined.

```
Product ID:U
Alarm Table Name:
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm copy` command.

For example, execute the following command when you want to copy the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) as the alarm table named `alarmtable1`:

```
jpctool alarm copy -key UNIX -table "PFM UNIX Solution Alarms 7.00" -name
alarmtable1
```

For details on the `jpctool alarm copy` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.



4. Execute the `jpctool alarm list` command to make sure that the alarm table has been copied.

Like in step 2, execute the command as follows:

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the alarm table `alarmtable1` is newly created.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.7.5 Deleting an alarm table

To delete an alarm table, you can use the `jpctool alarm delete` command.

1. Log on to the host where PFM - Manager is installed.

2. Execute the `jpctool alarm list` command to view the name of the alarm table to delete.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm delete` command.

For example, execute the following command when you want to delete the alarm table `alarmtable1` of the PFM - Agent for Platform (UNIX):

```
jpctool alarm delete -key UNIX -table alarmtable1
```

For further details on the `jpctool alarm delete` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm table has been deleted.

Like in step 2, execute the command as follows:

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the alarm table `alarmtable1` has been deleted.

```
Product ID:U
Alarm Table Name:
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.7.6 Deleting an alarm

To delete an individual alarm, you can use the `jpctool alarm delete` command.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table containing the definition you want to delete.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm list` command to view the name of the alarm to delete.

For example, execute the following command when you want to view the alarm names defined in the alarm table named `alarmtable1` of the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX -table alarmtable1
```

The output is shown below. In this example, you can see that the alarms `Kernel CPU 01`, `Kernel CPU 02`, and `User CPU 01` are defined in the alarm table `alarmtable1`.

```
Product ID:U
DataModelVersion:4.0
Alarm Table Name:alarmtable1
Alarm Name:
  Kernel CPU 01          [active]
  Kernel CPU 02          [active]
  User CPU 01            [active]
```

```
The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

4. Execute the `jpctool alarm delete` command.

For example, execute the following command when you want to delete the alarm `Kernel CPU 02` in the alarm table `alarmtable1` of the PFM - Agent for Platform (UNIX):

```
jpctool alarm delete -key UNIX -table alarmtable1 -alarm "Kernel CPU 02"
```

For further details on the `jpctool alarm delete` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

5. Execute the `jpctool alarm list` command to make sure that the alarm has been deleted.

Like in step 2, execute the command as follows:

```
jpctool alarm list -key UNIX -table alarmtable1
```

The output is shown below. In this example, you can see that the alarm table `Kernel CPU 02` has been deleted.

```
Product ID:U
DataModelVersion:4.0
Alarm Table Name:alarmtable1
Alarm Name:
  Kernel CPU 01          [active]
  User CPU 01           [active]

The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

## 6.8 Operating alarms by using commands

You can use the Quick Guide to set simplified alarms. For details on the Quick Guide, see [6.5 Setting alarms using the Web browser \(Quick Guide\)](#).

### 6.8.1 Associating an alarm table with a monitoring agent

To bind the alarm table to the monitoring agent, use the `jpctool alarm bind` command.

#### (1) When the functionality for binding multiple alarm tables is enabled

To bind multiple alarm tables when the functionality for binding multiple alarm tables is enabled:

1. Log on to the host where PFM - Manager is installed.

2. Execute the `jpctool alarm list` command to view the name of the alarm table to bind.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can confirm that a monitoring template and UNIX Alarm CPU are defined.

```
Product ID:U
Alarm Table Name:
  UNIX Alarm CPU
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm bind` command.

For example, execute the following command when you want to bind the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) to the agent on `host01`:

```
jpctool alarm bind -key UNIX -table "PFM UNIX Solution Alarms 7.00" -id
UA1host01
```

4. Execute the `jpctool alarm bind` command with the `-add` option specified.

For example, to add UNIX Alarm CPU to an agent on `host01`, execute the following command:

```
jpctool alarm bind -key UNIX -table "UNIX Alarm CPU" -id UA1host01 -add
```

You can bind up to 50 alarm tables at the same time.

For further details on the `jpctool alarm bind` command, see the chapter that describes the commands in the *JPI/Performance Management Reference*.

5. Execute the `jpctool alarm list` command to make sure that the alarm table has been bound.

Specify and execute the command as follows:

```
jpctool alarm list -id UA1host01
```

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 and UNIX Alarm CPU are bound to an agent UA1host01.

```
Service ID:UA1host01
Bound Alarm Table Name:
  UNIX Alarm CPU
  PFM UNIX Solution Alarms 7.00
```

For details of the `jpctool alarm list` command, see the chapter about commands in the *JPI/Performance Management Reference*.

## (2) When the functionality for binding multiple alarm tables is disabled

### Note

Each agent can only have one alarm table bound to it. If you bind an alarm table to an agent already bound to another alarm table, the existing alarm table is unbound automatically and the new alarm table is bound.

To bind an alarm table when the functionality for binding multiple alarm tables is disabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to bind.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that only the monitoring template is defined.

```
Product ID:U
Alarm Table Name:
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For details on the `jpctool alarm list` command, see the chapter that describes the commands in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm list` command to determine which agent the alarm table to bind is bound to. For example, execute the following command when you want to determine which agent the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) is bound to:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to the hosts `hostA` and `hostB`.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time      [active]
  I/O Wait Time          [active]
  Kernel CPU              [active]
  Pagescans               [active]
```

```
Run Queue           [active]
Swap Outs           [active]
User CPU            [active]
```

```
The Bound Agent:
UA1hostA
UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

#### 4. Execute the `jpctool alarm bind` command.

For example, execute the following command when you want to bind the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) to the agent on `host01`:

```
jpctool alarm bind -key UNIX -table "PFM UNIX Solution Alarms 7.00" -id
UA1host01
```

For further details on the `jpctool alarm bind` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

#### 5. Execute the `jpctool alarm list` command to make sure that the alarm table has been bound.

Like in step 3, execute the command as follows:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to the hosts `host01`, `hostA`, and `hostB`.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time   [active]
  I/O Wait Time       [active]
  Kernel CPU          [active]
  Pagescans           [active]
  Run Queue           [active]
  Swap Outs           [active]
  User CPU            [active]

The Bound Agent:
UA1host01
UA1hostA
UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

## 6.8.2 Unbinding an alarm table bound to a monitoring agent

To unbind an alarm table, use the `jpctool alarm unbind` command.

## (1) When the functionality for binding multiple alarm tables is enabled

To unbind an alarm table when the functionality for binding multiple alarm tables is enabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to make sure that the alarm table has been bound.

Specify and execute the command as follows:

```
jpctool alarm list -id UA1host01
```

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 and UNIX Alarm CPU are bound to an agent UA1host01.

```
Service ID:UA1host01
Bound Alarm Table Name:
  UNIX Alarm CPU
  PFM UNIX Solution Alarms 7.00
```

For details of the `jpctool alarm list` command, see the chapter that describes the commands in the *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm unbind` command.

For example, to unbind all the alarm tables bound to the agent UA1host01, execute the following command:

```
jpctool alarm unbind -key UNIX -all -id UA1host01
```

For details of the `jpctool alarm unbind` command, see the chapter that describes the commands in the manual *JPI/Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm table has been unbound.

Like in step 2, execute the command as follows:

```
jpctool alarm list -id UA1host01
```

The output is shown below. In this example, you can confirm that no alarm table is bound to the agent UA1host01.

```
Service ID:UA1host01
Bound Alarm Table Name:
```

For details of the `jpctool alarm list` command, see the chapter that describes the commands in the *JPI/Performance Management Reference*.

## (2) When the functionality for binding multiple alarm tables is disabled

To unbind an alarm table when the functionality for binding multiple alarm tables is disabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to unbind.  
For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that only the monitoring template is defined.

```
Product ID:U
Alarm Table Name:
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

- Execute the `jpctool alarm list` command to determine which agent the alarm table to unbind is bound to. For example, execute the following command when you want to determine which agent the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) is bound to:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to the hosts `host01`, `hostA`, and `hostB`.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time      [active]
  I/O Wait Time          [active]
  Kernel CPU              [active]
  Pagescans               [active]
  Run Queue               [active]
  Swap Outs               [active]
  User CPU                [active]

The Bound Agent:
  UA1host01
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

- Execute the `jpctool alarm unbind` command.

For example, execute the following command when you want to unbind all the hosts whose name begins with `host` in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

```
jpctool alarm unbind -key UNIX -table "PFM UNIX Solution Alarms 7.00" -id
"UA1host*"
```

For further details on the `jpctool alarm unbind` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

- Execute the `jpctool alarm list` command to make sure that the alarm table has been unbound. Like in step 3, execute the command as follows:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to no host.

```
Product ID:U
DataModelVersion:3.0
```



```
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time      [active]
  I/O Wait Time          [active]
  Kernel CPU             [active]
  Pagescans              [active]
  Run Queue              [active]
  Swap Outs              [active]
  User CPU               [active]
```

The Bound Agent:

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

### 6.8.3 Checking the connection between an alarm table and a monitoring agent

To check whether an alarm table is bound, you can use the `jpctool alarm list` command.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table whose binding you want to check.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that only the monitoring template is defined.

```
Product ID:U
Alarm Table Name:
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool alarm list` command to determine which agent the alarm table is bound to.
- For example, execute the following command when you want to determine which agent the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) is bound to:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that the monitoring template is bound to the agents on the host01, hostA, and hostB.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time      [active]
  I/O Wait Time          [active]
  Kernel CPU             [active]
```

```
Pagescans           [active]
Run Queue           [active]
Swap Outs           [active]
User CPU             [active]
```

```
The Bound Agent:
UA1host01
UA1hostA
UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

## 6.8.4 Stopping monitoring with an alarm

You can use the `jpctool alarm inactive` command to disable an alarm.

To disable an alarm:

1. Log on to the host where PFM - Manager is installed.
2. Execute `jpctool alarm list` command to view the name and the status of the alarm to disable.

For example, execute the following command when you want to view the status of each alarm in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. Displays `active` at the right of the alarm name for enabled alarms. In this example, you can see that all the alarms are enabled.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time    [active]
  I/O Wait Time        [active]
  Kernel CPU           [active]
  Pagescans            [active]
  Run Queue            [active]
  Swap Outs            [active]
  User CPU             [active]

The Bound Agent:
UA1hostA
UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

3. Execute the `jpctool alarm inactive` command.

For example, execute the following command when you want to disable the alarm Disk Service Time in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

```
jpctool alarm inactive -key UNIX -table "PFM UNIX Solution Alarms 7.00" -
alarm "Disk Service Time"
```

For further details on the `jpctool alarm inactive` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm has been disabled.

Like in step 2, execute the command as follows:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. Displays `inactive` at the right of the alarm name for disabled alarms. In this example, you can see that the alarm `Disk Service Time` is now disabled.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time    [inactive]
  I/O Wait Time       [active]
  Kernel CPU          [active]
  Pagescans           [active]
  Run Queue           [active]
  Swap Outs           [active]
  User CPU            [active]

The Bound Agent:
  UAlhostA
  UAlhostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.8.5 Starting monitoring with an alarm

You can use the `jpctool alarm active` command to enable an alarm.

To enable an alarm:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name and the status of the alarm to enable.

For example, execute the following command when you want to view the status of each alarm in the monitoring template `PFM UNIX Solution Alarms 7.00` of the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. The output displays `active` at the right of the alarm name for enabled alarms, and `inactive` for disabled alarms. In this example, you can see that the alarm `Disk Service Time` is disabled.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time    [inactive]
  I/O Wait Time       [active]
  Kernel CPU          [active]
  Pagescans           [active]
```

```
Run Queue           [active]
Swap Outs           [active]
User CPU            [active]
```

```
The Bound Agent:
UA1hostA
UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

### 3. Execute the `jpctool alarm active` command.

For example, execute the following command when you want to enable the alarm Disk Service Time in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

```
jpctool alarm active -key UNIX -table "PFM UNIX Solution Alarms 7.00" -
alarm "Disk Service Time"
```

For further details on the `jpctool alarm active` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

### 4. Execute the `jpctool alarm list` command to make sure that the alarm has been enabled.

Like in step 2, execute the command as follows:

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that the alarm Disk Service Time is now enabled.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time   [active]
  I/O Wait Time       [active]
  Kernel CPU          [active]
  Pagescans           [active]
  Run Queue           [active]
  Swap Outs           [active]
  User CPU            [active]

The Bound Agent:
UA1hostA
UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.8.6 Checking the properties of an alarm table

You can display a list of the alarm tables defined for a specific PFM - Agent or PFM - RM, or a list of defined alarms and a list of the agents bound for a specific alarm table.

Note:

You cannot view the definition information of an individual alarm, such as the alarm threshold. To view the definition information of an alarm, you must use `jpctool alarm export` command to export the alarm definition to be checked. For details on how to export alarm definitions, see [6.7.3 Modifying an alarm definition](#).

## (1) Displaying a list of alarm tables

To list the alarm tables defined for a specific PFM - Agent or PFM - RM, you can use the `jpctool alarm list` command.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command.

For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

The following table describes the information displayed by executing the `jpctool alarm list` command with only the `-key` option specified.

**Table 6–13: Information displayed by the `jpctool alarm list` command (-key option specified)**

Order	Information	Description
1	Product ID	The product ID indicating the PFM - Agent or PFM - RM type. For details on the product ID for each PFM - Agent or PFM - RM, see the ID list in an appendix of each PFM - Agent or PFM - RM manual.
2	Alarm Table Name	The alarm table name.

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## (2) Viewing the information for the alarms in an alarm table

To list the alarms defined in and the agents bound to a specific alarm table, you can use the `jpctool alarm list` command.

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command.

For example, execute the following command when you want to view the information for the alarms defined in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

```
jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms 7.00"
```

The output is shown below. In this example, you can see that all the alarms in the monitoring template are enabled, and that the monitoring template is bound to the hosts `hostA` and `hostB`.

```

Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time      [active]
  I/O Wait Time          [active]
  Kernel CPU              [active]
  Pagescans               [active]
  Run Queue               [active]
  Swap Outs               [active]
  User CPU                [active]

The Bound Agent:
  UAhostA
  UAhostB

```

The following table describes the information displayed by executing the `jpctool alarm list` command with the `-key` and `-table` options specified.

**Table 6–14:** Information displayed by the `jpctool alarm list` command (`-key` and `-table` options specified)

Order	Information	Description
1	Product ID	The product ID indicating the PFM - Agent or PFM - RM type. For details on the product ID for each PFM - Agent or PFM - RM, see the ID list in an appendix of each PFM - Agent or PFM - RM manual.
2	Data Model Version	The version of the data model.
3	Alarm Table Name	The alarm table name.
4	Alarm Name	Indicates whether the alarm name is valid and the alarm is enabled. <ul style="list-style-type: none"> <li>• <code>active</code>: the alarm is enabled.</li> <li>• <code>inactive</code>: the alarm is disabled.</li> </ul>
5	The Bound Agent	Indicates the service ID of the agent for the alarm table to be bound to.

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

## 6.9 Notes on alarms

---

This section contains cautionary notes on alarms.

### 6.9.1 Notes on creating alarms

#### (1) Time for evaluating the alarm

If monitoring conditions of multiple records are set for an alarm and the monitoring intervals and offsets of the records are different, the alarm is only evaluated when their collection schedules match. You must review the collection interval setting if necessary.

#### (2) Saving of records to be evaluated in the alarm

You do not have to save the records that you selected for the alarm conditions in the Store database.

#### (3) Limitation on the number of alarms

You can define a maximum of 1,024 alarm tables per Agent product.

You can register up to 250 alarms in one alarm table. In addition, you can bind up to 50 alarm tables to one agent.

Binding a large number of alarms to PFM - Agent or PFM - RM in the Performance Management system, might delay the processing of PFM - Manager, PFM - Agent, or PFM - RM.

We recommend that you keep the number of bound alarms within the following limits:

- 250 alarms per agent.
- 20,000 alarms across the entire Performance Management system.

#### (4) Changing the character set

If you use double-byte characters or Japanese single-byte Katakana characters when you create reports, do not change the character code used by PFM - Manager. If you change from one character code to another, you will no longer be able to use the alarms and reports you defined before the change.

- If you change the character set used by the operating system, uninstall PFM - Manager and then rebuild the environment.

#### (5) When you set an alarm to monitor whether a value exists

If you have selected **Monitor whether the value exists**, the value specified in the conditional expression does not exist when the alarm is reported. For this reason, the variable `%CVS` specified in the Message or the Mail Subject is replaced with (N/A) if the function for measurement value output at alarm recovery is enabled, and an empty string if the feature is disabled.

## (6) How the number of alarm occurrences affects the PFM - Agent or PFM - RM connection

In Performance Management, the PFM - Manager receives the alarms issued by PFM - Agent or PFM - RM, and handles them sequentially, for example, by storing them in the Store database (Master Store). If alarms are issued very frequently, or by several instances of PFM - Agent or PFM - RM at once, there might be delays in alarm processing by PFM - Manager. In such a case, pending alarms accumulate in the memory of the PFM - Manager host, which can decrease the amount of available memory and adversely affect system performance.

We therefore recommend that you consider how frequently an alarm will be issued when you define alarms, making sure that the number of alarms issued does not exceed the number of alarms PFM - Manager can process in a given unit of time. We also recommend that you determine the number of PFM - Agent or PFM - RM instances to be connected to PFM - Manager, beforehand. For details on the relationship between the alarm damping and the number of PFM - Agent or PFM - RM instances to be connected to PFM - Manager, see the sections that describe the system configuration in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

## (7) How the number of alarm occurrences affects the system resources

If a large number of alarms for which an action is specified are issued at the same time, when the actions are executed, the system might become unstable due to a large consumption of system resources. If you want to reduce consumption of system resources due to actions, you can limit the number of command actions (remote actions and local actions) that are simultaneously executed in a single Action Handler service. To do so, change the setting value of the `Action Handler Section` section of the startup information file (`jpccomm.ini`).

For details about the `jpccomm.ini` file, see the part that explains the startup information file (`jpccomm.ini`) in the appendixes of the manual *JPI/Performance Management Reference*.

## (8) Product version for monitoring the operating status for each instances

The product version used to monitor the operating status for each instances is different from the version used for other operating status monitoring. For details about monitoring of operating status for each instance, see the *JPI/Performance Management Planning and Configuration Guide*.

### 6.9.2 Notes on the relationship between alarm damping and the issuing of alarm events



#### Note

The cases in this example assume that a multi-instance record is used to create an alarm. A multi-instance record is a record consisting of multiple instances collected at the same time. For example, assume a multi-instance record that checks the status of disk A and disk B. During alarm evaluation, the status of the disks is evaluated for alarms, and if either (or both) of the disks meets an alarm condition, an alarm is issued for each disk.

- 6.9.2(1)(c) When the alarm damping is  $n/n$  ( $n=n$ ) (Always is cleared and All is selected)
- 6.9.2(1)(d) When the alarm damping is  $n/n$  ( $n=n$ ) (Always is selected and All is selected)
- 6.9.2(2)(c) When the alarm damping is  $n/m$  ( $n<m$ ) (Always is cleared and All is selected)
- 6.9.2(2)(d) When the alarm damping is  $n/m$  ( $n<m$ ) (Always is selected and All is selected)



## (1) When the alarm damping is n/n (n=n)

The relationship between alarm damping and the issuing of alarm events depends on the combination of the **Always notify** and **Evaluate all data** settings in the **Advanced settings** area of the New Alarm > Main information or Edit > Main Information window. The following table lists the section in this manual that describes relationship for each combination of settings.

Evaluate all data	Always notify	
	Cleared	Selected
Cleared	<i>6.9.2(1)(a)</i>	<i>6.9.2(1)(b)</i>
Selected	<i>6.9.2(1)(c)</i>	<i>6.9.2(1)(d)</i>

In the cases described below, the check box names are referred to as follows:

- **Always**: Indicates the **Always notify**.
- **All**: Indicates the **Evaluate all data**.

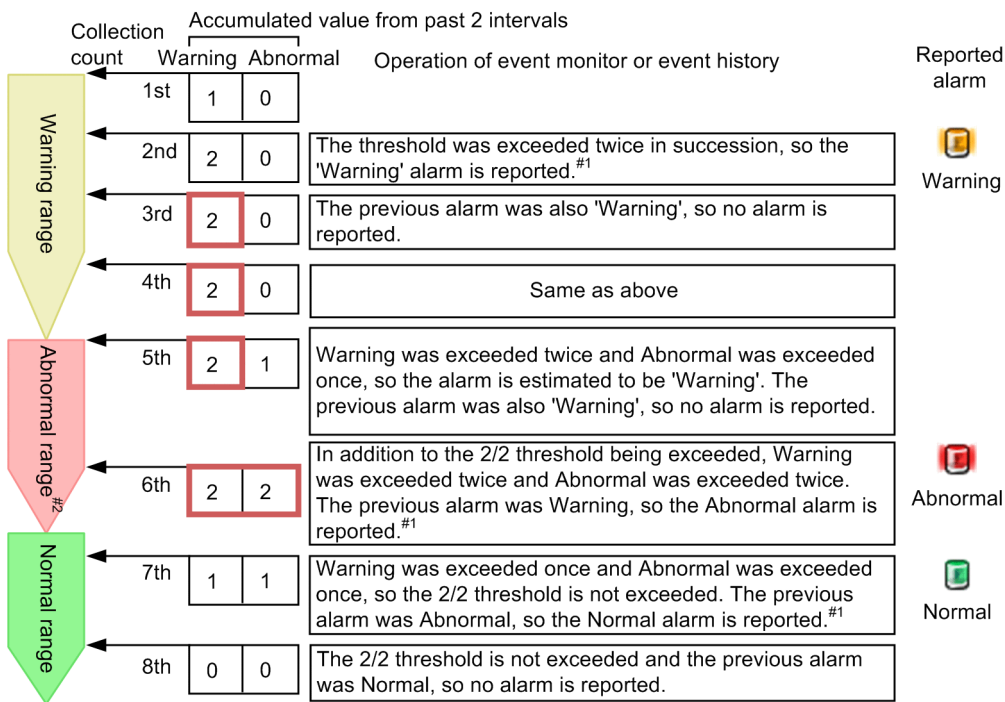
### (a) When the alarm damping is n/n (n=n) (Always is cleared and All is cleared)

If **Always** and **All** are both cleared, the following occurs:

- An alarm is issued when a threshold is exceeded  $n$  times in  $n$  evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- Among the instances that were collected at the time of reporting the alarm, the alarm status of the instance that indicates the highest severity is reported.

This functionality is illustrated by the following examples:

- When damping is 2/2:



Legend:

  : Indicates that the n/n threshold was exceeded.

#1: The Always check box is cleared, so the cumulative value is not reset.

#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

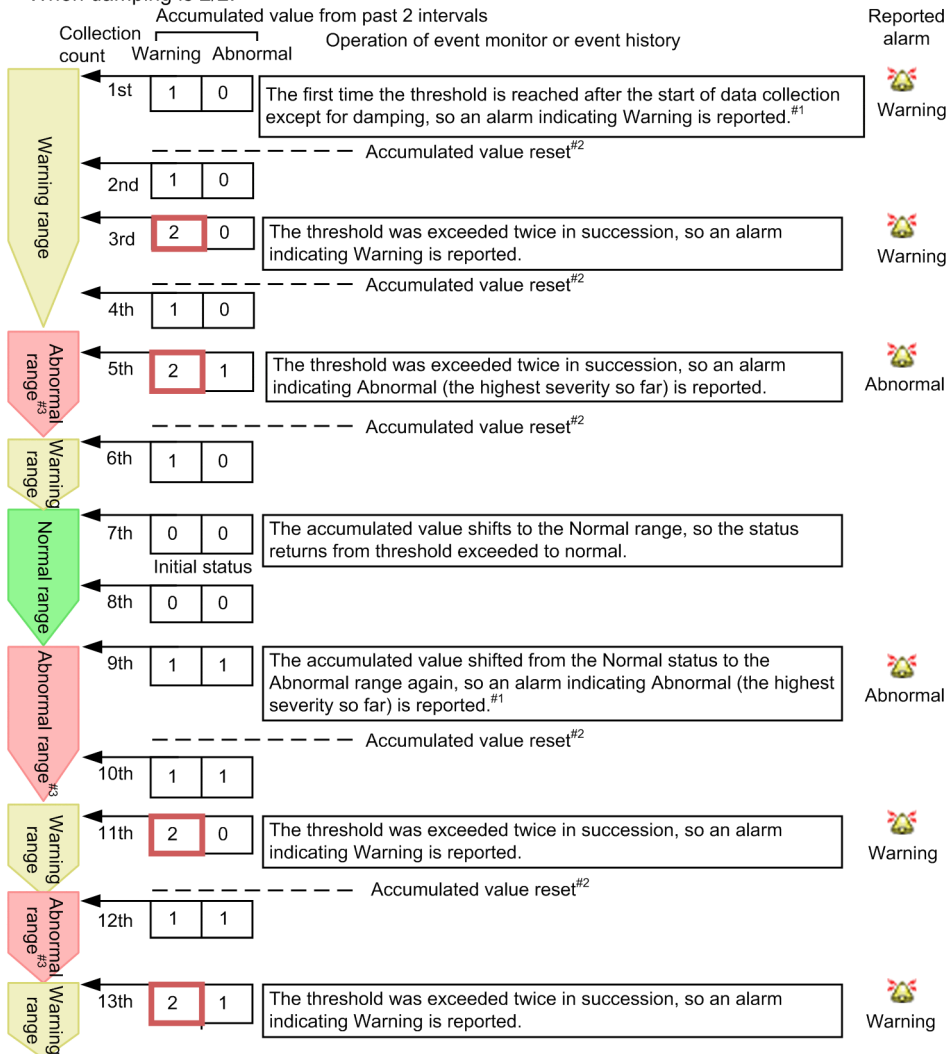
## (b) When the alarm damping is n/n (n=n) (Always is selected and All is cleared)

If **Always** is selected and **All** is cleared, the following occurs:

- An alarm is issued when a threshold is exceeded  $n$  times in  $n$  evaluations. You can use this to control the frequency of the alarm.
- The instance that indicates the highest severity at the time of reporting the alarm is reported.

This functionality is illustrated by the following examples:

- When damping is 2/2:



Legend:   : Indicates that the n/n threshold was exceeded.

#1: If Always is selected and alarm damping is n/n (n = n), an alarm is first issued when the following conditions are met:

- When the first time the threshold is reached after the start of data collection except for damping
- When the accumulated value has shifted from Warning or Abnormal to Normal, and then has again shifted to Warning or Abnormal

#2: The Always check box is selected, so the cumulative value is reset when an alarm is reported.

#3: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

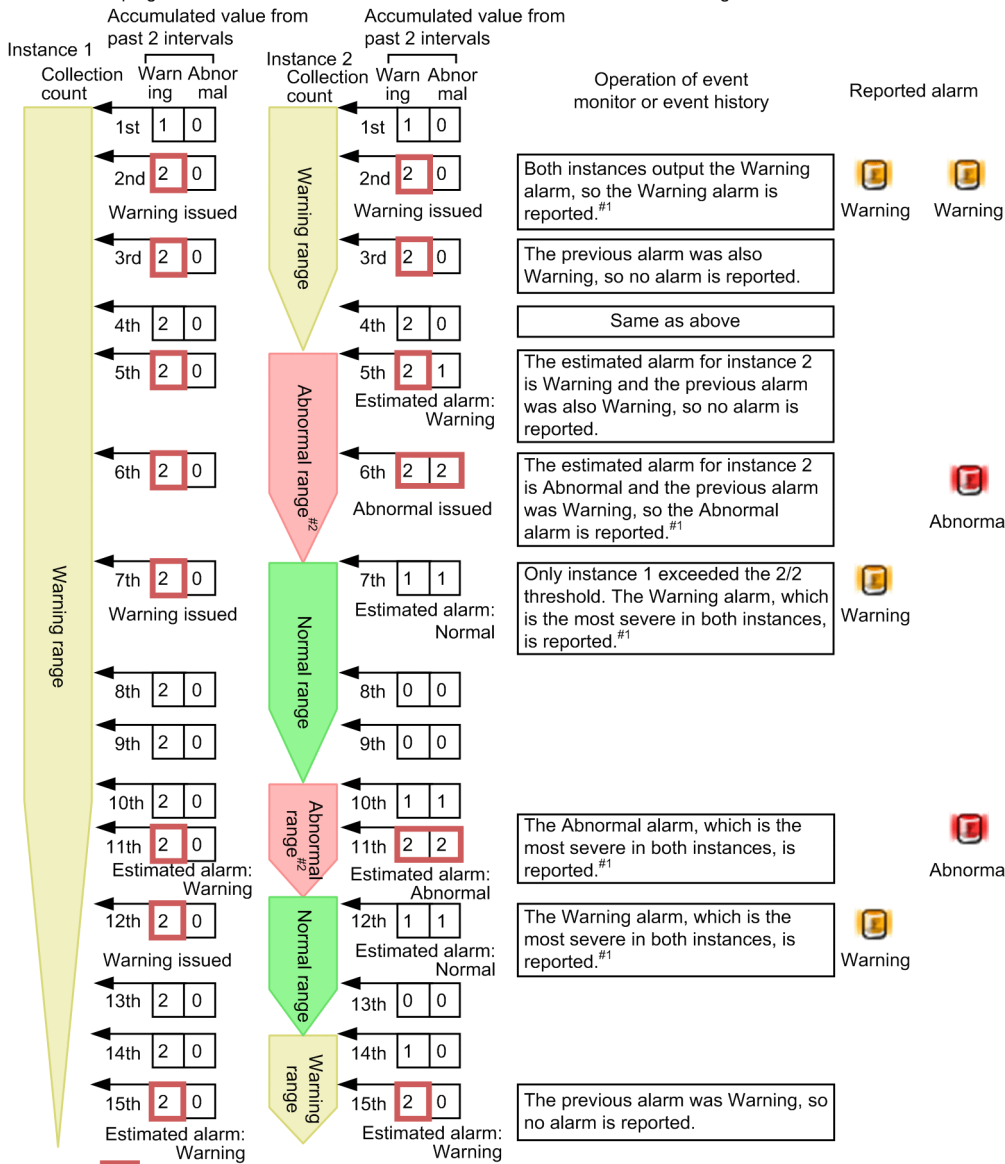
### (c) When the alarm damping is n/n (n=n) (Always is cleared and All is selected)

If **Always** is cleared and **All** is selected, the following occurs:

- An alarm is issued when a threshold is exceeded  $n$  times in  $n$  evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- If the status is Warning or Abnormal, the alarm statuses of all the instances that meet the status condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:

- When damping is 2/2 and there are two records collected at the same time for a single alarm:



Legend:  : Indicates that the n/n threshold was exceeded.

#1: The Always check box is cleared, so the cumulative value is not reset.

#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

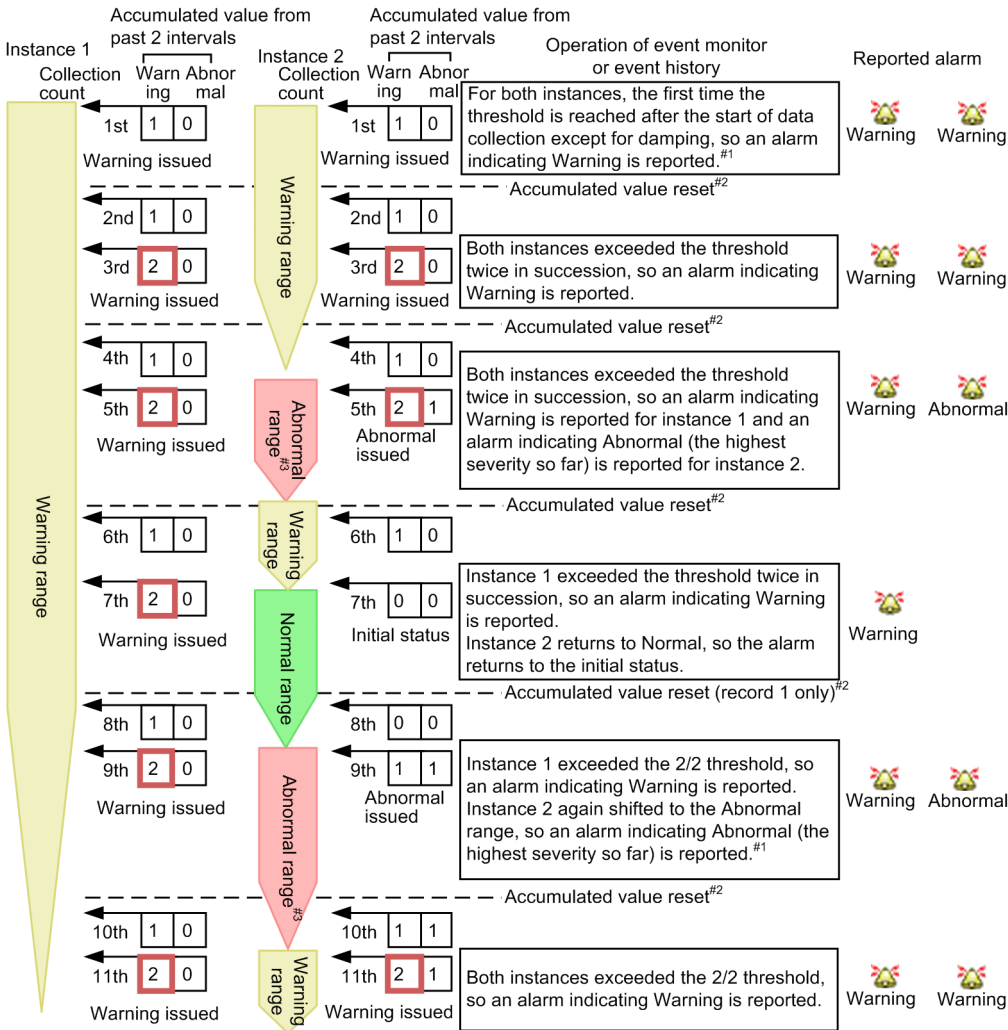
### (d) When the alarm damping is n/n (n=n) (Always is selected and All is selected)

If **Always** and **All** are both selected, the following occurs:

- An alarm is issued when a threshold is exceeded *n* times in *n* evaluations. You can use this to control the frequency of the alarm.
- All of the instances that meet the Warning or Abnormal condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:

- When damping is 2/2 and there are two records collected at the same time for a single alarm:



- Legend:  : Indicates that the n/n threshold was exceeded.
- #1: If Always is selected and alarm damping is n/n (n = n), an initial alarm is issued when the following conditions are met:
    - When the first time the threshold is reached after the start of data collection except for damping
    - When the accumulated value has shifted from Warning or Abnormal to Normal, and then has again shifted to Warning or Abnormal
  - #2: The Always check box is selected, so the cumulative value is reset when an alarm is reported.
  - #3: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

## (2) When the alarm damping is n/m (n<m)

The relationship between alarm damping and the issuing of alarm events depends on the combination of the **Always notify** and **Evaluate all data** settings in the **Advanced settings** area of the New Alarm > Main Information or Edit > Main Information window. The following table lists the section in this manual that describes relationship for each combination of settings.

Evaluate all data	Always notify	
	Cleared	Selected
Cleared	6.9.2(2)(a)	6.9.2(2)(b)
Selected	6.9.2(2)(c)	6.9.2(2)(d)

In the cases described below, the check box names are referred to as follows:

- **Always:** Indicates the **Always notify**.
- **All:** Indicates the **Evaluate all data**.

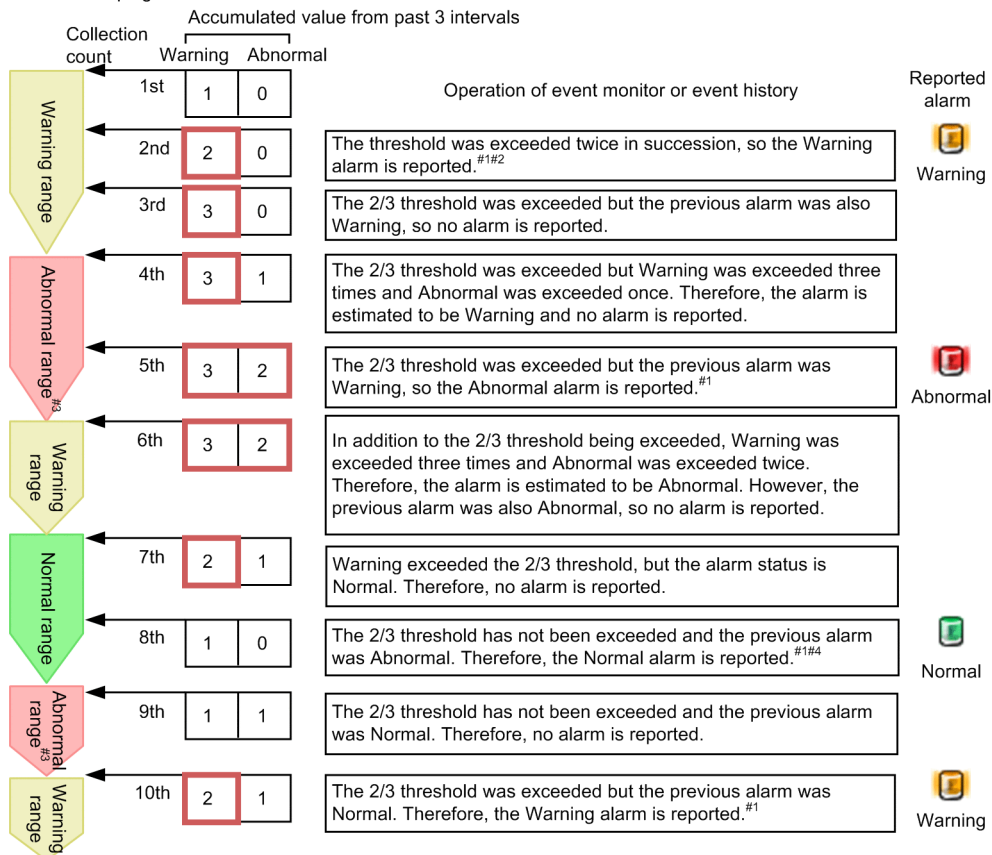
### (a) When the alarm damping is n/m (n<m) (Always is cleared and All is cleared)

If **Always** and **All** are both cleared, the following occurs:

- You can specify whether the alarm status changes when a threshold is exceeded *n* times in *m* evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- Among the instances that were collected at the time of reporting the alarm, the alarm status of the instance that indicates the highest severity is reported.

This functionality is illustrated by the following examples:

- When damping is 2/3:



Legend:  : Indicates that the n/m threshold was exceeded.

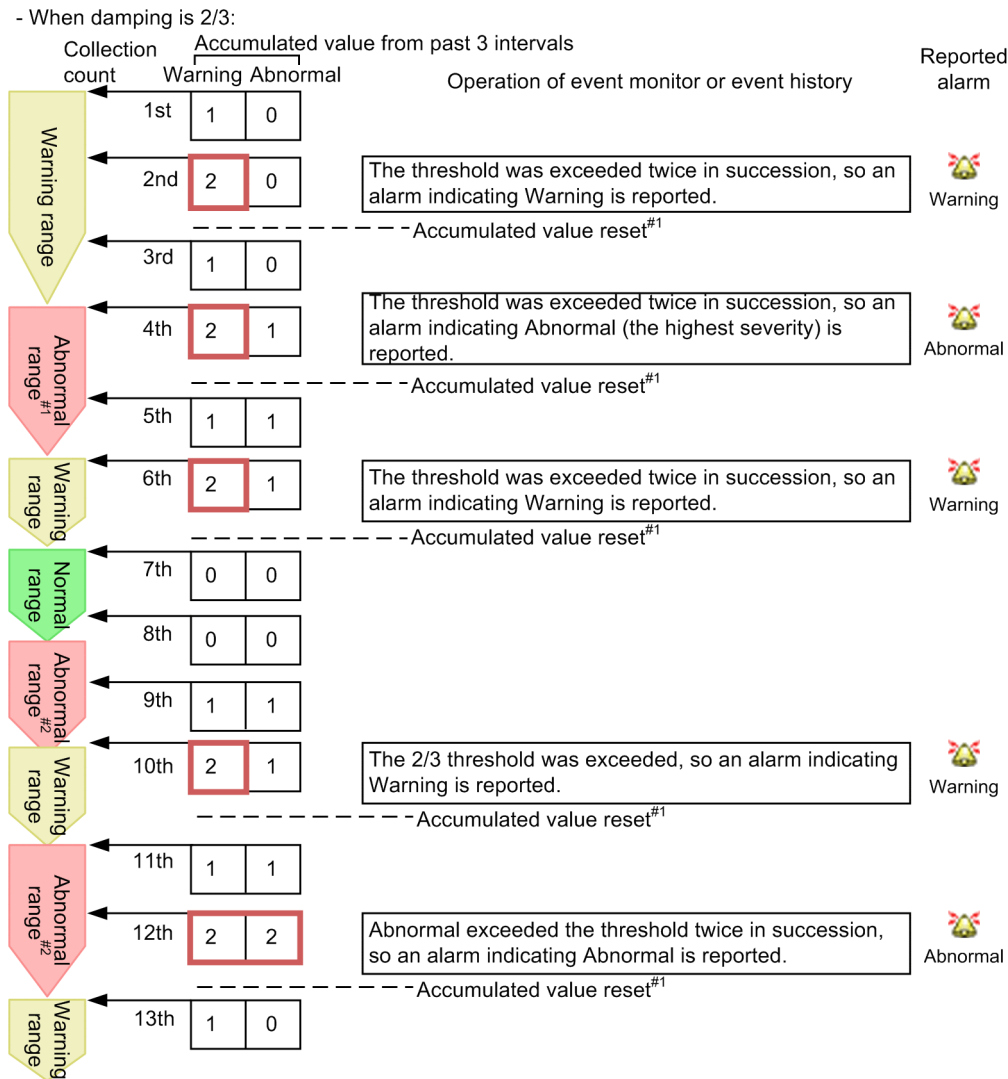
- #1: The Always check box is cleared, so the cumulative value is not reset.
- #2: Although alarm damping is 2/3, the Warning alarm is reported when the threshold is exceeded twice in succession.
- #3: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.
- #4: The following explains patterns of operation of the alarm at the 8th collection that differ from the example given above.
  - When the 8th collection is in the Warning range or Abnormal range:  
In the past three intervals, Warning was exceeded twice and Abnormal was not exceeded (or exceeded once for the Abnormal range). Therefore, Warning exceeds the 2/3 threshold. Furthermore, the previous alarm was Abnormal, so the Warning alarm is reported. Always was not checked, so the accumulated value is not reset.
  - When the 6th collection is in the Abnormal range, the 7th collection is in the Normal range, and the 8th collection is in the Abnormal range:  
In the past three intervals for the 8th collection, Warning was exceeded twice and Abnormal was exceeded twice. Therefore, Abnormal exceeds the 2/3 threshold. However, the previous alarm was Abnormal, so no alarm is reported.

## (b) When the alarm damping is n/m (n<m) (Always is selected and All is cleared)

If **Always** is selected and **All** is cleared, the following occurs:

- You can specify whether an alarm is reported when a threshold is exceeded  $n$  times in  $m$  evaluations. You can use this to control the frequency of the alarm.
- The instance that indicates the highest severity at the time of reporting the alarm is reported.

This functionality is illustrated by the following examples:



Legend:

  : Indicates that the n/m threshold was exceeded.

#1: The Always check box is selected, so the cumulative value is reset when an alarm is reported.

#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

## (c) When the alarm damping is n/m (n<m) (Always is cleared and All is selected)

If **Always** is cleared and **All** is selected, the following occurs:

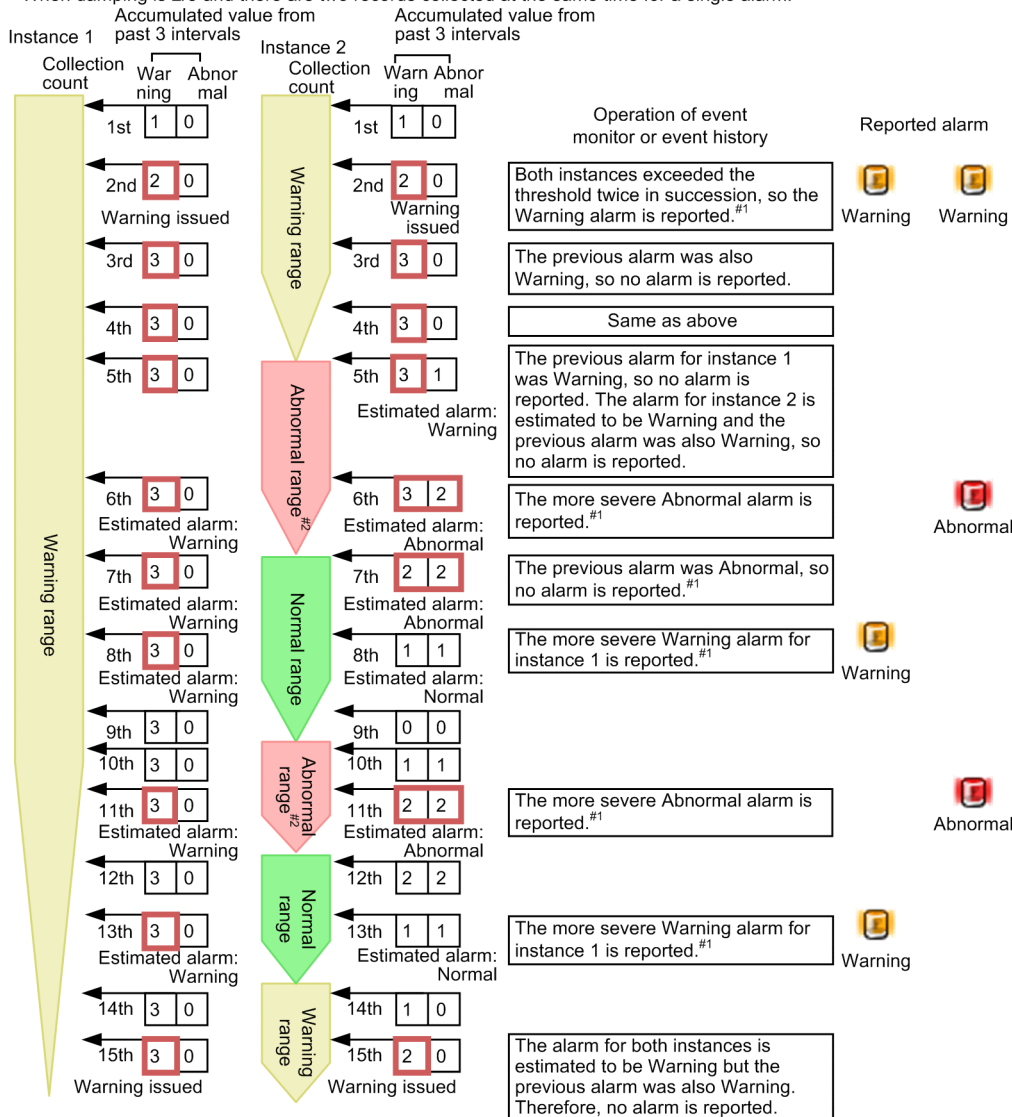
- You can specify whether the alarm status changes when a threshold is exceeded  $n$  times in  $m$  evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.



- If the status is Warning or Abnormal, the alarm statuses of all the instances that meet the status condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:

- When damping is 2/3 and there are two records collected at the same time for a single alarm:



Legend:   : Indicates that the n/m threshold was exceeded.

#1: The Always check box is cleared, so the cumulative value is not reset.  
 #2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

### (d) When the alarm damping is n/m (n<m) (Always is selected and All is selected)

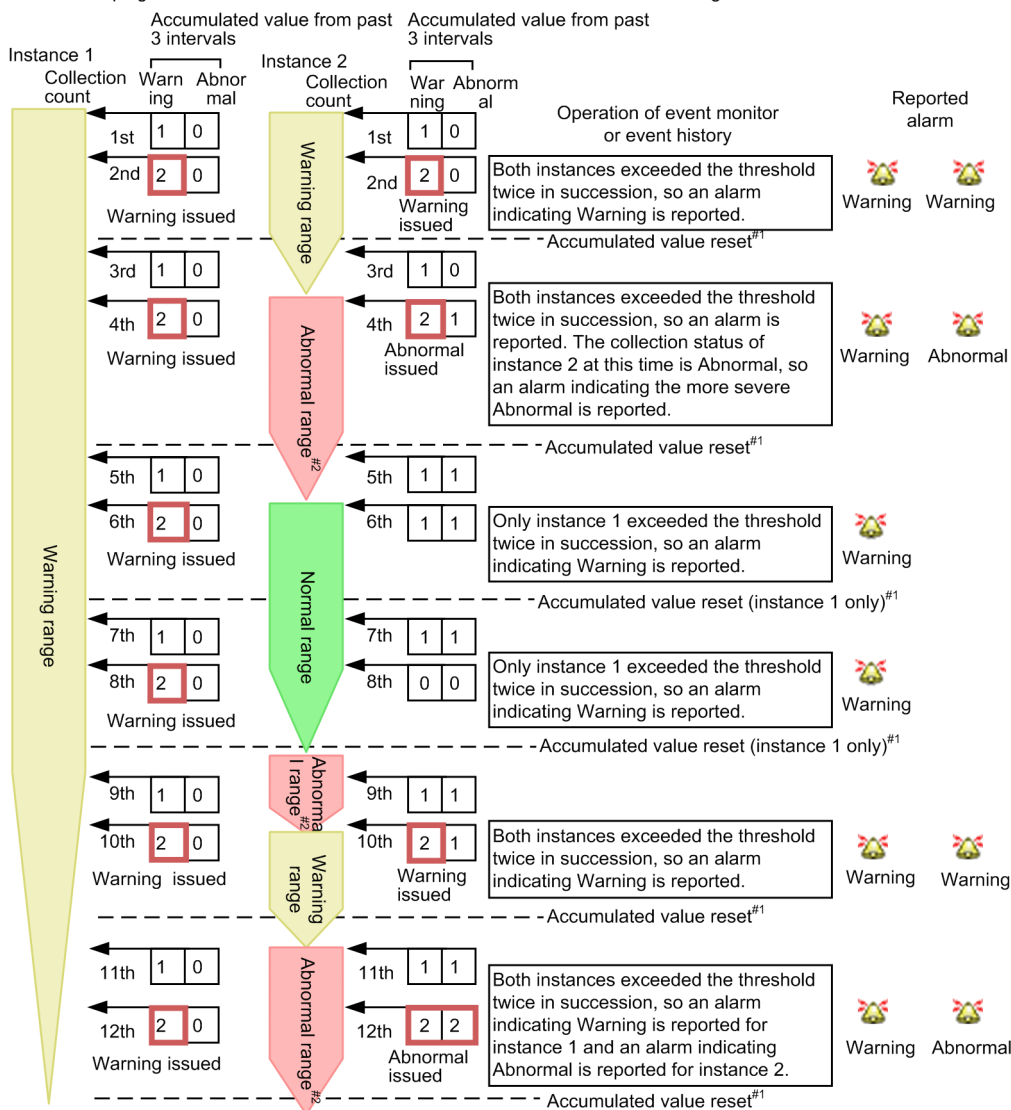
If Always and All are both selected, the following occurs:

- You can specify whether an alarm is reported when a threshold is exceeded *n* times in *m* evaluations. You can use this to control the frequency of the alarm.
- All of the instances that meet the Warning or Abnormal condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:



- When damping is 2/3 and there are two records collected at the same time for a single alarm:



Legend:  : Indicates that the n/m threshold was exceeded.

#1: The Always check box is selected, so the cumulative value is reset when an alarm is reported.

#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

### 6.9.3 Notes on evaluating alarms

This subsection provides cautionary notes on alarm evaluation.

#### (1) Limitation on the number of instances evaluated in an alarm

If multi-instance records are collected in PFM - Agent or PFM - RM, the maximum number of instances handled by a collection is 32,767. When alarms are bound to PFM - Agent or PFM - RM, up to 32,767 instances are evaluated. More than 32,767 instances cannot be evaluated.

## (2) Interval for evaluating the alarm

An alarm is evaluated at fixed intervals. The interval is the record collection interval for each agent. For details on the collection interval of each record, see the appropriate chapters (the Collection Interval value of each record) that describe records of each PFM - Agent or PFM - RM manual.

To modify the record collection interval, perform the following procedure:

1. From the Web browser of the monitoring console, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Services** tab.
3. Select the monitoring agent that the alarm is bound to.
4. In the method frame, select **Properties**.
5. Expand the `Detail Records` or `Interval Records` folder.
6. Change the value of the **Collection Interval** property.
7. The record (performance data) collection interval changes to the value you set.

## (3) Character encoding during alarm evaluation

If you use Japanese or Chinese in an alarm definition, the instance of PFM - Agent or PFM - RM to which the alarm table is bound must use the same character set as PFM - Manager. If the agent or PFM - RM uses a different character set, the following can occur:

- Characters appear garbled in the Event Monitor
- Message displayed when an action is executed appear garbled
- The status of an alarm remains normal in PFM - Web Console despite the alarm definition indicating an abnormal or warning status
- An alarm does not enter normal status in PFM - Web Console despite the alarm definition indicating a return to normal from abnormal or warning status

The character set used by the Performance Management services is determined as follows:

- When started by a command  
The character set specified in the environment where the `jpcspm start` command is executed applies.
- When started automatically at OS startup  
The character encoding set when the OS starts applies.  
In UNIX, if the character set applied at OS startup is not the character set you want to use with Performance Management, enter a character code setting in the service automatic start script (`jpc_start`).

## (4) Evaluating alarms when PFM - Agent or PFM - RM is stopped

When PFM - Agent or PFM - RM is stopped, alarms are evaluated as follows.

- If you stop the PFM - Agent or PFM - RM service while it is in abnormal or warning status, all of the alarms in the alarm tables bound to PFM - Agent or PFM - RM revert to normal status. When PFM - Agent or PFM - RM restarts, the evaluation process begins again from a normal status, not the status at the previous startup.

- If you stop the PFM - Agent or PFM - RM instance to which an alarm table that contains an alarm for which damping is set is bound, the alarm damping measurement is reset.

When the PFM - Agent or PFM - RM restarts, the measurement also restarts.

## 6.9.4 Notes about alarm application status

This subsection provides notes about alarm application status.

### (1) If PFM - Manager version 11-00 or later was installed by overwriting a PFM - Manager version earlier than 11-00

The first time the monitoring manager service is started after the overwrite installation, all application statuses are shown as `Successful` regardless of whether alarm information has been applied.

### (2) If the PFM - Manager services are stopped

If a PFM - Manager service is stopped, the previous application status in effect before the service was stopped is restored the next time the service is started. This is because when a service stops, the applied data is output to a recording file for the alarm application state. When the service is restarted, data is imported from that file.

Note that the previous application status is not restored in the cases listed below. In these cases, execute the `jpctool config sync` command to synchronize the monitoring manager and the monitoring agent to apply the correct alarm information.

- Output of data to the recording file for the alarm application state failed.  
The `KAVE00545-W` message is output to the common message log and the applied data is discarded.
- Data import from the recording file for the alarm application state failed.  
The `KAVE00544-W` message is output to the common message log and the application status is treated as being `Successful`.
- The monitoring manager service terminated abnormally.  
The application status is treated as being `Successful` regardless of whether alarm information has been applied.

### (3) If the recording file for the alarm application state has been deleted when the monitoring manager service starts

If the recording file for the alarm application state has been deleted when the monitoring manager service starts, all service application statuses are shown as being `Successful`. In this case, the `KAVE00544-W` message is output to the common message log.

### (4) Scenarios where application status becomes Uncertain

The application status becomes `Uncertain` in the following cases:

- The environment does not allow the target monitoring agent or service to send responses.  
If the application has not been completed, the `KAVE00348-W` or `KAVE00169-E` message is output to the common message log. If this occurs, take one of the following corrective actions:
  - Execute the `jpctool config alarmsync -target uncertain` command.
  - Apply alarm information from the Alarm Application Status window.

- Restart the service.
- Bind or unbind the alarm table.

If the `KAVE00348-W` or `KAVE00169-E` message has not been issued, no corrective action is needed because alarm information has been applied.

- An attempt to access the monitoring manager's database failed.

The `KAVE00531-E` message is output to the common message log. Take the corrective action provided in that message.

- All alarm tables were unbound from a remote agent or a group agent that does not send responses.

Take one of the following corrective actions:

- Execute the `jpctool config alarmsync -target uncertain` command.
- Restart the remote agent.

## (5) If the service is running but the application status is Inactive

If the service is running but the application status is `Inactive`, check for one of the problems listed below. If either of these problems exists, eliminate the cause of the problem, and then restart the service.

- The firewall pass-through settings are invalid.
- The target service is busy.

## (6) If alarm information has been applied to remote agents or group agents

- If alarm information is applied to a remote agent or a group agent and the source PFM - RM service is stopped, the alarm application status of all remote agents and group agents under that PFM - RM becomes `Inactive`.
- If alarm information is applied to a remote agent or a group agent, the application processing is performed on all remote agents and group agents under the same PFM - RM.

## (7) If failover occurs in a cluster system

When failover occurs in a cluster system, the alarm application status is inherited from the primary system to the secondary system. However, if either of the following occurs during failover processing, the alarm application status is not inherited to the secondary system:

- The Master Manager service terminates abnormally.
- Failover processing is not successful.

In such a case, all services' application status is shown as `Successful`. Execute the `jpctool config sync` command in the primary system environment.

## (8) If the primary and secondary systems were swapped in a multiple-monitoring environment

If the primary and secondary systems were swapped by the `jpccconf primmgr notify` or `jpccconf mgrhost define -shift` command, all services' application status is shown as `Successful`.

# 7

## Displaying Events

This chapter describes how to display events issued by a monitoring agent in the Web browser of the monitoring console.

## 7.1 Displaying the latest events

---

You can view information on the latest events from the Event Monitor window of PFM - Web Console. In this window, you can check the following three types of event information:

- **Agent events**  
Events that indicate changes in an agent's status
- **Alarm events**  
Events that indicate alarms that have been triggered by an agent
- **Health check events**  
Events issued in response to changes in the health check status

In the Event Monitor window, you can monitor the status change of an agent in real time since the display information is periodically updated automatically. You can also display only events that occurred in particular agents by setting the display conditions and color-code the events according to the event status.

You can also check event information using the Summary View displayed in the Agents tree information frame. In this case, only Abnormal and Warning statuses are displayed for the alarm and agent events. It does not show health check events. For details on summary display, see [3.4.5 Using summary display to check the operating status](#).

### 7.1.1 Displaying the latest events information

In the Event Monitor window, events are listed in chronological order.

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. From the menu bar frame of the main window, select the **Event Monitor** menu.
3. From the **View** menu of the Event Monitor window, select the event type you want to display.  
From the following five items, select an event type you want to display in the Event Monitor window:
  - **All events**
  - **Agent events**
  - **Alarm events**
  - **Health check events**
  - **Health check statuses**

The default is **All events**.

Selecting an event type lists the appropriate events. However, when you select **Health check statuses**, only the icon, Agent, Host, and Status are displayed.

For details about the items displayed in the Event Monitor window, see the explanation of the Event Monitor window in the manual *JPI/Performance Management Reference*.

4. Click the **Close** menu on the upper right of the window to close the window.  
The Event Monitor window closes.



Reference note:

If a large number of alarm events or health check events are issued within a short period of time, creating a situation in which more events exist than can be displayed in the Event Monitor window, the operator might not be able to

check every event. In this scenario, the operator can review the status of problematic agents by checking the event history of agents that have generated alerts in the Agents tree.

## 7.1.2 Displaying a report associated with an alarm

If an alarm event is issued within the Performance Management system, the report associated with the alarm can be displayed from the Event Monitor window.

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. From the menu bar frame of the main window, select the **Event Monitor** menu.  
The Event Monitor window appears as a separate window. If a report associated with an alarm exists, the report icon (when Agent for Platform,  or  ) is displayed in the **Report** column.
3. Click the report icon of the event whose report is displayed.  
The View Report window associated with the alarm is displayed in a new window.  
If you want to close the View Report window and the Event Monitor window, click the **Close** button in the upper-right corner of the window.

## 7.1.3 Displaying alarm properties

Clicking the icon for an alarm event (alarm icon) in the Event Monitor window displays the Properties window for the alarm.

In the Properties window, you can view the definition of the alarm corresponding to the alarm event displayed in the Event Monitor window.

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. From the menu bar frame of the main window, select the **Event Monitor** menu.
3. From the **View** menu of the Event Monitor window, select **Alarm Events**.
4. In the list of alarm events, click the icon for the alarm event whose definition you want to view.  
The Alarm Properties window appears as a separate window, so you can confirm the content of the alarm definition. Selecting the following items enables you to jump to the view area for the appropriate settings.

### **Main Information**

Jump to the view area for the main information.

### **Alarm Conditions**

Jump to the view area for the alarm conditions.

### **Actions**

Jump to the view area for the action settings to be executed.

### **Action Definitions**

Jump to the view area for the action definitions.

You can close the Properties window and the Event Monitor window by clicking **Close** in the upper-right corner of each window.

Reference note:

You can also display the Properties window from the Alarms window if your account has administrator user permissions. For details on how to confirm the alarm properties from the Alarms window, see [6.6.6 Displaying alarm properties \(definitions\)](#).

## 7.1.4 Setting the display conditions for the Event Monitor window



You can set the display conditions for the Event Monitor window, including which agents to display in the window and the maximum number of events to display.

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. From the menu bar frame of the main window, select the **Event Monitor** menu.
3. In the Event Monitor window, click the **Show Options** tab.
4. Set the display conditions on the Show Options page of the Event Monitor window.



Set display conditions for the following items, if necessary:

### Filter Settings

If you want to display the events that occurred in all the agents, select **Display all agents**. By default, this is selected.

When you want to display only the specific agents, deselect **Display all agents** and using the move buttons (  /  ), move the agent to be displayed into **Visible agents** and move the agent not to be displayed into **Hidden agents**.

When you, however, deselect **Display all agents**, no event can be displayed unless you specify at least one agent in **Visible agents**.

If access control based on business groups is enabled, you can filter the displayed agents by business group. You can then use the move buttons (  /  ) to move all the displayed agents.

### Color Settings

You can color-code events to be displayed in the Event Monitor window according to their status (normal, warning, or abnormal). By default, **Event color scheme** is **None** (no color-coded).

If you want to color-code the events, from the **Event color scheme** pull-down menu, select the color (**Pastel colors** or **Bright colors**) to be color-coded.

### Event Settings

You can set the maximum number of events (records) to be displayed in the Event Monitor window. When you set it, enter an integer from 1 to 999 in **Maximum number of events to display**. The default is 256.

5. Click the **OK** button.

The settings take effect, and you are returned to the Report page. Events in the Report page are displayed according to the display conditions you set.

Reference note:

The display conditions set in this operation are available during the session. When you log off, the display conditions are not saved and are reset to the initial values.



## 7.2 Displaying the event history

---

The information on the previous events that occurred in the Performance Management system can be checked from the PFM - Web Console Event History window.

One Event History window is displayed per agent. You can display the Event History window by specifying the date range for the data, an alarm name, the maximum number of records, and so on.

### 7.2.1 Displaying the event history

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. In the navigation frame of the Agents window, select the agent whose event history you want to display. When you want to select multiple agents, select **Multi select**. The selected agents are marked with checkmarks.

Reference note:

If you do not select an agent, the histories of events that occurred in all the agents are displayed.

4. In the method frame of the Agents window, select the **Event History** method.
5. In the Event History window, set the items in the **Settings for the report display period** area. Set display conditions for the following items, if necessary:

#### **Date range**

When you set the date range for the data you want to display as an event history, select the appropriate date range from the **Date range** pull-down menu.

The selectable values are as follows:

- **Specify when displayed**
- **Within the past hour**
- **Within the past 24 hours**
- **Within the past 7 days**
- **Within the past month**
- **Within the past year**

The default is **Within the past 24 hours**.

When you select something other than **Specify when displayed**, the dates and times corresponding to the **Start time** and **End time** are automatically set.

#### **Start time and End time**

When you select **Specify when displayed** in **Date range**, set the Start time and End time of the date range for displaying the event.

You should specify the **Start time** and **End time** in a display format corresponding to the locale.

For details, see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

The range of dates and times you can specify is from 1971/01/01 00:00 to 2035/12/31 23:59. For the **End time**, specify a date and time after the **Start time** you specified.

Note that when you select something other than **Specify when displayed**, the appropriate date and time is automatically set. Additionally, if you change the date and time that are automatically displayed, settings for the **Date range** change to **Specify when displayed**.

### **Display the start time data and Display the end time data**

These check boxes determine whether reports include the data for the times specified in **Start time** and **End time**. The check boxes are selected by default. You can specify the default state of the check boxes in the `excludeTerminalData` parameter within the `<vsa>` tag in the initialization file (`config.xml`). For details on how to enter settings in the initialization file (`config.xml`), see the section describing the initialization file in the appendixes of the manual *JPI/Performance Management Reference*.

When either check box is selected, the report includes data that matches the time specified in **Start time** or **End time**.

If a check box is cleared, data that matches the time specified in **Start time** or **End time** is excluded from the report.

### 6. Set the **Maximum number of records**.

Set the display conditions for the following items, if necessary:

#### **Maximum number of records**

The maximum number of events to be displayed as an event history on the Report page, as an integer from 1 to 1440. The default is 1000.

However, you can specify the maximum number of records (`maxFetchCount`) from 1 to 2147483647 in the initialization settings file (`config.xml`) of PFM - Web Console. In this case, you can specify the maximum number of records within the range of values you specified in the `config.xml` file.

### 7. Set the individual items in **Filter**.

Set the display conditions for the following items, if necessary:

#### **Alarm Name**

Specify the alarm names for which to display events, using no more than 2,048 bytes of single or double-byte characters. Specifying an alarm name in this item enables an event at which the alarm occurred to be displayed.

By default, an asterisk (a wildcard character) is used.

#### **Alarm Table**

Specify the names of the alarm tables for which to display events, using no more than 2,048 bytes of single or double-byte characters. Specifying an alarm table name in this item enables you to display events that occurred and that are for alarms of the alarm table.

By default, an asterisk (a wildcard character) is used.

#### **Message**

Specify the message text of events to display, using no more than 2,048 bytes of single or double-byte characters. Specifying message text in this item enables you to display events that output the message text.

By default, an asterisk (a wildcard character) is used.

### 8. Click the **OK** button.

Note:

When displaying events for multiple agents, it might take a long time to search for events, causing the process to time out. If this occurs, reduce the number of selected agents and try again.

The following table describes the display items of the Event History window.

### 9. Click **Close** at the upper right of the Event History window to close the window.

The Event History window closes.

Supplemental information:

- If no displayable event exists, a message indicating this is displayed.
- The display conditions set in this operation are available only while the Event History window is being displayed, and the settings are not saved.

Reference note:

If the number of records exceeds the maximum number of records, the records from the oldest one to the maximum number of records are displayed.

## 7.3 Outputting the event history

---

### 7.3.1 Outputting the event history in CSV format

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. From the navigation frame in the Agents window, select an agent whose data you want to output in the CSV format.  
If you want to select multiple agents, select **Multi select**.  
Each selected agent is marked with a checkmark.  
Reference note:  
If you do not select an agent, the histories of events that occurred in all the agents are displayed.
4. In the method frame of the Agents window, select the **Event History** method.
5. In the menu bar of the Event History window, click **Export**.
6. In the Save As dialog box, specify a name and location for the file and then click **Save**.  
The event history data is output to a file.

### 7.3.2 Outputting the event history in HTML format

1. From the monitoring console Web browser, log on to PFM - Web Console.
2. In the navigation frame of the main window, select the **Agents** tab.
3. From the navigation frame in the Agents window, select an agent whose data you want to output in the HTML format.  
If you want to select multiple agents, select **Multi select**.  
Each selected agent is marked with a checkmark.  
Reference note:  
If you do not select an agent, the histories of events that occurred in all the agents are displayed.
4. In the method frame of the Agents window, select the **Event History** method.
5. In the menu bar of the Event History window, click **Print**.  
The Print window opens in a new window, displaying the event history data in a format suitable for printing or saving to disk.
6. Print or save the report using your Web browser.  
When saving the report, use the option that saves the complete web page.

# 8

## Suspending and Resuming Monitoring

This chapter describes how to suspend and resume monitoring. Additionally, this chapter describes operation monitoring statuses when monitoring is suspended.

## 8.1 Overview of the monitoring suspension function

You can use Performance Management to suspend or resume monitoring of operations such as alarms and health checks for monitoring targets for which maintenance work is performed while the monitoring targets are running. The functions to suspend and resume monitoring are collectively called the *monitoring suspension function*.

When a monitored host or service is stopped by maintenance work during operation, an alarm event or health check event that indicates an abnormal or warning situation occurs in normal monitoring. At this time, you can suspend monitoring for the monitoring target to be stopped in advance to prevent the stopping of the host or service from being reported as an abnormal situation. Additionally, you can select whether or not to store operating information from when monitoring is suspended, allowing you to analyze the operation status by using data that excludes the corresponding duration of suspension.

Suspending and resuming monitoring can be set in the Monitoring Suspension Settings window in the Agents tree or by using a command. You can select targets by host or agent and specify the monitoring suspension settings for them by using one operation.

Major functions related to the monitoring suspension function are described below:

- Alarm  
Alarms bound to an agent for which monitoring is to be suspended are suspended.
- Health check  
Health checks for a host and agent for which monitoring is to be suspended are suspended.
- Storage of operating information  
Storage of operating information is suspended. Note that you can set storage of operating information to be continued when you specify the monitoring suspension settings.

You can check the monitoring suspension duration in the Event Monitor window or Event History window.

Note that, even if storage of operating information is suspended, real-time reports can be displayed.

### 8.1.1 Prerequisites for the monitoring suspension function

Prerequisite programs and versions for using the monitoring suspension function are as follows:

Table 8–1: Prerequisite program version

Host	Product name	Supporting version
PFM - Manager host	PFM - Manager	10-50 or later
	PFM - Agent	10-00 or later
	PFM - RM	10-00 or later
PFM - Web Console host	PFM - Web Console	10-50 or later
PFM - Agent host or PFM - RM host	PFM - Base	10-50 or later
	PFM - Agent	10-00 or later
	PFM - RM	10-00 or later

The suspension setting can be specified for monitoring agents that do not satisfy the above prerequisite version condition and the monitoring agents are displayed as suspended. However, monitoring performed by the monitoring agents is not actually suspended.

Additionally, if you want to use the monitoring suspension function, you need to enable the monitoring suspension function option in PFM - Manager.

For details about the monitoring suspension function option, see [8.3.1 Monitoring suspension function option](#).

## 8.1.2 Alarms while monitoring is suspended

While monitoring is suspended, alarm evaluation in the suspended monitoring agent is suspended and no alarm event is issued. The alarm status at this time is Suspended.

### (1) Alarm evaluation after monitoring is resumed

Alarm evaluation is determined based on the results of alarm evaluations up to the previous alarm evaluation. After monitoring is resumed, alarm evaluation is performed based on the results of alarm evaluations before monitoring is suspended because there is no record of alarm evaluation while monitoring is suspended.

If Damping is specified in an alarm definition, the integrated values of damping (the Abnormal count and the Warning count) before monitoring is suspended are inherited.

## 8.1.3 Health check while monitoring is suspended

While monitoring is suspended, health check for the suspended host and agent is suspended and no health check event is issued. The health check status at this time is Suspended.

### Note

- If there is a host or agent for which monitoring is suspended in the system, the monitoring level of the health check agent cannot be changed.  
To change the monitoring level, you need to resume all monitoring and change the monitoring level of the health check agent, and then suspend monitoring again.
- Even if the health check function is disabled, monitoring can be suspended. When you change the health check function from disabled to enabled, the health check status of the suspended host and agent is Suspended.

### (1) When suspension or resumption of monitoring is reflected on the health check status

Suspension or resumption of monitoring is reflected on the health check status when polling of the health check function is performed. Note that, if you resume monitoring, the health check status prior to when monitoring was suspended is inherited until polling is performed.

For details about polling of the health check function, see [16.2.4 Notes on the health check function](#).

## (2) Health check records while monitoring is suspended

Health check records related to monitoring suspension are as follows:

### Health Check Detail (PD\_HC)

If you suspend monitoring by the host, the information of all the agents on the specified host is not stored. If you suspend monitoring by the agent, the information of the specified agent is not stored.

### Host Availability (PI\_HAVL)

If you suspend monitoring by the host, the information of the specified host is not stored.

### Host Detail (PD\_HOST) record

The number of agents for which monitoring is suspended is stored for each host.

Note that, if you suspend monitoring by the host, the information of the specified host is not stored.

### System Overview (PI\_SYS) record

The information of monitoring suspension in the system is stored as a summary of operation status.

For details about health check records, see the section that explains health check in the appendixes of the *JPI/Performance Management Planning and Configuration Guide*.

## 8.1.4 Operating information while monitoring is suspended

When you suspend monitoring, you can select whether to store operating information. If you specify the settings so that operating information is not stored, information for the duration of monitoring suspension is not reflected on historical reports.

Note that, even if you specify the settings so that operating information is not stored, information collection from the monitoring target might not be stopped depending on the processing method or settings of the monitoring agent. Therefore, a history of accesses to the monitoring target or error messages when collection fails might be output to a log.

## 8.1.5 Monitoring suspension function and system linkage

This subsection describes cases of using the monitoring suspension function in various environments.

### (1) When using the monitoring suspension function in a multiple-monitoring environment

Only the primary manager can suspend or resume monitoring. Therefore, the settings that were specified on the primary manager need to be applied to the secondary manager. Enable the automatic synchronization options of the settings information for the monitoring suspension function in the startup information file (`jpccomm.ini`) to set the settings to be synchronized automatically.

For details about the automatic synchronization options of the settings information for the monitoring suspension function, see [8.3.2 Automatic synchronization options of the settings information for the monitoring suspension function \(for multiple-monitoring\)](#).



## **(2) When using the monitoring suspension function in an environment with linkage with JP1/IM**

For hosts or agents for which monitoring is suspended, only JP1 events related to monitoring suspension or resumption are issued. Targets for which JP1 events are not issued differ depending on the unit by which to suspend monitoring as follows.

When monitoring is suspended by the host

- JP1 events related to all the agents on the host are not issued.
- If you specify a host on which PFM - RM has been installed, JP1 events related to the remote agent are also not issued.
- If you specify a host on which PFM - Manager has been installed, JP1 events related to the services (Name Server, Master Manager, Master Store, Correlator, Trap Generator, and View Server) of PFM - Manager are issued.

When monitoring is suspended by the agent

- JP1 events related to the specified agent are not issued.
- If you specify PFM - RM, JP1 events related to the remote agent are also not issued.

Note that, if you suspend monitoring while a PFM service is stopped, a JP1 event might be issued when the service starts. Likewise, if you resume monitoring while a PFM service is stopped, a JP1 event might not be issued when the service starts.

## **(3) When using the monitoring suspension function in an environment with linkage with JP1/SLM**

If you specify the settings so that operating information is not stored while monitoring is suspended, the operating information of the suspended agent is not sent to JP1/SLM. Note that, if there is operating information that failed to be sent before monitoring was suspended, the operating information is retransmitted.

After monitoring is resumed, operating information for which delta values are sent is calculated based on the values before monitoring is suspended. Note that, a record with settings in which real-time reports are displayed in temporary log mode is calculated based on the values collected for real-time reports.

For details about operating information that is sent to JP1/SLM, see [13.2.5 Recording performance data collected when linked with JP1/SLM](#).

## 8.2 Range of suspending or resuming monitoring

---

Set the monitoring suspension function with the unit (host or agent) specified according to the range of suspending monitoring. Note that, when you resume monitoring, make sure that you specify the same unit as the unit by which monitoring was suspended.

### 8.2.1 Range of monitoring suspended or resumed by the host

If you suspend monitoring by the host, monitoring that has been performed by monitoring agents on the specified host is suspended.

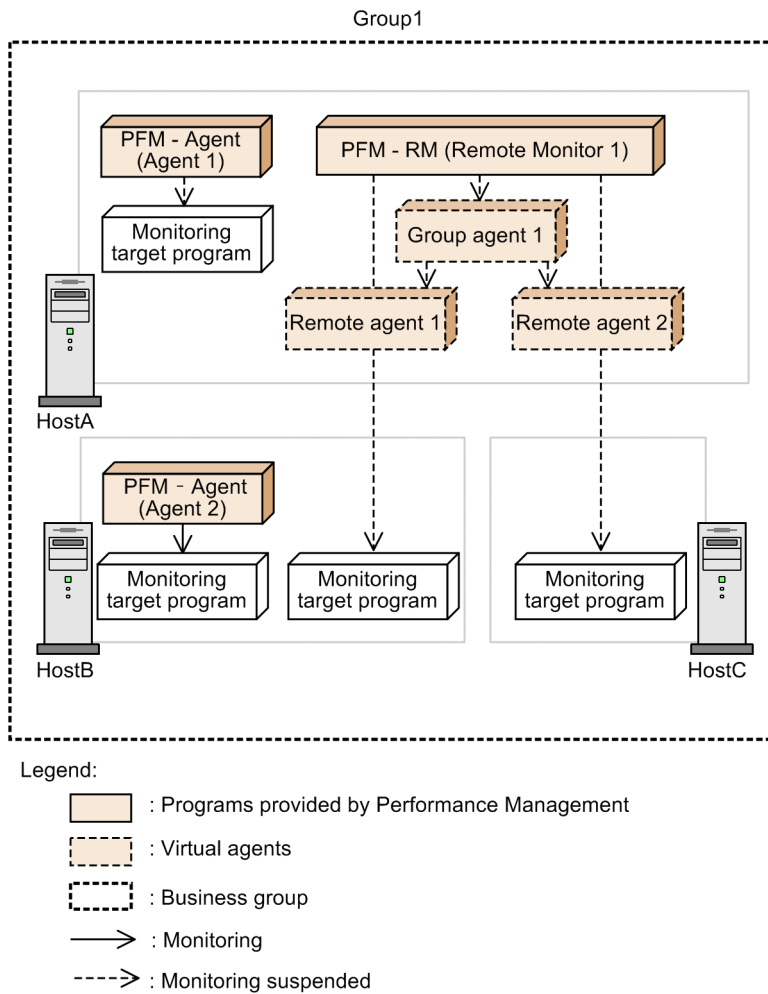
If you specify a host on which PFM - RM has been installed, monitoring that has been performed by the remote agent is also suspended. Note that, if you specify the monitored host of the remote agent, monitoring for the monitoring-source Remote Monitor is not suspended.

When the monitoring level of the health check provides host-level monitoring of operating statuses, monitoring for health checks for the specified host is also suspended.

Additionally, when you resume monitoring by the host, the same range as that when you suspended monitoring is resumed.

The range of suspended monitoring when HostA is specified is explained by using the following environment as an example.

Figure 8–1: Example of an environment in which monitoring is suspended by the host



At this time, suspended monitoring is as follows:

- Alarm evaluation and storage of operating information  
Alarm evaluation and storage of operating information are suspended in Agent 1, Remote Monitor 1, Group agent 1, Remote agent 1, and Remote agent 2.
- When the monitoring level of the health check provides host-level monitoring of operating statuses  
Health checks for HostA are suspended.
- When the monitoring level of the health check provides service-level monitoring of operating statuses  
Health checks for Agent 1, Remote Monitor 1, Remote agent 1, and Remote agent 2 are suspended.

## 8.2.2 Range of monitoring suspended or resumed by the agent

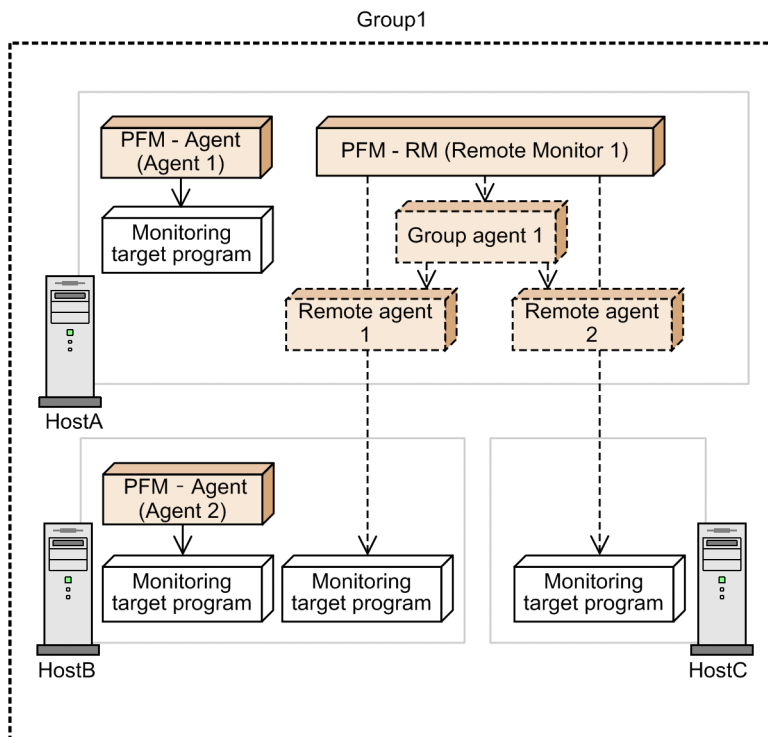
If you suspend monitoring by the agent, monitoring that has been performed by the specified monitoring agents is suspended.

If you specify PFM - RM, monitoring that has been performed by the remote agent is also suspended. Note that, if you specify only the remote agent, monitoring for the monitoring-source Remote Monitor is not suspended.

Additionally, when you resume monitoring by the agent, the same range as that when you suspend monitoring is resumed.

The range of suspended monitoring when Remote Monitor 1 on HostA is specified is explained by using the following environment as an example.

Figure 8–2: Example of an environment in which monitoring is suspended by the agent



Legend:

- : Programs provided by Performance Management
- : Virtual agents
- : Business group
- : Monitoring
- : Monitoring suspended

At this time, suspended monitoring is as follows:

- Alarm evaluation and storage of operating information  
Alarm evaluation and storage of operating information are suspended in Remote Monitor 1, Group agent 1, Remote agent 1, and Remote agent 2.
- When the monitoring level of the health check provides service-level monitoring of operating statuses  
Health checks for Remote Monitor 1, Remote agent 1, and Remote agent 2 are suspended.

## 8.3 Setting the monitoring suspension function

---

To use the monitoring suspension function, you need to enable the monitoring suspension function option in the startup information file (`jpccomm.ini`) in advance.

Additionally, when you suspend or resume monitoring in a multiple-monitoring environment, you need to enable the automatic synchronization options of the settings information for the monitoring suspension function in advance. Doing this allows the settings information for the monitoring suspension function to be automatically synchronized between the primary and secondary systems.

You can suspend or resume monitoring in the Monitoring Suspension Settings window in the Agents tree or by using the `jpctool monitor` command.

For details about the command, see the chapter that explains commands in the manual *JPI/Performance Management Reference*.

### 8.3.1 Monitoring suspension function option

When the value of `Monitoring Suspend Mode` in the `Common Section` section of the startup information file (`jpccomm.ini`) of PFM - Manager is 1, the monitoring suspension function option is enabled. This option is set to be enabled by default.

For details about how to change the `jpccomm.ini` file, see the section that explains the startup information file (`jpccomm.ini`) in the appendixes of the manual *JPI/Performance Management Reference*.

### 8.3.2 Automatic synchronization options of the settings information for the monitoring suspension function (for multiple-monitoring)

The automatic synchronization options of the settings information for the monitoring suspension function are disabled at initial installation. To enable the options, change the value of `Auto Sync for Suspend Setting` to 1 in the `Common Section` section of the startup information file (`jpccomm.ini`) of PFM - Manager on the primary and secondary managers.

For details about how to change the `jpccomm.ini` file, see the part that explains the startup information file (`jpccomm.ini`) in the appendixes of the manual *JPI/Performance Management Reference*.

Note that, you need to satisfy the following conditions in PFM - Manager on the primary and secondary managers to achieve automatic synchronization.

- The automatic synchronization options of the settings information for the monitoring suspension function are enabled.
- PFM - Manager is running.
- The Master Manager service is fixed to the same port number.
- The setting values (the values specified in the `Monitoring Level` property in the `Health Check Configurations` folder of health check agents) of monitoring level of the health check function are the same.

If automatic synchronization failed because the conditions were not satisfied or due to other reasons, a KAVE00517-W message is output to a common message log of PFM - Manager on the primary manager. In this case, you need to duplicate definition information. For details, see [11.5 Duplicating definition information](#).

### Important

In a multiple-monitoring environment, the monitoring suspension function does not operate correctly if the settings information is not identical between the primary and secondary managers.

## 8.3.3 Suspending monitoring from a Web browser

You can suspend monitoring in the Monitoring Suspension Settings window in the Agents tree.

### Prerequisite conditions

- The monitoring suspension function is enabled in the startup information file (`jpccomm.ini`) on the connection-target PFM - Manager host.
- The login is performed by administrator user permission.

### Operation

1. In the navigation frame of the Main window, select the **Agents tree** tab.
2. Select a folder or agent containing a host or agent for which you want to suspend monitoring in the navigation frame. You can also select multiple folders or agents or select them by the business group. A check mark is displayed at the selected folder or agent.
3. In the method frame, select the **Monitoring Suspension Settings** method.
4. Click the **Change Settings** button in the Monitoring Suspension Settings window.
5. Select the **Suspend monitoring** radio button in the section in which to select the processing type for the setup in the Monitoring Suspension Settings > Change Settings window. Choose the processing unit for the setup and the targets to setup and then click the **Next** button.  
If you want to store operating information while monitoring is suspended, select **Continue recording performance data to StoreDB**.
6. In the Monitoring Suspension Settings > Check Changes window, confirm that the contents of **Monitoring status** and **Settings** are what you expect.
7. Click the **Execute** button.
8. A message indicating that the updating of the settings information is completed is displayed in the Monitoring Suspension Settings > Check Results window. Click the **OK** button.  
Monitoring for the target host or agent is suspended based on the settings information.
9. If you enable the automatic synchronization options of the settings information for the monitoring suspension function in a multiple-monitoring environment, confirm that automatic synchronization succeeds.  
Log in to PFM - Web Console on the secondary manager and confirm that the specified settings are applied. If the specified settings are not applied, duplicate the definition information. For details, see [11.5 Duplicating definition information](#).

## 8.3.4 Resuming monitoring from a Web browser

You can resume monitoring in the Monitoring Suspension Settings window in the Agents tree.

### Prerequisite conditions

- The monitoring suspension function is enabled in the startup information file (`jpccomm.ini`) on the connection-target PFM - Manager host.
- The login is performed by administrator user permission.

### Operation

1. In the navigation frame of the Main window, select the **Agents tree** tab.
2. Select a folder or agent containing a host or agent for which you want to resume monitoring in the navigation frame. You can also select multiple folders or agents or select them by the business group. A check mark is displayed at the selected folder or agent.
3. In the method frame, select the **Monitoring Suspension Settings** method.
4. Check the unit by which monitoring was suspended in the Monitoring Suspension Settings window. If you do not know the unit by which monitoring was suspended, see an icon in the **Monitoring suspension** column of **Settings**.



#### Note

When you resume monitoring, make sure that you specify the same unit as the unit (host or agent) by which monitoring for the target agent was suspended.

5. Click the **Change Settings** button in the Monitoring Suspension Settings window.
6. Select the **Resume monitoring** radio button in the section in which to select the processing type for the setup in the Monitoring Suspension Settings > Change Settings window. Choose the processing unit for the setup and the targets to setup and then click the **Next** button.
7. In the Monitoring Suspension Settings > Check Changes window, confirm that the contents of **Monitoring status** and **Settings** are what you expect.
8. Click the **Execute** button.
9. A message indicating that the updating of the settings information is completed is displayed in the Monitoring Suspension Settings > Check Results window. Click the **OK** button. Monitoring for the target host or agent is resumed based on the settings information.
10. If you enable the automatic synchronization options of the settings information for the monitoring suspension function in a multiple-monitoring environment, confirm that automatic synchronization succeeds. Log in to PFM - Web Console on the secondary manager and confirm that the specified settings are applied. If the specified settings are not applied, duplicate the definition information. For details, see [11.5 Duplicating definition information](#).

# 9

## Backing Up and Restoring Data

This chapter explains how to back up and restore a Performance Management system. The procedure is intended for system administrators.

It is important to consider backing up your Performance Management system as part of your backup plan for the entire system.



## 9.1 Overview of backing up and restoring data

Some data used in Performance Management might be unrecoverable: for example, when the Performance Management system becomes inoperable due to a disk failure. To prepare for such situations, you need to back up the definition information and operation monitoring data periodically. When an aspect of the Performance Management system or its host machine fails, you can restore the data from when a backup was last taken.

### 9.1.1 Information that needs to be backed up

#### (1) Types of information

The following table lists the types of information related to Performance Management that need to be backed up.

Table 9–1: Types of information requiring backup

Information requiring backup	Description	
Definition information	Definition information required for Performance Management to operate	
	Report definition information	Definition information required to display reports.
	Alarm definition information	Definition information required to generate alarms.
	Business group definition information	Definition information required to set business groups.
	Service definition information	Definition information required to start Performance Management.
	Bookmark definition information	Bookmark definition information set for individual users.
	Definition information for process monitoring templates	Definition information required to use definition templates for process monitoring.
Operation monitoring data	Operation monitoring data collected by Performance Management	
	Event data	Data that records the events that occurred in Performance Management. Event data is stored in the Store database and managed in PFM - Manager.
	Performance data	Data that records performance information collected by PFM - Agent or PFM - RM for a monitored program on a monitored agent. Performance data is stored in the Store database and managed in PFM - Agent or PFM - RM.

#### (2) Information requiring backup on each host

The following table lists the information that needs to be backed up on each Performance Management host.

Table 9–2: Information requiring backup on each host

Information requiring backup		Host				
		PFM - Manag er	PFM - Web Consol e	PFM - Base	PFM - Agent	PFM - RM
Definition information	Report definition information	Y	--	--	--	--
	Alarm definition information	Y	--	--	--	--
	Business group definition information	Y	--	--	--	--
	Service definition information	Y	Y	Y	Y	Y
	Bookmark definition information	--	Y	--	--	--
	Definition information for process monitoring templates	--	Y	--	--	--
Operation monitoring data	Event data	Y	--	--	--	--
	Performance data	--	--	--	Y	Y

Legend:

Y: Requires backup.

--: Not applicable.

### (3) When to back up data

When planning backup operations, you need to consider the timing with which each type of data is updated. The following table describes when each type of data is updated, and when it is appropriate to back up the data.

Table 9–3: Backup timing for data requiring backup

Information requiring backup		Update timing	Backup timing
Definition information	Report definition information	When the system is set up When definition information is changed	When the system is set up, when changes are made to the system configuration, and when changes are made to definition information.
	Alarm definition information	When the system is set up When definition information is changed	
	Business group definition information	When the system is set up When changes are made to the system configuration	
	Service definition information	When the system is set up When changes are made to the system configuration When definition information is changed	
	Bookmark definition information	When the system is set up When definition information is changed	

Information requiring backup		Update timing	Backup timing
Definition information	Definition information for process monitoring templates	When the system is set up When definition information is changed	When the system is set up, when changes are made to the system configuration, and when changes are made to definition information.
Operation monitoring data	Event data	Continuously while the system is running	Back up the data regularly, at an appropriate interval.
	Performance data	Continuously while the system is running	

## 9.1.2 Notes on backup and restoration in a cluster system

Note the following when using Performance Management in a cluster system:

- When using Performance Management in a cluster system, back up data on the shared disk, the executing host, and the standby host.
- Data backed up from a logical host must be restored to a logical host with the same name.

## 9.2 Backing up and restoring definition information

You have to back up and restore the service definition information on the hosts for PFM - Manager, PFM - Web Console, PFM - Base, PFM - Agent, and PFM - RM respectively.

The following gives cautionary notes on backing up and restoring the service definition information:

Notes:

- If you restore the service definition information only to the PFM - Agent or PFM - RM host, node information on the instance and others added after backup remain on the host of PFM - Manager and PFM - Web Console. In this case, do the following operations to delete the unnecessary agent information:  
To delete the unnecessary agent information:
  1. Execute the `jpctool service delete` command.
  2. Restart the PFM - Manager programs and services.
  3. Restart the PFM - Web Console programs and services.
- If PFM - Manager is used to back up or restore service definition information when a PFM - Agent or PFM - RM instance is added to the system or a port used to communicate with PFM - Agent or PFM - RM is dynamic, the port used when the data is backed up might differ from the port used after the data is restored. If this occurs, PFM - Manager might not be able to communicate with PFM - Agent or PFM - RM, or PFM - Web Console might not be able to display information correctly. In such a case, restart the relevant PFM - Agent or PFM - RM services.



### Tip

Agent information refers to the information required for PFM - Manager, PFM - Web Console, and other products to manage and display PFM - Agent and PFM - RM.

### 9.2.1 Methods of backing up and restoring definition information

The following table describes the methods you can use to back up and restore definition information associated with Performance Management.

Table 9–4: Ways to back up and restore definition information

Use case	Backup and restoration method	Supported versions	Available while services are running	Available while services are stopped	Refer to
Backing up definition information for PFM - Manager, PFM - Agent, and PFM - RM, or PFM - Base, PFM - Agent, and PFM - RM, on the same host	Backup: Execute a command Restore: Manually copy restore files	Version 10-00 or later of PFM - Manager or PFM - Base Version 10-00 or later of PFM - Agent or PFM - RM	Backup: Yes, Restore: No	Backup: Yes, Restore: Yes	<a href="#">9.2.2</a>
Executing a backup operation without stopping the PFM - Web Console service	Backup: Execute a command	Version 10-00-10 or later of PFM	Backup: Yes, Restore: Yes	Backup: Yes, Restore: Yes	<a href="#">9.2.3</a>

Use case	Backup and restoration method	Supported versions	Available while services are running	Available while services are stopped	Refer to
Executing a backup operation without stopping the PFM - Web Console service	Restore: Manually copy restore files	- Manager, PFM - Base, or PFM - Web Console	Backup: Yes, Restore: Yes	Backup: Yes, Restore: Yes	9.2.3
Backing up definition information in the batch mode on hosts where you cannot use the <i>Execute a command</i> method	Copy files manually	All versions	Backup: No, Restore: No	Backup: Yes, Restore: Yes	9.2.4 9.2.5 9.2.6 9.2.7
Migrating PFM - Manager report definitions, alarm definitions, or business group definitions to an instance of PFM - Manager on another host for each type of definition information	Import and export data	All versions	Backup: Yes, Restore: Yes	Backup: No, Restore: No	9.2.8 9.2.9 9.2.10
Migrating PFM - Web Console bookmark definitions and process monitoring definition templates to an instance of PFM - Web Console on another host	Copy files manually (definitions can be copied separately)	All versions	Backup: No, Restore: No	Backup: Yes, Restore: Yes	9.2.12 9.2.13

Legend:

Yes: Can be used.

No: Cannot be used.

We recommend that you use the *Execute a command* method to back up definition information. However, if the versions of PFM - Agent and PFM - RM are earlier than 10-00, you must copy the target files manually to back them up.

The following table describes the definition information each backup and restoration method is able to collect.

**Table 9–5: Definition information collected by each backup and restoration method**

Information requiring backup		Backup and restoration method			
		Execute a command	Copy files manually	Copy files manually (definitions can be copied separately)	Import and export data
Definition information	Report definition information	Y	Y	--	Y
	Alarm definition information			--	Y
	Business group definition information			--	Y
	Service definition information			--	--
	Bookmark definition information			Y	--
	Definition information for process monitoring templates			Y	--

Legend:

Y: Can be collected.

--: Cannot be collected.

## 9.2.2 Using a command to back up and restore definition information (other than PFM - Web Console)

You can back up definition information for Performance Management from the command line without stopping the service. By implementing this process as part of a batch process, you can operate a system in which backups are made automatically.

For Performance Management other than PFM - Web Console, execute the `jpccfgbackup` command to back up definition information and copy the files to restore the definition information.

### (1) Backing up definition information

Make sure that the following prerequisites are met before you use a command to back up definition information.

Prerequisites

- To run the script in UNIX, you must be able to use the Korn (ksh).
- When using a command to back up definition information specific to a certain type of PFM - Agent or PFM - RM, the version of the PFM - Agent or PFM - RM instance must be 10-00 or later. For earlier versions, copy the definition information manually.

Notes:

- When backing up definition information, keep a record of the version numbers of the products in the environment where the backup was taken.  
See the *Release Notes* for details on the product version numbers.
- Do not specify a backup destination on a network drive.
- Do not make any changes to definitions or the system configuration while the command is running. The following operations involve changes to definitions or the system configuration:
  - When using commands: Any operation that requires administrator role to execute.
  - When using PFM - Web Console: Any operation that requires administrator role to execute.If any such changes are made, the command might fail to execute. If the command provides a return value of 235, execute the command again while leaving the definitions and system configuration unchanged.

To back up definition information:

1. Log on to the host where you want to back up definition information.
2. Navigate to the following directory:  
`installation-folder\tools` (in Windows)  
`/opt/jp1pc/tools` (in UNIX)
3. Execute the `jpccfgbackup` command.

In a non-cluster system:

For example, to back up definition information to the folder `C:\backup`, execute the command as follows:

```
jpccfgbackup C:\backup
```

In a cluster system:

On the executing node:

For example, to back up the definition information for the executing node to the folder `C:\backup\jp1-ha1`, execute the command as follows with the shared disk connected to the executing node:

```
jpccfgbackup C:\backup\jp1-ha1
```

On the standby node:

For example, to back up the definition information for the standby node to the folder `C:\backup\jp1-ha2`, execute the command as follows without the shared disk connected to the standby node:

```
jpccfgbackup C:\backup\jp1-ha2
```

## (2) Restoring definition information

Make sure that the following prerequisites are met before you restore definition information backed up by a command.

Prerequisites

- All the Performance Management services on the host which you want to restore must be stopped.
- The configuration of the system managed by PFM - Manager must be the same as it was when the backup was taken<sup>#</sup>.
- Each host must have the same host name as it did when the backup was taken.
- The PFM product configuration in the backup environment (the name and version of PFM products, the number of instances of PFM - Agent and PFM - RM, and the name of each instance) must be the same as the PFM product configuration in the environment where the data is being restored.

#

Refers to the following aspects of the instances of PFM - Agent and PFM - RM managed by PFM - Manager:

- Network configuration (host name, IP address)
- Instance names, monitoring target names
- Product versions

Note:

When you restore Performance Management settings, the version numbers of the products in the restoration environment must exactly match those in the backup environment. See the *Release Notes* for details on the product version numbers.

To restore definition information:

1. Log on to the host where you want to restore definition information.
2. Make sure that all Performance Management programs and services are stopped on the host.
3. Restore the definition information.

In a non-cluster system:

For example, if the definition files backed up by the command are stored in the `C:\backup` folder, move the entire contents of `C:\backup\jp1pcbackup\localhost` to the following directory:

Windows: *installation-folder*, UNIX: `/opt/jp1pc`

In a cluster system:

On the executing node:

For example, if the definition files backed up on the executing node by the command are stored in the C:\backup\jpl-ha1 folder, move the entire contents of C:\backup\jpl-ha1\jplpcbbackup\localhost to the following directory:

*installation-folder* (in Windows)

/opt/jplpc (in UNIX)

With the shared disk connected to the executing node, move the entire contents of C:\backup\jpl-ha1\jplpcbbackup\*logical-host-name*<sup>#1</sup> to the following directory:

*environment-directory*<sup>#2</sup>\jplpc\ (in Windows)

*environment-directory*<sup>#2</sup>/jplpc/ (in UNIX)

#1

Replace *logical-host-name* with the name of the logical host where the backup was taken.

#2

*environment-directory* is the directory created on the shared disk when creating logical hosts.

On the standby node:

For example, if the definition files backed up on the standby node by the command are stored in the C:\backup\jpl-ha2 folder, move the entire contents of C:\backup\jpl-ha2\jplpcbbackup\localhost to the following directory:

*installation-folder* (in Windows)

/opt/jplpc (in UNIX)

#### 4. If you have assigned fixed port numbers to programs or services, restore the port number information.

In a non-cluster system:

For example, if the definition files backed up by the command are stored in the C:\backup folder, execute the following command to restore port information:

```
jpccconf port define -key all -input C:\backup\jplpcbbackup\pfm_port.def
```

In a cluster system:

After restoring port information on the executing node, do the same for the standby node.

On the executing node:

For example, if the definition files backed up by the command on the executing node are stored in the C:\backup\jpl-ha1 folder, execute the command shown below to restore port information. For *logical-host-name*, enter the logical host name used by the cluster system.

To restore port information for the physical host:

```
jpccconf port define -key all -input C:\backup\jpl-ha1\jplpcbbackup\pfm_port.def
```

To restore port information for the logical host:

```
jpccconf port define -key all -lhost logical-host-name -input C:\backup\jpl-ha1\jplpcbbackup\pfm_port_logical-host-name.def
```

After restoring the port information, export the logical host environment definition from the executing node so that the port settings on the standby node can be synchronized with those of the executing node. Execute the command as follows to export port information to the file *jpl-ha.conf*:

```
jpccconf ha export -f jpl-ha.conf
```

On the standby node:

For example, if the definition files backed up by the command on the standby node are stored in the C:\backup\jpl-ha2 folder, execute the following command to restore port information:

To restore port information for the physical host:



```
jpccconf port define -key all -input C:\backup\jpl-ha2\jplpcbackup
\pfm_port.def
```

Execute the following command to apply the logical host environment definition of the executing node to the standby node:

```
jpccconf ha import -f jpl-ha.conf
```

5. In a non-cluster system, use the `jpccspm start` command to start the PFM services. In a cluster system, use the cluster software to start the services.

6. If you restored PFM - Manager, execute the following synchronization command from the PFM - Manager to perform synchronization processing for the PFM services of the PFM - Agent or PFM - RM host that connects to the PFM - Manager.

```
jpctool config sync
```

For details about the `jpctool config sync` command, see the chapter that describes commands in the manual *JP1/Performance Management Reference*.

### 9.2.3 Using a command for backup and file copying for restoration (PFM - Web Console)

You can back up definition information for PFM - Web Console from the command line without stopping the service. By implementing this process as part of a batch process, you can operate a system in which backups are made automatically.

For PFM - Web Console, execute the `jpccwbackup` command to back up definition information and copy the files to restore the definition information.

#### (1) Prerequisites

You can use the backup command on hosts with PFM - Web Console installed.

#### (2) Collective backup using the backup command

The backup command allows you to collectively back up the definition information provided by PFM - Web Console without stopping the service. You can back up the information to a directory of your choice.

The backup command backs up the following information:

- Definition information for the PFM - Web Console service
- Bookmark information
- Process monitoring template information

The following table describes the directory structure the backup command creates at the specified backup directory.

Table 9–6: Directory structure at backup destination

Directory structure	Description
<i>backup-directory</i>	A directory chosen by the operator, specified in the command line.
<i>backup-directory</i> \jplpcwbackup	Backup destination for PFM - Web Console service definition information, authentication key files, and bookmark information.

Directory structure	Description
<i>backup-directory</i> \jplpcwcbbackup\ \Backup_info_wc.txt	PFM - Web Console configuration information file
<i>backup-directory</i> \jplpcwcbbackup\jplpcWebCon	Backup destination for PFM - Web Console service definition information
<i>backup-directory</i> \jplpcwcbbackup\jplpcWebCon\ \CPSB	Backup destination for PFM - Web Console service definition information (Web server settings files and encrypted communication files) <sup>#1</sup>
Service definition information in <i>backup-directory</i> \ jplpcwcbbackup\jplpcWebCon\CPSB\ \	PFM - Web Console service definition information (Web server settings files and encrypted communication files)
<i>backup-directory</i> \jplpcwcbbackup\jplpcWebCon\ \conf	Backup destination for PFM - Web Console service definition information (PFM - Web Console settings files)
Service definition information in <i>backup-directory</i> \ jplpcwcbbackup\jplpcWebCon\conf\ \	PFM - Web Console service definition information (PFM - Web Console settings files)
<i>backup-directory</i> \jplpcwcbbackup\jplpcWebCon\ \cmdkey	Backup destination for authentication key files
Authentication keys in <i>backup-directory</i> \ jplpcwcbbackup\jplpcWebCon\cmdkey\ \	Authentication key file (JPCCMDKEY) <sup>#2</sup>
<i>backup-directory</i> \jplpcwcbbackup\bookmarks	Backup destination for bookmark information
Bookmark information in <i>backup-directory</i> \ jplpcwcbbackup\bookmarks\ \	Bookmark definition files (across several folders and files) <sup>#3</sup>
<i>backup-directory</i> \jplpcwcbbackup\ \processMonitoringTemplates	Backup destination for process monitoring template information
Process monitoring template information in <i>backup-</i> <i>directory</i> \jplpcwcbbackup\ \processMonitoringTemplates\ \	Process monitoring template files (across several folders and files) <sup>#3</sup>
<i>backup-directory</i> \info	Storage location for maintenance information associated with backup process <sup>#4</sup>

#1

The folder structure under CPSB is as follows:

- CPSB\httpsd\conf\  
\
- CPSB\httpsd\conf\ssl\server\  
\
- CPSB\CC\web\redirector\  
\
- CPSB\CC\web\containers\PFMWebConsole\usrconf\  
\

#2

If the `jpcmkkey` command has never been executed, backup data might not be acquired because there is no directory to back up.

#3

In the standby node of a cluster system or an environment where the PFM - Web Console has never started, backup data might not be acquired because there is no data to back up.

#4

The `info` directory and its contents are acquired as maintenance information for troubleshooting purposes.

In order to restore the data you backed up, the configuration of PFM - Web Console on the host must be the same as it was when the backup was taken.

The `backup` command outputs information about the PFM - Web Console configuration on the host to a file. You can check for consistency between the backup and restoration environments by viewing the contents of this file.

The following table provides an overview of PFM - Web Console configuration information file.

Table 9–7: Overview of PFM - Web Console configuration information file

Item	Description
File name	Backup_info_wc.txt
Output file path	In Windows: <i>backup-directory\jplpcwcbbackup\Backup_info_wc.txt</i> In UNIX: <i>backup-directory/jplpcwcbbackup/Backup_info_wc.txt</i>
Contents	The date and time of the backup, and configuration information for PFM - Web Console on the host.

For details on the contents of the PFM - Web Console configuration information file (`Backup_info_wc.txt`), the format of each item, and the items you need to check, see [Table 9-9 List of PFM - Web Console configuration items to be checked](#).

### (a) Backup in a cluster environment

When you use a command to back up definition information in a cluster environment, the command is unable to access the logical host environment directory from the standby node. This means that some of the information that can be backed up from the executing host cannot be backed up from the standby host. The following table describes the differences between the executing and standby hosts in terms of the definition information that can be backed up.

Table 9–8: Differences in definition information backed up on executing and standby hosts

Host in cluster system	Definition information that can be backed up by the backup command		
	Physical host	Shared disk	
	Service definition information	Bookmark information	Process monitoring template information
Executing host	Y	Y	Y
Standby host	Y	N	N

Legend:

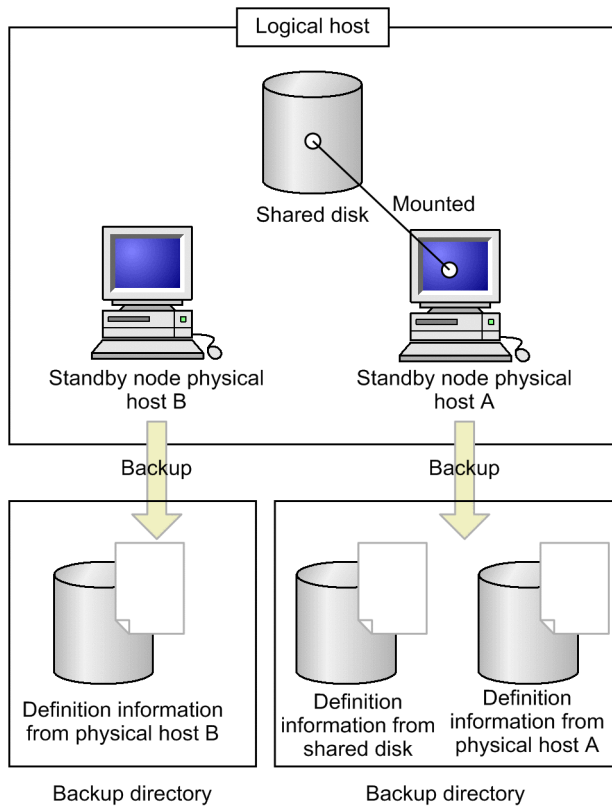
Y: Can be backed up.

N: Cannot be backed up.

When you use the backup command on the standby node, the command does not collect definition information (bookmark information and process monitoring template information) from the shared disk. At this time, the message KAVJT6551-W is output notifying the operator that this part of the backup process has been skipped.

The following figure illustrates the backup process when the backup command is executed on the executing and standby hosts in a cluster system.

Figure 9–1: Execution of backup command in a cluster system



### (3) Backup procedures

#### (a) Backup procedure in a non-cluster system

1. Log on to the host where PFM - Web Console is installed.
2. Navigate to the directory *installation-folder\tools* where the backup command file is located.
3. Back up the definition information by executing the `jpcwbackup -d directory` command as a user with Administrators or Backup Operators permission.

#### (b) Backup procedure in a cluster system

In a cluster system, the backup command must be executed on the executing host and the standby host. If a failover occurs before the backup process is completed, execute the command again on both hosts after the failover.

1. Log on to the executing host where PFM - Web Console is installed.
2. Navigate to the directory *installation-folder\tools* where the backup command file is located.
3. Back up the definition information by executing the `jpcwbackup -d directory` command as a user with Administrators or Backup Operators permission.
4. Log on to the standby host where PFM - Web Console is installed.
5. Navigate to the directory *installation-folder\tools* where the backup command file is located.
6. Back up the definition information by executing the `jpcwbackup -d directory` command as a user with Administrators or Backup Operators permission.

## (4) Restoration procedure

In order to restore data from a backup, the configuration of PFM - Web Console on the host must be the same as it was when the backup was taken.

For each item in the PFM - Web Console configuration information (`Backup_info_wc.txt`), the table below describes the contents of each item and its output format. It also describes each item, and whether you need to check the item for consistency between the backup and restoration environments.

Table 9–9: List of PFM - Web Console configuration items to be checked

No.	Content	Output format	Description and checking	Must match
1	Date and time of command backup	<code>DateTime=</code> <i>date-and-time-of-command-execution</i>	The date and time when the backup command began executing, according to the time zone setting of the user who executed the command. The value of this item depends on the locale and operating system. Examples: In Windows with Japan as the locale <code>yyyy/mm/ddΔHH:MM:SS</code> In Linux with Japan as the locale <code>yyyy-mm-ddΔHH:MM:SS</code>	N
2	Host name of machine with PFM - Web Console installed	<code>Hostname=</code> <i>host-name</i>	The host name of the machine on which PFM - Web Console is installed. To be checked: Make sure that the host name matches that of the machine on which the backup was taken.	Y
3	Path of PFM - Web Console installation directory	<code>InstallDirectory=</code> <i>installat ion-directory-path</i>	The folder where PFM - Web Console is installed, as an absolute path. To be checked: Make sure that the installation directory matches the directory in which PFM - Web Console is installed in the restoration environment.	Y
4	Installation	<code>PFM - Web ConsolePP-nameΔ: Δ</code> <i>VV-RR-SS</i>	The PP name of the installed instance of PFM - Web Console, followed by the PP version in the format <i>VV-RR-SS</i> . For versions with no value for <i>SS</i> (such as 10-00), 00 is output for <i>SS</i> . To be checked: Make sure that the program product model name and the <i>VV</i> , <i>RR</i> , and <i>SS</i> values of the version information match that of the restoration environment. For details about how to check the program product model name and the version information, see the appendix that describes how to check the version information in the <i>JP1/Performance Management Planning and Configuration Guide</i> .	Y
5	PFM - Web Console information	<code>bookmarkRepository=</code> <i>locati on-of-bookmark-definition-information</i>	The location of bookmark definition information, as the value of the <code>bookmarkRepository</code> parameter in the <code>config.xml</code> file. If the parameter is not specified in <code>config.xml</code> , <code>bookmarkRepository=</code> is output for this item.	N

No.	Content	Output format	Description and checking	Must match
5	PFM - Web Console information	<code>bookmarkRepository=location-of-bookmark-definition-information</code>	To be checked: Whether the path is accessible on the machine where PFM - Web Console is installed in the restoration environment.	N
6	Location of bookmark definition information	<code>processMonitoringTemplatesRepository=location-of-process-monitoring-template-information</code>	The location of process monitoring template information, as the value of the <code>processMonitoringTemplatesRepository</code> parameter in the <code>config.xml</code> file. If the parameter is not specified in <code>config.xml</code> , <code>processMonitoringTemplatesRepository=</code> is output for this item.  To be checked: Whether the path is accessible on the machine where PFM - Web Console is installed in the restoration environment.	N

Legend:

Y: Needs to match the backup environment.

N: Does not need to match the backup environment.

The following table lists the source and destination paths for restored data.

Table 9–10: Source and destination paths for data to be restored (in Windows)

Data to be restored	Backup file path of data to be restored <sup>#</sup>	Restoration path	
		Result of checking Backup_info_wc.txt	Path
Service definition information	D:\backup \jplpcwcbbackup \jplpcWebCon	--	<i>installation-folder</i> \
Bookmark information	D:\backup \jplpcwcbbackup \bookmarks	<code>bookmarkRepository</code> has no value	<i>installation-folder</i> \bookmarks
		All other situations	Path specified for <code>bookmarkRepository</code> in <code>Backup_info_wc.txt</code>
Process monitoring template information	D:\backup \jplpcwcbbackup \processMonitoringTemplates	<code>processMonitoringTemplatesRepository</code> has no value	<i>installation-folder</i> \processMonitoringTemplates
		All other situations	Path specified for <code>processMonitoringTemplatesRepository</code> in <code>Backup_info_wc.txt</code>

Legend:

--: Not applicable.

#

Assuming the backup destination folder is D:\backup.

Table 9–11: Source and destination paths for data to be restored (in UNIX)

Data to be restored	Backup file path of data to be restored <sup>#</sup>	Restoration path	
		Result of checking Backup_info_wc.txt	Path
Service definition information	/tmp/backup/ jplpcwcbbackup/ jplpcWebCon	--	/opt/jplpcwebcon
Bookmark information	/tmp/backup/ jplpcwcbbackup/ bookmarks	bookmarkRepository has no value	/opt/jplpcwebcon/bookmarks
		All other situations	Path specified for bookmarkRepository in Backup_info_wc.txt
Process monitoring template information	/tmp/backup/ jplpcwcbbackup/ processMonitoringTemplates	processMonitoringTemplatesRepository has no value	/opt/jplpcwebcon/ processMonitoringTemplates
		All other situations	Path specified for processMonitoringTemplatesRepository in Backup_info_wc.txt

Legend:

--: Not applicable.

#

Assuming the backup directory is /tmp/backup.

### (a) Restoration procedure in a non-cluster environment

1. Check the PFM - Web Console configuration.

Make sure that the items in the PFM - Web Console configuration information file (Backup\_info\_wc.txt) in the backup data are the same as in the restoration environment.

When checking bookmark definition information and process monitoring template definition information:

When there is no setting for `bookmarkRepository` or `processMonitoringTemplatesRepository` in the PFM - Web Console configuration information file (Backup\_info\_wc.txt), the default directory is used.

2. If you are using encrypted communication, use the `jpcwtool https output certtext` command to check the expiration date of the server certificate.  
Check that the server certificate for the backup data has not expired.  
If the server certificate has expired, contact the certificate authority that issued the server certificate to find out how to renew the server certificate, and then prepare the server certificate in the restoration-target environment. For details, see the procedure that describes how to prepare a certificate (server certificate or self-signed certificate) in the section that describes what to do when a certificate (server certificate or self-signed certificate) has expired in the *JPI/Performance Management Planning and Configuration Guide*.
3. Log on to the PFM - Web Console host where you want to restore the data.
4. Stop the PFM - Web Console service on the host by executing the `jpcwstop` command.
5. Check the location of the backup files.  
Make sure that backup files are available that were created on the same host.
6. Delete or move the data at the location where the backup data is to be restored.

When restoring service definition information:

Because the restoration process will overwrite the files listed below, keep a copy of the data if needed:

- Initialization file (*installation-folder*\conf\config.xml)
- All files in the encrypted communication file storage folder

When restoring bookmark definition information or process monitoring template definition information:

After the restoration process, the storage directories for bookmark information and process monitoring template information are those specified as the values of the `bookmarkRepository` and `processMonitoringTemplatesRepository` parameters in the PFM - Web Console configuration information file (`Backup_info_wc.txt`). These directories must be empty when you restore the data. Delete any data in these directories, or move the data to another location.

#### 7. Restore the definition information.

Check the source and destination paths of the data being restored, and copy all of the files at the backup file path to the restoration destination, maintaining the directory structure.

#### 8. Make sure that the settings in the initialization file (*installation-folder*\conf\config.xml) match the system environment at the restoration destination.

#### 9. If you have renewed the server certificate in step 2, store the file in the restoration-target environment and specify the settings needed to use encrypted communication.

For details, see the subsections beginning with the procedure that describes where to store encrypted communication files in the section that describes what to do when a certificate (server certificate or self-signed certificate) has expired in the *JPI/Performance Management Planning and Configuration Guide*.

#### 10. Start the PFM - Web Console service on the host by executing the `jpcwstart` command.

## (b) Restoration procedure in a cluster environment

Restoration procedure on the executing host:

#### 1. Check the PFM - Web Console configuration.

Make sure that the items in the PFM - Web Console configuration information file (`Backup_info_wc.txt`) in the backup data are the same as in the restoration environment.

#### 2. If you are using encrypted communication, use the `jpcwtool https output certtext` command to check the expiration date of the server certificate.

Check that the server certificate for the backup data has not been expired.

If the server certificate has expired, contact the certificate authority that issued the server certificate to find out how to renew the server certificate, and then prepare the server certificate in the restoration-target environment. For details, see the procedure that describes how to prepare a certificate (server certificate or self-signed certificate) in the section that describes what to do when a certificate (server certificate or self-signed certificate) has expired in the *JPI/Performance Management Planning and Configuration Guide*.

#### 3. Log on to the executing host where you want to restore the data.

#### 4. Stop the PFM - Web Console service on the host by using the cluster software.

#### 5. Check the location of the backup files.

When restoring service definition information:

Make sure that backup files are available that were created on the same host.



When restoring bookmark definition information or process monitoring template definition information:

Make sure that backup files are available that were created on the executing host.

Backup data taken while a host is operating as the standby host after a failover does not include bookmark definition information or process monitoring template information. This information is only collected from hosts operating as the executing host. For this reason, you must use backup data that was collected from an executing host (the physical host has no bearing).

6. Delete or move the data at the location where the data is to be restored.

When restoring service definition information:

Because the restoration process will overwrite the files listed below, keep a copy of the data if needed:

- Initialization file (*installation-folder\conf\config.xml*)
- All files in the encrypted communication file storage folder

When restoring bookmark definition information or process monitoring template definition information:

Delete or move the bookmark information and process monitoring template information present at the restore destination.

After the restoration process, the storage directories for bookmark information and process monitoring template information are those specified as the values of the `bookmarkRepository` and `processMonitoringTemplatesRepository` parameters in the PFM - Web Console configuration information file (*Backup\_info\_wc.txt*). These directories must be empty when you restore the data. Delete any data in these directories, or move the data to another location.

7. Restore the definition information.

Check the source and destination paths of the data being restored, and copy all of the files at the backup file path to the restoration destination, maintaining the directory structure.

8. Make sure that the settings in the initialization file (*installation-folder\conf\config.xml*) match the system environment at the restoration destination.

9. If you have renewed the server certificate in step 2, store the file in the restoration-target environment and specify the settings needed to use encrypted communication.

For details, see the subsections beginning with the procedure that describes where to store encrypted communication files in the section that describes what to do when a certificate (server certificate or self-signed certificate) has expired in the *JPI/Performance Management Planning and Configuration Guide*.

10. Start the PFM - Web Console service on the host using the cluster software.

Restoration procedure on the standby host:

1. Check the PFM - Web Console configuration.

Make sure that the items in the PFM - Web Console configuration information file (*Backup\_info\_wc.txt*) in the backup data are the same as in the restoration environment.

2. If you are using encrypted communication, use the `jpcwtool https output certtext` command to check the expiration date of the server certificate.

Check that the server certificate for the backup data has not been expired.

If the server certificate has expired, contact the certificate authority that issued the server certificate to find out how to renew the server certificate, and then prepare the server certificate in the restoration-target environment. For details, see the procedure that describes how to prepare a certificate (server certificate or self-signed certificate) in the section that describes what to do when a certificate (server certificate or self-signed certificate) has expired in the *JPI/Performance Management Planning and Configuration Guide*.

3. Log on to the standby host where you want to restore the data.
4. Stop the PFM - Web Console service on the host by using the cluster software.
5. Check the location of the backup files.

When restoring service definition information:

Make sure that backup files are available that were created on the same host.

Note:

Because the standby host cannot access the shared disk, you cannot restore bookmark definition information and process monitoring template information on a standby host.

6. Delete or move the data at the location where the data is to be restored.

When restoring service definition information:

Because the restoration process will overwrite the files listed below, keep a copy of the data if needed:

- Initialization file (*installation-folder*\conf\config.xml)
- All files in the encrypted communication file storage folder

7. Restore the definition information.

Check the source and destination paths of the data being restored, and copy all of the files at the backup file path to the restoration destination, maintaining the directory structure.

8. Make sure that the settings in the initialization file (*installation-folder*\conf\config.xml) match the system environment at the restoration destination.
9. If you have renewed the server certificate in step 2, store the file in the restoration-target environment and specify the settings needed to use encrypted communication.  
For details, see the subsections beginning with the procedure that describes where to store encrypted communication files in the section that describes what to do when a certificate (server certificate or self-signed certificate) has expired in the *JP1/Performance Management Planning and Configuration Guide*.
10. Start the PFM - Web Console service on the host using the cluster software.

## 9.2.4 Backing up and restoring definition information by copying files (other than PFM - Web Console)

### (1) Backing up definition information

Make sure that the following prerequisites are met before backing up definition information.

Prerequisites

- All Performance Management services must be stopped.

Notes:

- When backing up definition information, keep a record of the version numbers of the products in the environment where the backup was taken. See the *Release Notes* for details on the product version numbers.
- Different operating systems impose different limits on the lengths of file paths. If the full path of the backup directory exceeds the length restrictions of the operating system, the backup process will not work correctly. After taking the backup, make sure that the data has been copied correctly.

To back up definition information:

1. Log on to the host where you want to back up definition information.
2. Make sure that all Performance Management programs and services are stopped on the host.
3. Copy the definition information files to your chosen backup destination. For details about the definition information files that need to be backed up, see [9.2.6 Files to be backed up \(in Windows\)](#) or [9.2.7 Files to be backed up \(in UNIX\)](#).

## (2) Restoring definition information

Make sure that the following prerequisites are met before you restore definition information:

Prerequisites

- All the Performance Management services on the host which you want to restore must be stopped.
- The configuration of the system managed by PFM - Manager must be the same as it was when the backup was taken<sup>#</sup>.
- Each host must have the same host name as it did when the backup was taken.
- The PFM product configuration in the backup environment (the name and version of PFM products, the number of instances of PFM - Agent and PFM - RM, and the name of each instance) must be the same as the PFM product configuration in the environment where the data is being restored.

#

Refers to the following aspects of the instances of PFM - Agent and PFM - RM managed by PFM - Manager:

- Network configuration (host names and IP addresses)
- Instance names and monitoring target names
- Product versions

Note:

When you restore Performance Management settings, the version numbers of the products in the restoration environment must exactly match those in the backup environment. See the *Release Notes* for details on the product version numbers.

When restoring data to a PFM - Base host

1. Log on to the host where you want to restore the data.
2. Make sure that all Performance Management programs and services are stopped on the host (including any logical hosts).
3. Overwrite the definition information files on the host with those in the backup data.
4. Start the Performance Management services.

When restoring data to a PFM - Manager host

1. Log on to the host where you want to restore the data.
2. Make sure that all Performance Management programs and services are stopped on the host (including any logical hosts).
3. Overwrite the definition information files on the host with those in the backup data.
4. Start PFM - Manager.
5. Execute the `jpctool config sync` command.

For details about the `jpctool config sync` command, see the chapter that describes commands in the manual *JP1/Performance Management Reference*.

## 9.2.5 Backing up and restoring definition information by copying files (PFM - Web Console)

### (1) Backing up definition information

Make sure that the following prerequisites are met before backing up definition information.

Prerequisites

- All Performance Management services must be stopped.

Notes:

- When backing up definition information, keep a record of the version numbers of the products in the environment where the backup was made. See the *Release Notes* for details about the product version numbers.
- Different operating systems impose different limits on the lengths of file paths. If the full path of the backup directory exceeds the length restrictions of the operating system, the backup process will not work correctly. After making the backup, check that the data has been copied correctly.

To back up definition information:

1. Log on to the host where you want to back up definition information.
2. Make sure that all PFM - Web Console programs and services are stopped on the host.
3. Copy the definition information files to your chosen backup destination. For details about the definition information files that need to be backed up, see [9.2.6 Files to be backed up \(in Windows\)](#) or [9.2.7 Files to be backed up \(in UNIX\)](#).

You can back up definition information associated with PFM - Web Console while the services are running. However, because the operations listed in the following table modify the definition information you are backing up, do not perform any of these operations while a backup is in progress.

Table 9–12: Prohibited operations when backing up PFM - Web Console data with services running

Operation	Window		Updated definition information
Registering a baseline	Agents tree	Baseline window	Bookmark definition information
Registering a bookmark or combination bookmark		Bookmark window	
Editing a combination bookmark	Bookmarks tree	Edit window	
Saving a tiled layout		Tiling Display window	
Creating a new bookmark folder		New Folder window	
Renaming a bookmark folder, bookmark, combination bookmark, or baseline		Rename window	
Deleting a bookmark folder, bookmark, combination bookmark, registered report, or baseline		Bookmark window (Delete method)	

Operation	Window		Updated definition information
Creating an application definition template	Agents tree	Process Monitoring Settings > Create a New Application Definition Template window	Definition information for process monitoring definition templates
Editing an application definition template		Process Monitoring Settings > Edit an Application Definition Template window	
Deleting an application definition template		Process Monitoring Settings > Delete an Application Definition Template window	
Saving an application definition template		Process Monitoring Settings > Save an Application Definition Template window	
Executing the <code>jpcmkkey</code> command	--	--	Information about PFM - Manager for the connection destination
Executing the <code>jpcwconf https enable</code> command	--	--	Web server settings file
Executing the <code>jpcwconf https disable</code> command	--	--	Web server settings file

Legend:

--: Not applicable.

## (2) Restoring definition information

Make sure that the following prerequisites are met before you restore definition information:

### Prerequisites

- All the PFM - Web Console services on the host which you want to restore must be stopped.
- Each host must have the same host name that it did when the backup was made.

### Note:

When you restore Performance Management settings, the version numbers of the products in the restoration environment must exactly match those in the backup environment. See the *Release Notes* for details about the product version numbers.

1. Log on to the host where you want to restore the data.
2. Make sure that all PFM - Web Console services are stopped on the host (including any logical hosts).
3. Overwrite the definition information files on the host with the files in the backup data.
4. Start the PFM - Web Console services.

## 9.2.6 Files to be backed up (in Windows)

This subsection lists the files to be backed up by copying files in Windows. Note that depending on the functions that are used, some of these files are not created.

## (1) List of PFM - Manager files to be backed up (in Windows)

The following tables list the definition information files for PFM - Manager that need to be backed up.

Table 9–13: PFM - Manager definition information files to be backed up (in Windows on a physical host)

Folder or file name	Description
<i>installation-folder</i> \jpchosts	Host information configuration file for Performance Management
<i>installation-folder</i> \*.ini	Settings file common to Performance Management
<i>installation-folder</i> \jpcautobind.cfg	Auto alarm bind setting file for Performance Management
<i>installation-folder</i> \bin\action\*.ini	Settings file for the Action Handler service
<i>installation-folder</i> \bin\statsvr\*.ini	Settings file for the Status Server service
<i>installation-folder</i> \mgr\clator\*.ini	Settings file for the Correlator service
<i>installation-folder</i> \mgr\manager\*.ini	Settings file for the Master Manager service
<i>installation-folder</i> \mgr\manager\*.DB	Database file for the Master Manager service <sup>#3</sup>
<i>installation-folder</i> \mgr\manager\*.IDX	Index file for the Master Manager service <sup>#3</sup>
<i>installation-folder</i> \mgr\manager\*.DAT (*.dat)	Data model file for the Master Manager service
<i>installation-folder</i> \mgr\store\*.ini	Settings file for the Master Store service
<i>installation-folder</i> \mgr\store\*.DAT	Data model file for the Master Store service
<i>installation-folder</i> \mgr\namesvr\*.ini	Settings file for the Name Server service
<i>installation-folder</i> \mgr\namesvr\*.DB	Database file for the Name Server service
<i>installation-folder</i> \mgr\namesvr\*.IDX	Index file for the Name Server service
<i>installation-folder</i> \mgr\trapgen\*.ini	Settings file for the Trap Generator service
<i>installation-folder</i> \mgr\viewsvr\*.ini	Settings file for the View Server service
<i>installation-folder</i> \mgr\viewsvr\data\*	User definition information file for the View Server service
<i>installation-folder</i> \mgr\viewsvr\reports\*	Report definition information file for the View Server service <sup>#4</sup>
<i>installation-folder</i> \agt0\agent\*.ini	Settings file for the Agent Collector service (files for the health check agent)
<i>installation-folder</i> \agt0\agent\*.DB	Database file for the Agent Collector service (files for the health check agent)
<i>installation-folder</i> \agt0\agent\*.IDX	Index file for the Agent Collector service (files for the health check agent)
<i>installation-folder</i> \agt0\store\*.ini	Settings file for the Agent Store service (files for the health check agent)
<i>installation-folder</i> \sys\*.ini	Common settings file for Performance Management
<i>installation-folder</i> \sys\*.dat	Common data model file for Performance Management
<i>installation-folder</i> \mgr\ITSLM\*.ini	JP1/SLM linkage definition file
<i>installation-folder</i> \ITSLM\monitoringitems.cfg	Definition file for JP1/ITSLM-linkage custom monitoring items

**Table 9–14: PFM - Manager definition information files to be backed up (in Windows on a logical host)**

Folder or file name	Description
<i>installation-folder</i> \jpc\hosts	Host information configuration file for Performance Management
<i>environment-directory</i> <sup>#1</sup> \jplpc\*.ini	Settings file common to Performance Management
<i>environment-directory</i> <sup>#1</sup> \jplpc\jpc\autobind.cfg	Auto alarm bind setting file for Performance Management
<i>environment-directory</i> <sup>#1</sup> \jplpc\bin\action\*.ini	Settings file for the Action Handler service
<i>installation-folder</i> \bin\statsvr\*.ini <sup>#2</sup>	Settings file for the Status Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\clator\*.ini	Settings file for the Correlator service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\manager\*.ini	Settings file for the Master Manager service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\manager\*.DB	Database file for the Master Manager service <sup>#3</sup>
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\manager\*.IDX	Index file for the Master Manager service <sup>#3</sup>
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\manager\*.DAT (* .dat)	Data model file for the Master Manager service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\store\*.ini	Settings file for the Master Store service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\store\*.DAT	Data model file for the Master Store service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\namesvr\*.ini	Settings file for the Name Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\namesvr\*.DB	Database file for the Name Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\namesvr\*.IDX	Index file for the Name Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\trapgen\*.ini	Settings file for the Trap Generator service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\viewsvr\*.ini	Settings file for the View Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\viewsvr\*.ini	Settings file for the View Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\viewsvr\data\*	User definition information file for the View Server service
<i>environment-directory</i> <sup>#1</sup> \jplpc\mgr\viewsvr\reports\*	Report definition information file for the View Server service <sup>#4</sup>
<i>environment-directory</i> <sup>#1</sup> \jplpc\agt0\agent\*.ini	Settings file for the Agent Collector service (files for the health check agent)
<i>environment-directory</i> <sup>#1</sup> \jplpc\agt0\agent\*.DB	Database file for the Agent Collector service (files for the health check agent)
<i>environment-directory</i> <sup>#1</sup> \jplpc\agt0\agent\*.IDX	Index file for the Agent Collector service (files for the health check agent)
<i>environment-directory</i> <sup>#1</sup> \jplpc\agt0\store\*.ini	Settings file for the Agent Store service (files for the health check agent)
<i>installation-folder</i> \sys\*.ini	Common settings file for Performance Management
<i>environment-directory</i> <sup>#1</sup> \sys\*.dat	Common data model file for Performance Management
<i>environment-directory</i> <sup>#1</sup> \mgr\ITSLM\*.ini	JP1/SLM linkage definition file
<i>environment-directory</i> <sup>#1</sup> \ITSLM\monitoringitems.cfg	Definition file for JP1/ITSLM-linkage custom monitoring items



- #1  
The environment directory is a directory on the shared disk created when a logical host is created.
- #2  
The settings file for the Status Server service exists only on the physical host even when Performance Management is run in a cluster system.
- #3  
Includes alarm definition information.
- #4  
Includes report definition information.

## (2) List of PFM - Web Console files to be backed up (in Windows)

You can back up the files associated with PFM - Web Console even while the service is running. However, certain operations should not be performed while a backup is in progress. For details, see [Table 9-12 Prohibited operations when backing up PFM - Web Console data with services running](#).

The following tables list the definition information files for PFM - Web Console that need to be backed up.

**Table 9–15: PFM - Web Console definition information files to be backed up (in Windows on a physical host)**

Folder or file name	Description
<i>installation-folder</i> \conf\*	Settings file for PFM - Web Console
<i>installation-folder</i> \bookmarks\* (when installed using the default settings)	Bookmark definition information file for PFM - Web Console
<i>installation-folder</i> \cmdkey\*	Authentication key file for the PFM - Web Console command
<i>installation-folder</i> \CPSB\httpsd\conf\*.conf	Settings file for PFM - Web Console
<i>installation-folder</i> \CPSB\httpsd\conf\ssl\server\*	Encrypted communication file for PFM - Web Console
<i>installation-folder</i> \CPSB\CC\web\redirector\workers.properties	Settings file for PFM - Web Console
<i>installation-folder</i> \CPSB\CC\web\containers\PFMWebConsole\usrconf\*.cfg	Settings file for PFM - Web Console
<i>installation-folder</i> \CPSB\CC\web\containers\PFMWebConsole\usrconf\usrconf.properties	Settings file for PFM - Web Console
<i>installation-folder</i> \processMonitoringTemplates\*#1 (when installed using the default settings)	Definition templates for PFM - Web Console process monitoring

**Table 9–16: PFM - Web Console definition information files to be backed up (in Windows on a logical host)**

Folder or file name	Description
<i>installation-folder</i> \conf\*	Settings file for PFM - Web Console
<i>environment-directory</i> #2\jp1pcWebCon\bookmarks\* (when installed using the default settings)	Bookmark definition information file for PFM - Web Console
<i>installation-folder</i> \cmdkey\*	Authentication key file for the PFM - Web Console command
<i>installation-folder</i> \CPSB\httpsd\conf\*.conf	Settings file for PFM - Web Console



Folder or file name	Description
<i>installation-folder</i> \CPSB\httpsd\conf\ssl\server\*	Encrypted communication file for PFM - Web Console
<i>installation-folder</i> \CPSB\CC\web\redirector\workers.properties	Settings file for PFM - Web Console
<i>installation-folder</i> \CPSB\CC\web\containers\PFMWebConsole\usrconf\*.cfg	Settings file for PFM - Web Console
<i>installation-folder</i> \CPSB\CC\web\containers\PFMWebConsole\usrconf\usrconf.properties	Settings file for PFM - Web Console
<i>environment-directory</i> <sup>#2</sup> \jplpcWebCon\processMonitoringTemplates\* <sup>#1</sup> (when installed using the default settings)	Definition templates for PFM - Web Console process monitoring

#1

Include any subfolders when you back up the `processMonitoringTemplates` folder.

The path shown here is the default path. You can change the location of definition templates for PFM - Web Console process monitoring by specifying the new location in the `processMonitoringTemplatesRepository` parameter in the `<process-monitoring>` tag within the `<vsa>` tag in the initialization file (`config.xml`). If you change the location, back up the files and folders at the new location.

#2

The environment directory is a folder on the shared disk created when a logical host is created.

### (3) List of PFM - Base files to be backed up (in Windows)

The following tables list the definition information files for PFM - Base that need to be backed up.

Table 9–17: PFM - Base definition information files to be backed up (in Windows on a physical host)

Folder or file name	Description
<i>installation-folder</i> \jpchosts	Host information configuration file for Performance Management
<i>installation-folder</i> \*.ini	Settings file common to Performance Management
<i>installation-folder</i> \bin\action\*.ini	Settings file for the Action Handler service
<i>installation-folder</i> \bin\statsvr\*.ini	Settings file for the Status Server service
<i>installation-folder</i> \sys\*.ini	Common settings files for Performance Management
<i>installation-folder</i> \sys\*.dat	Common data model file for Performance Management

Table 9–18: PFM - Base definition information files to be backed up (in Windows on a logical host)

Folder or file name	Description
<i>installation-folder</i> \jpchosts	Host information configuration file for Performance Management
<i>environment-directory</i> <sup>#1</sup> \jplpc\*.ini	Settings file common to Performance Management
<i>environment-directory</i> <sup>#1</sup> \jplpc\bin\action\*.ini	Settings file for the Action Handler service
<i>installation-folder</i> <sup>#2</sup> \bin\statsvr\*.ini	Settings file for the Status Server service
<i>installation-folder</i> \sys\*.ini	Common settings files for Performance Management
<i>environment-directory</i> <sup>#1</sup> \sys\*.dat	Common data model file for Performance Management

#1

The environment directory is a folder on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

## (4) List of PFM - Agent files to be backed up (in Windows)

The tables below list the definition information files for PFM - Agent that need to be backed up.

The tables list the files that need to be backed up for every type of PFM - Agent. Depending on your environment, other definition information files specific to certain types of PFM - Agent might also need to be backed up. For details, see the appropriate PFM - Agent manual.

Table 9–19: PFM - Agent definition information files to be backed up (in Windows on a physical host)

File name	Description
<i>installation-folder\xxx#1\agent\*.ini</i>	Settings file for the Agent Collector service
<i>installation-folder\xxx#1\agent\*.DB</i>	Database files for the Agent Collector service
<i>installation-folder\xxx#1\agent\*.IDX</i>	Index files for the Agent Collector service
<i>installation-folder\xxx#1\agent\*.dat</i>	Data model file for the Agent Collector service
<i>installation-folder\xxx#1\agent\instance-name#2\*.ini</i>	Settings file for the Agent Collector service
<i>installation-folder\xxx#1\agent\instance-name#2\*.DB</i>	Database files for the Agent Collector service
<i>installation-folder\xxx#1\agent\instance-name#2\*.IDX</i>	Index files for the Agent Collector service
<i>installation-folder\xxx#1\agent\instance-name#2\*.dat</i>	Data model file for the Agent Collector service
<i>installation-folder\xxx#1\store\*.ini</i>	Settings file for the Agent Store service
<i>installation-folder\xxx#1\store\instance-name#2\*.ini</i>	Settings file for the Agent Store service

Table 9–20: PFM - Agent definition information files to be backed up (in Windows on a logical host)

File name	Description
<i>installation-folder\xxx#1\agent\*.ini</i>	Settings file for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\*.ini</i>	Settings file for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\*.DB</i>	Database files for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\*.IDX</i>	Index files for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\*.dat</i>	Data model file for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\instance-name\*.ini</i>	Settings file for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\instance-name\*.DB</i>	Database files for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\instance-name\*.IDX</i>	Index files for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\agent\instance-name#2\*.dat</i>	Data model file for the Agent Collector service
<i>environment-directory#3\jp1pc\xxx#1\store\*.ini</i>	Settings file for the Agent Store service

File name	Description
<i>environment-directory</i> <sup>#3</sup> \jplpc\xxx <sup>#1</sup> \store\instance-name <sup>#2</sup> \*.ini	Settings file for the Agent Store service

#1

xxxx represents the service key of the PFM - Agent. For details on the service key for each PFM - Agent instance, see the section that describes naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

These are folders that exist when running in an instance environment. In an instance configuration, one folder is created for each instance. For details on instance environments, see the appropriate PFM - Agent or PFM - RM manual.

#3

The environment directory is a folder on the shared disk created when a logical host is created.

## (5) List of PFM - RM files to be backed up (in Windows)

The tables below list the definition information files for PFM - RM that need to be backed up.

The tables list the files that need to be backed up for each type of PFM - RM. Depending on your environment, other definition information files specific to certain types of PFM - RM might also need to be backed up. For details, see the appropriate PFM - RM manual.

Table 9–21: PFM - RM definition information files to be backed up (in Windows on a physical host)

File name	Description
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\*.ini	Settings file for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \*.ini	Settings file for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \groups\*.ini	Settings file for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \*.IDX	Index files for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \*.dat	Data model file for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \groups\*.ini	Settings files for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \targets\*.ini	Settings file for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \agent\instance-name <sup>#2</sup> \targets\*.dat	Data model file for the Remote Monitor Collector service
<i>installation-folder</i> \xxx <sup>#1</sup> \store\*.ini	Settings file for the Remote Monitor Store service
<i>installation-folder</i> \xxx <sup>#1</sup> \store\instance-name <sup>#2</sup> \*.ini	Settings file for the Remote Monitor Store service

Table 9–22: PFM - RM definition information files to be backed up (in Windows on a logical host)

File name	Description
<i>installation-folder\xxx#1\agent\*.ini</i>	Settings file for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name\*.ini</i>	Settings file for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name\*.DB</i>	Database files for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name\*.IDX</i>	Index files for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name#2\*.dat</i>	Data model file for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name\groups\*.ini</i>	Settings file for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name\targets\*.ini</i>	Settings file for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\agent\instance-name#2\targets\*.dat</i>	Data model file for the Remote Monitor Collector service
<i>environment-directory#3\jplpc\xxx#1\store\*.ini</i>	Settings file for the Remote Monitor Store service
<i>environment-directory#3\jplpc\xxx#1\store\instance-name#2\*.ini</i>	Settings file for the Remote Monitor Store service

#1

xxx indicates the service key of each PFM - RM. For details on the PFM - RM service keys, see the description of the naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

These are folders that exist when running in an instance environment. In an instance configuration, one folder is created for each instance. For details on instance environments, see the appropriate PFM - Agent or PFM - RM manual.

#3

The environment directory is a folder on the shared disk created when a logical host is created.

## 9.2.7 Files to be backed up (in UNIX)

This subsection lists the files to be backed up by copying files in UNIX. Note that depending on the functions that are used, some of these files are not created.

### (1) List of PFM - Manager files to be backed up (in UNIX)

The following tables list the definition information files for PFM - Manager that need to be backed up.

Table 9–23: PFM - Manager definition information files to be backed up (in UNIX on a physical host)

Folder or file name	Description
<i>/opt/jplpc/jpchosts</i>	Host information configuration file for Performance Management
<i>/opt/jplpc/*.ini</i>	Settings file common to Performance Management
<i>/opt/jplpc/jpcautobind.cfg</i>	Auto alarm bind setting file for Performance Management

Folder or file name	Description
/opt/jplpc/bin/action/*.ini	Settings file for the Action Handler service
/opt/jplpc/bin/statsvr/*.ini	Settings file for the Status Server service
/opt/jplpc/mgr/clator/*.ini	Settings file for the Correlator service
/opt/jplpc/mgr/manager/*.ini	Settings file for the Master Manager service
/opt/jplpc/mgr/manager/*.DB	Database file for the Master Manager service
/opt/jplpc/mgr/manager/*.IDX	Index file for the Master Manager service
/opt/jplpc/mgr/manager/*.DAT (*.dat)	Data model file for the Master Manager service
/opt/jplpc/mgr/store/*.ini	Settings file for the Master Store service
/opt/jplpc/mgr/store/*.DAT	Data model file for the Master Store service
/opt/jplpc/mgr/namesvr/*.ini	Settings file for the Name Server service
/opt/jplpc/mgr/namesvr/*.DB	The database file for the Name Server service
/opt/jplpc/mgr/namesvr/*.IDX	Index file for the Name Server service
/opt/jplpc/mgr/trapgen/*.ini	Settings file for the Trap Generator service
/opt/jplpc/mgr/viewsvr/*.ini	Settings file for the View Server service
/opt/jplpc/mgr/viewsvr/jpcvsvr	Settings file for the View Server service
/opt/jplpc/mgr/viewsvr/data/*	User definition information file for the View Server service
/opt/jplpc/mgr/viewsvr/Reports/*	Report definition information file for the View Server service
/opt/jplpc/agt0/agent/*.ini	Settings file for the Agent Collector service (files for the health check agent)
/opt/jplpc/agt0/store/*.ini	Settings file for the Agent Store service (files for the health check agent)
/opt/jplpc/agt0/agent/*.IDX	Index files for the Agent Collector service (files for the health check agent)
/opt/jplpc/agt0/store/*.ini	Settings files for the Agent Store service (files for the health check agent)
/opt/jplpc/sys/*.ini	Common settings files for Performance Management
/opt/jplpc/sys/*.dat	Common data model files for Performance Management
/opt/jplpc/mgr/ITSLM/*.ini	JP1/SLM linkage definition files
/opt/jplpc/ITSLM/monitoringitems.cfg	Definition file for JP1/ITSLM-linkage custom monitoring items

**Table 9–24: PFM - Manager definition information files to be backed up (in UNIX on a logical host)**

Folder or file name	Description
/opt/jplpc/jpchosts	Host information configuration file for Performance Management
/environment-directory <sup>#1</sup> /jplpc/*.ini	Settings file common to Performance Management
/environment-directory <sup>#1</sup> /jplpc/jpcautobind.cfg	Auto alarm bind setting file for Performance Management
/environment-directory <sup>#1</sup> /jplpc/bin/action/*.ini	Settings file for the Action Handler service
/opt/jplpc/bin/statsvr/*.ini <sup>#2</sup>	Settings file for the Status Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/clator/*.ini	Settings file for the Correlator service

Folder or file name	Description
/environment-directory <sup>#1</sup> /jplpc/mgr/manager/*.ini	Settings file for the Master Manager service
/environment-directory <sup>#1</sup> /jplpc/mgr/manager/*.DB	Database file <sup>#3</sup> for the Master Manager service
/environment-directory <sup>#1</sup> /jplpc/mgr/manager/*.IDX	Index file <sup>#3</sup> for the Master Manager service
/environment-directory <sup>#1</sup> /jplpc/mgr/manager/*.DAT (* .dat)	Data model file for the Master Manager service
/environment-directory <sup>#1</sup> /jplpc/mgr/store/*.ini	Settings file for the Master Store service
/environment-directory <sup>#1</sup> /jplpc/mgr/store/*.DAT	Data model file for the Master Store service
/environment-directory <sup>#1</sup> /jplpc/mgr/namesvr/*.ini	Settings file for the Name Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/namesvr/*.DB	Database file for the Name Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/namesvr/*.IDX	Index file for the Name Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/trapgen/*.ini	Settings file for the Trap Generator service
/opt/jplpc/mgr/viewsvr/*.ini	Settings files for the View Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/viewsvr/*.ini	Settings file for the View Server service
/opt/jplpc/mgr/viewsvr/jpcsvr	Settings file for the View Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/viewsvr/data/*	User definition information file for the View Server service
/environment-directory <sup>#1</sup> /jplpc/mgr/viewsvr/ Reports/*	Report definition information file <sup>#4</sup> for the View Server service
/environment-directory <sup>#1</sup> /jplpc/agt0/agent/*.ini	Settings file for the Agent Collector service (files for the health check agent)
/environment-directory <sup>#1</sup> /jplpc/agt0/agent/*.DB	Database files for the Agent Collector service (files for the health check agent)
/environment-directory <sup>#1</sup> /jplpc/agt0/agent/*.IDX	Index files for the Agent Collector service (files for the health check agent)
/environment-directory <sup>#1</sup> /jplpc/agt0/store/*.ini	Settings file for the Agent Store service (files for the health check agent)
/opt/jplpc/sys/*.ini	Common settings files for Performance Management
/environment-directory <sup>#1</sup> /jplpc/sys/*.dat	Common data model files for Performance Management
/environment-directory <sup>#1</sup> /mgr/ITSLM/*.ini	JP1/SLM linkage definition files
/environment-directory <sup>#1</sup> /ITSLM/monitoringitems.cfg	Definition file for JP1/ITSLM-linkage custom monitoring items

#1

The environment directory is a directory on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

#3

Includes alarm definition information.

#4

Includes report definition information.

## (2) List of PFM - Web Console files to be backed up (in UNIX)

You can back up the files associated with PFM - Web Console even while the service is running. However, certain operations should not be performed while a backup is in progress. For details, see [Table 9-12 Prohibited operations when backing up PFM - Web Console data with services running](#).

The following tables list the definition information files for PFM - Web Console that need to be backed up.

**Table 9–25: PFM - Web Console definition information files to be backed up (in UNIX on a physical host)**

Folder or file name	Description
/opt/jplpcwebcon/conf/*	Settings file for PFM - Web Console
/opt/jplpcwebcon/bookmarks/* (when installed using the default settings)	Bookmark definition information file for PFM - Web Console
/opt/jplpcwebcon/cmdkey/*	Authentication key file for the PFM - Web Console command
/opt/jplpcwebcon/CPSB/httpsd/conf/*.conf	Settings file for PFM - Web Console
/opt/jplpcwebcon/CPSB/httpsd/conf/ssl/server/*	Encrypted communication file for PFM - Web Console
/opt/jplpcwebcon/CPSB/CC/web/redirector/workers.properties	Settings file for PFM - Web Console
/opt/jplpcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/*.cfg	Settings file for PFM - Web Console
/opt/jplpcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/usrconf.properties	Settings file for PFM - Web Console
/opt/jplpcwebcon/processMonitoringTemplates/* <sup>#1</sup> (when installed using the default settings)	Definition templates for PFM - Web Console process monitoring

**Table 9–26: PFM - Web Console definition information files to be backed up (in UNIX on a logical host)**

Folder or file name	Description
/opt/jplpcwebcon/conf/*	Settings file for PFM - Web Console
/environment-directory <sup>#2</sup> /jplpcwebcon/bookmarks/* (when installed using the default settings)	Bookmark definition information file for PFM - Web Console
/opt/jplpcwebcon/cmdkey/*	Authentication key file for the PFM - Web Console command
/opt/jplpcwebcon/CPSB/httpsd/conf/*.conf	Settings file for PFM - Web Console
/opt/jplpcwebcon/CPSB/httpsd/conf/ssl/server/*	Encrypted communication file for PFM - Web Console
/opt/jplpcwebcon/CPSB/CC/web/redirector/workers.properties	Settings file for PFM - Web Console
/opt/jplpcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/*.cfg	Settings file for PFM - Web Console
/opt/jplpcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/usrconf.properties	Settings file for PFM - Web Console
/environment-directory <sup>#2</sup> /jplpcwebcon/processMonitoringTemplates/* <sup>#1</sup> (when installed using the default settings)	Definition templates for PFM - Web Console process monitoring



#1

Include any subdirectories when you back up the `processMonitoringTemplates` directory.

The path shown here is the default path. You can change the location of definition templates for PFM - Web Console process monitoring by specifying the new location in the `processMonitoringTemplatesRepository` parameter in the `<process-monitoring>` tag within the `<vsa>` tag in the initialization file (`config.xml`). If you change the location, back up the files and directories at the new location.

#2

The environment directory is a folder on the shared disk created when a logical host is created.

### (3) List of PFM - Base files to be backed up (in UNIX)

The following tables list the definition information files for PFM - Base that need to be backed up.

Table 9–27: PFM - Base definition information files to be backed up (in UNIX on a physical host)

Folder or file name	Description
<code>/opt/jplpc/jpchosts</code>	Host information configuration file for Performance Management
<code>/opt/jplpc/*.ini</code>	Settings file common to Performance Management
<code>/opt/jplpc/bin/action/*.ini</code>	Settings file for the Action Handler service
<code>/opt/jplpc/bin/statsvr/*.ini</code>	Settings file for the Status Server service
<code>/opt/jplpc/sys/*.ini</code>	Common settings files for Performance Management
<code>/opt/jplpc/sys/*.dat</code>	Common data model files for Performance Management

Table 9–28: PFM - Base definition information files to be backed up (in UNIX on a logical host)

Folder or file name	Description
<code>/opt/jplpc/jpchosts</code>	Host information configuration file for Performance Management
<code>/environment-directory<sup>#1</sup>/jplpc/*.ini</code>	Settings file common to Performance Management
<code>/environment-directory<sup>#1</sup>/jplpc/bin/action/*.ini</code>	Settings file for the Action Handler service
<code>/opt/jplpc/bin/statsvr/*.ini<sup>#2</sup></code>	Settings file for the Status Server service
<code>/opt/jplpc/sys/*.ini</code>	Common settings files for Performance Management
<code>/environment-directory<sup>#1</sup>/jplpc/sys/*.dat</code>	Common data model files for Performance Management

#1

The environment directory is a directory on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

### (4) List of PFM - Agent files to be backed up (in UNIX)

The tables below list the definition information files for PFM - Agent that need to be backed up.

The tables list the files that need to be backed up for every type of PFM - Agent. Depending on your environment, other definition information files specific to certain types of PFM - Agent might also need to be backed up. For details, see the appropriate PFM - Agent manual.



**Table 9–29: PFM - Agent definition information files to be backed up (in UNIX on a physical host)**

File name	Description
/opt/jp1pc/xxx <sup>#1</sup> /agent/*.ini	Settings file for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/*.DB	Database files for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/*.IDX	Index files for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/*.dat	Data model file for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.ini	Settings file for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.DB	Database files for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.IDX	Index files for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.dat	Data model file for the Agent Collector service
/opt/jp1pc/xxx <sup>#1</sup> /store/*.ini	Settings file for the Agent Store service
/opt/jp1pc/xxx <sup>#1</sup> /store/instance-name <sup>#2</sup> /*.ini	Settings file for the Agent Store service

**Table 9–30: PFM - Agent definition information files to be backed up (in UNIX on a logical host)**

File name	Description
/opt/jp1pc/xxx <sup>#1</sup> /agent/*.ini	Settings file for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/*.ini	Settings file for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/*.DB	Database files for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/*.IDX	Index files for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/*.dat	Data model file for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.ini	Settings file for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.DB	Database files for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.IDX	Index files for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.dat	Data model file for the Agent Collector service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /store/*.ini	Settings file for the Agent Store service
/environment-directory <sup>#3</sup> /jp1pc/xxx <sup>#1</sup> /store/instance-name <sup>#2</sup> /*.ini	Settings file for the Agent Store service

#1

xxx represents the service key of the PFM - Agent. For details on the service key for each PFM - Agent instance, see the section that describes naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

These are directories when running in an instance environment. In an instance configuration, one directory is created for each instance. For details on instance environments, see the appropriate PFM - Agent or PFM - RM manual.

#3

The environment directory is a directory on the shared disk created when a logical host is created.

## (5) List of PFM - RM files to be backed up (in UNIX)

The tables below list the definition information files for PFM - RM that need to be backed up.

The tables list the files that need to be backed up for each type of PFM - RM. Depending on your environment, other definition information files specific to certain types of PFM - RM might also need to be backed up. For details, see the appropriate PFM - RM manual.

**Table 9–31: PFM - RM definition information files to be backed up (in UNIX on a physical host)**

File name	Description
/opt/jplpc/xxx <sup>#1</sup> /agent/*.ini	Settings file for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.ini	Settings file for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.DB	Database files for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.IDX	Index files for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.dat	Data model file for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /groups/*.ini	Settings file for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /targets/*.ini	Settings file for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /targets/*.dat	Data model file for the Remote Monitor Collector service
/opt/jplpc/xxx <sup>#1</sup> /store/*.ini	Settings file for the Remote Monitor Store service
/opt/jplpc/xxx <sup>#1</sup> /store/instance-name <sup>#2</sup> /*.ini	Settings file for the Remote Monitor Store service

**Table 9–32: PFM - RM definition information files to be backed up (in UNIX on a logical host)**

File name	Description
/opt/jplpc/xxx <sup>#1</sup> /agent/*.ini	Settings file for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/*.ini	Settings file for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/*.DB	Database files for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/*.IDX	Index files for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /*.dat	Data model file for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /groups/*.ini	Settings file for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /targets/*.ini	Settings file for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /targets/*.dat	Data model file for the Remote Monitor Collector service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /store/*.ini	Settings file for the Remote Monitor Store service
/environment-directory <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /store/instance-name <sup>#2</sup> /*.ini	Settings file for the Remote Monitor Store service

#1

xxx indicates the service key of each PFM - RM. For details on the PFM - RM service keys, see the description of the naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

These are directories that exist when running in an instance environment. In an instance configuration, one directory is created for each instance. For details on instance environments, see the appropriate PFM - Agent or PFM - RM manual.

#3

The environment directory is a directory on the shared disk created when a logical host is created.

## 9.2.8 Backing up and restoring a report definition

You can use import and export functionality to back up and restore report definitions separately. For details on how to export report definitions, see [5.3.13 Exporting reports](#). For details on how to import report definitions, see [5.3.14 Importing reports](#).

Note the following when importing a report definition into an instance of PFM - Manager running on a different host from where it was exported:

- The data model used in the exported report must be set up at the PFM - Manager where the report is being imported.

## 9.2.9 Backing up and restoring an alarm definition

You can use import and export processes to back up and restore alarm definitions separately. For details on how to export alarm definitions, see [6.4.10 Exporting alarm tables](#). For details on how to import alarm definitions, see [6.4.11 Importing alarm tables](#).

Note the following when importing an alarm definition into an instance of PFM - Manager running on a different host from where the alarm was exported:

- If a report is associated with the alarm, the same report definition must be present at the PFM - Manager where the alarm is being imported.
- If the alarm specifies an action handler, an action handler with the same name must be present in the Performance Management system managed by the instance of PFM - Manager into which the alarm is being imported.
- If the alarm specifies an action in the form of a JP1 event, the JP1 event in the alarm definition must be updated to suit PFM - Manager at the new environment.
- The data model used in the exported alarm must be set up at the PFM - Manager where the alarm is being imported.
- The PFM - Manager where the alarm is imported must use the same character set as the PFM - Manager from which the alarm was exported.

## 9.2.10 Backing up and restoring a business group definition

You can use import and export processes to back up and restore business group definitions separately.

### (1) Backing up and restoring business group definitions defined in Performance Management

You can back up and restore the business groups defined in Performance Management by exporting and importing the definition information. For details on how to import and export these definitions, see [2.7.4\(2\)\(a\) Changing the configuration of business groups defined in Performance Management](#).

## (2) Backing up and restoring business group definitions defined in JP1/IM

Business groups defined in JP1/IM must be backed up and restored from within JP1/IM. Having restored business group definitions in JP1/IM, you can then export the definitions from JP1/IM and import them into Performance Management. For details on how to import business group definitions exported from JP1/IM into Performance Management, see [2.7.3\(3\) Importing business group definition information](#).

### 9.2.11 Backing up and restoring specific definition information (auto alarm bind definition information)

This subsection describes how to manually back up and restore auto alarm bind definition information (specifically, the auto alarm bind setting file).

By default, the auto alarm bind setting file is placed in the following location on the PFM - Manager host:

- In Windows:

*installation-folder*<sup>#1</sup>\jpcautobind.cfg

#1:

If you are operating PFM - Manager in a cluster system, the location of the file would be *environment-directory* \jplpc.

- In UNIX:

/opt/jplpc<sup>#2</sup>/jpcautobind.cfg

#2:

If you are operating PFM - Manager in a cluster system, the location of the file would be */environment-directory*/jplpc.

### (1) Backing up auto alarm bind definition information

You can manually back up only the auto alarm bind setting file by following the procedure described below. This procedure assumes that the file is stored in the default location.

1. Stop the PFM - Manager services.

For details about how to stop the services, see [1.3.1 Stopping services on monitoring managers and monitoring agents](#).

2. Back up the `jpcautobind.cfg` file located under the auto alarm bind setting file storage directory.

Back up the file by copying it to any location you like or using a similar manner.

3. Start the PFM - Manager services.

For details about how to start the services, see [1.2.1 Starting services on monitoring managers and monitoring agents](#).

### (2) Restoring auto alarm bind definition information

You can manually restore only the auto alarm bind setting file by following the procedure described below. This procedure assumes that the file is stored in the default location.

1. Stop the PFM - Manager services.

For details about how to stop the services, see *1.3.1 Stopping services on monitoring managers and monitoring agents*.

2. Copy the backed-up `jpcautobind.cfg` file to the auto alarm bind setting file storage directory.

3. Start the PFM - Manager services.

For details about how to start the services, see *1.2.1 Starting services on monitoring managers and monitoring agents*.

## 9.2.12 Backing up and restoring a bookmark definition

This subsection describes how to back up and restore bookmark definition information separately.

### Important

When backing up and restoring bookmark definition information separately, copy the directory manually to a location of your choice. Make sure that the PFM - Web Console service is stopped before you restore the information. However, you should back up and restore the entire directory that contains the bookmark definition information as well as a part of files and directories at one time.

The default location of the bookmark definition information and bookmark folders is as follows: By default, the bookmark definition information and bookmark directories are stored in the following location on the PFM - Web Console host:

- In Windows:  
`installation-folder\bookmarks\`
- In UNIX:  
`/opt/jp1pcwebcon/bookmarks/`

Note:

If the storage directory for bookmark definition information has been changed from the default, the source and destination for backup and restoration operations is the directory specified in the `bookmarkRepository` parameter of the initialization file (`config.xml`).

### (1) Backing up bookmark definition information

The following describes how to back up the directories containing bookmark definition information, in their entirety.

The following example assumes that bookmark definition information is stored in the default location, and that the PFM - Manager host to which PFM - Web Console connects is named `hostA`.

Bookmark storage folder:

- In Windows:  
`installation-folder\bookmarks\hostA\0\`
- In UNIX:  
`/opt/jp1pcwebcon/bookmarks/hostA/0/`

1. Stop the PFM - Web Console service.

For details on how to stop the service, see *1.3.2 Stopping services on the monitoring console server*.

You can back up data associated with PFM - Web Console while the service is running. However, certain operations should not be performed while a backup is in progress. For details, see [Table 9-12 Prohibited operations when backing up PFM - Web Console data with services running](#).

2. Back up the 0 directory in the bookmark storage directory.

Back up the folder by copying it to your chosen backup destination.

3. Start the PFM - Web Console service.

For details on how to start the service, see [1.2.2 Starting services on the monitoring console server](#).

## (2) Restoring bookmark definition information

The following describes how to restore, in its entirety, a directory containing bookmark definition information. The following example assumes that bookmark definition information is stored in the default location, and that the PFM - Manager host to which PFM - Web Console connects is named `hostA`.

Bookmark storage directory:

- In Windows:

`installation-folder\bookmarks\hostA\0\`

- In UNIX:

`/opt/jp1pcwebcon/bookmarks/hostA/0/`

1. Stop the PFM - Web Console service.

For details on how to stop the service, see [1.3.2 Stopping services on the monitoring console server](#).

2. Copy the backed-up 0 directory to the bookmark storage directory.

3. Start the PFM - Web Console service.

For details on how to start the service, see [1.2.2 Starting services on the monitoring console server](#).

## (3) Inheritance of bookmark definition information

### Note

You cannot change the PFM - Manager host for connection target and inherit the bookmarks created before the change while using bookmarks. Recreate the bookmarks on the new PFM - Manager host.

### Important

- If you store bookmark definition information in the default location, the storage folder and the definition information it contains are deleted automatically at uninstallation. If you have changed the storage folder from the default, it is not deleted automatically. Delete it manually if necessary.
- Bookmark definition information is stored in multiple files. For this reason, if an error occurs during the creation, update, or deletion of a definition information file and processing cannot continue, the integrity of the definition information files might be compromised. In such cases, modify or discard the corrupted information.
- If a drill-down report is associated with a report registered in a bookmark, restore the report definition from the GUI.

If you use the `jpcrdef create` command to restore the report definition, you will be unable to display the drill-down report from the bookmark.

### (a) Inheriting bookmarks after changing the folder in which bookmark definition information is stored (in Windows)

In this scenario, you need to change the storage folder first, and then bring the original definition information into the new folder. The following describes how to make the new folder inherit bookmark definition information. The description below assumes that the `host` parameter value in the initialization file (`config.xml`) of PFM - Web Console is `hostB`, and that the bookmark folders are as follows:

Old bookmark storage folder

```
installation-folder\bookmarks\hostB\0\
```

New bookmark storage folder

```
C:\user1\bookmarks\
```

1. Stop the PFM - Web Console service.

For details on how to stop the service, see [1.3.2 Stopping services on the monitoring console server](#).

2. Back up the `hostB` folder located in the old bookmark storage folder.

Back up the folder by copying it to a location of your choice.

3. Change the bookmark storage folder defined in the initialization file (`config.xml`) to the new folder.

For details on how to change the storage folder for bookmark definition information, see the chapter on installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

4. Create the new bookmark storage folder.

5. Copy the folder you backed up in step 2 to the folder you created in step 4.

The folder `C:\user1\bookmarks` now contains the folder `hostB`.

6. Start the PFM - Web Console service.

For details on how to start the service, see [1.2.2 Starting services on the monitoring console server](#).

### (b) Inheriting bookmarks after migrating PFM - Manager and PFM - Web Console to a cluster configuration (in Windows)

Unlike a scenario in which you change the PFM - Manager host for connection destination, you can inherit the original bookmarks when you migrate PFM - Manager and PFM - Web Console from a non-cluster system to a cluster system. This is because PFM - Manager in a cluster system can inherit information about PFM - Agent and PFM - RM connected to PFM - Manager running in a non-cluster system. The description below assumes an environment with the following host names and other conditions:

In the non-cluster system

- PFM - Manager host name: `hostE`

- Host name of PFM - Manager for connection destination for PFM - Web Console: `hostE`

- Bookmark storage folder for PFM - Web Console:

```
installation-folder\jp1pcwebcon\bookmarks\hostE\0\
```



In the cluster system

- PFM - Manager logical host name: `lhostE`
- Host name of PFM - Manager for connection destination for PFM - Web Console: `lhostE`
- Bookmark storage folder for PFM - Web Console:  
`environment-directory\jplpcwebcon\bookmarks\`

1. Stop the PFM - Web Console service.<sup>#</sup>
2. Back up the `0` folder in the bookmark storage folder used in the non-cluster system.  
You can back up the folder by copying it to a location of your choice.
3. Change the bookmark storage folder defined in the initialization file (`config.xml`) to the folder you will use in the cluster system.  
For details on how to change the storage folder for bookmark definition information, see the chapter on installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.
4. Create the bookmark storage folder for use in the cluster system.
5. Create the folder `lhostE` as a subfolder of the bookmark storage folder used in the cluster system.
6. Copy the folder you backed up in step 2 to the `lhostE` folder you created in step 5.  
The folder `environment-directory\jplpcwebcon\bookmarks\lhostE` now contains the folder `0`.
7. Start the PFM - Web Console service.<sup>#</sup>  
  
<sup>#</sup>  
For details on how to start and stop the service, see *10.6.1 Starting and stopping Performance Management in a cluster system*.

### (c) Inheriting bookmarks after changing the directory in which bookmark definition information is stored (in UNIX)

In this scenario, you need to change the storage directory first, and then bring the original definition information into the new directory. The following describes how to make the new directory inherit the original bookmark definition information. The description below assumes that the `host` parameter value in the initialization file (`config.xml`) of PFM - Web Console is `hostB`, and that the bookmark directories are as follows:

Old bookmark storage directory

`/opt/jplpcwebcon/bookmarks/hostB/0/`

New bookmark storage directory

`/opt/user1/bookmarks/`

1. Stop the PFM - Web Console service.  
For details on how to stop the service, see *1.3.2 Stopping services on the monitoring console server*.
2. Back up the `hostB` directory located in the old bookmark storage directory.  
Back up the directory by copying it to a location of your choice.
3. Change the bookmark storage directory defined in the initialization file (`config.xml`) to the new directory.  
For details on how to change the storage directory for bookmark definition information, see the chapter on installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.



4. Create the new bookmark storage directory.
5. Copy the directory you backed up in step 2 to the directory you created in step 4.  
The directory `/opt/user1/bookmarks` now contains the directory `hostB`.
6. Start the PFM - Web Console service.

For details on how to start the service, see [1.2.2 Starting services on the monitoring console server](#).

#### **(d) Inheriting bookmarks after migrating PFM - Manager and PFM - Web Console to a cluster configuration (in UNIX)**

Unlike a scenario in which you change the PFM - Manager host for connection destination, you can inherit the original bookmarks when you migrate PFM - Manager and PFM - Web Console from a non-cluster system to a cluster system. This is because PFM - Manager in a cluster system can inherit information about PFM - Agent and PFM - RM connected to PFM - Manager running in a non-cluster system. The description below assumes an environment with the following host names and other conditions:

In the non-cluster system

- PFM - Manager host name: `hostE`
- Host name of PFM - Manager for connection destination for PFM - Web Console: `hostE`
- Bookmark storage directory for PFM - Web Console:  
`/opt/jp1pcwebcon/bookmarks/hostE/0/`

In the cluster system

- PFM - Manager logical host name: `lhostE`
- Host name of PFM - Manager for connection destination for PFM - Web Console: `lhostE`
- Bookmark storage directory for PFM - Web Console:  
`environment-directory/jp1pcwebcon/bookmarks/`

1. Stop the PFM - Web Console service.<sup>#</sup>
2. Back up the `0` directory in the bookmark storage directory used in the non-cluster system.  
You can back up the directory by copying it to a location of your choice.
3. Change the bookmark storage directory defined in the initialization file (`config.xml`) to the directory you will use in the cluster system.  
For details on how to change the storage directory for bookmark definition information, see the chapter on installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.
4. Create the bookmark storage directory for use in the cluster system.
5. Create the directory `lhostE` as a subdirectory of the bookmark storage directory used in the cluster system.
6. Copy the directory you backed up in step 2 to the `lhostE` directory you created.  
The directory `environment-directory/jp1pcwebcon/bookmarks/lhostE` now contains the directory `0`.
7. Start the PFM - Web Console service.<sup>#</sup>  
  
<sup>#</sup>  
For details on how to start and stop the service, see [10.6.1 Starting and stopping Performance Management in a cluster system](#).

## 9.2.13 Backing up and restoring a process monitoring definition template

This subsection describes how to separately back up and restore definition information for process monitoring definition templates.

Note:

You can back up and restore process monitoring definition templates by manually copying the directory to another location. The PFM - Web Console service must be stopped when you restore the information. Because the definition information for process monitoring definition templates is stored in a directory structure that includes subdirectories, you must back up and restore the directory structure as a whole.

By default, the definition information for process monitoring definition templates is stored in the following location on the PFM - Web Console host:

- In Windows:  
`installation-folder\processMonitoringTemplates\`
- In UNIX:  
`/opt/jp1pcwebcon/processMonitoringTemplates/`

Note:

If you have changed the location of definition information for process monitoring definition templates from the default, the data you need to back up and restore will be located in the directory specified in the `processMonitoringTemplatesRepository` parameter of the initialization file (`config.xml`).

### (1) Backing up definition information for process monitoring definition templates

The following describes how to back up the directory structure that contains definition information for process monitoring definition templates. The example below assumes that the definition information is stored in the default location.

Storage directory for process monitoring definition templates:

- In Windows:  
`installation-folder\processMonitoringTemplates\system\`  
`installation-folder\processMonitoringTemplates\user\`
- In UNIX:  
`/opt/jp1pcwebcon/processMonitoringTemplates/system/`  
`/opt/jp1pcwebcon/processMonitoringTemplates/user/`

#### 1. Stop the PFM - Web Console service.

For details on how to stop the service, see [1.3.2 Stopping services on the monitoring console server](#).

You can back up the files associated with PFM - Web Console even while the service is running. However, certain operations should not be performed while a backup is taking place. For details, see [Table 9-12 Prohibited operations when backing up PFM - Web Console data with services running](#).

#### 2. Back up the `system` and `user` directories in the storage directory for process monitoring definition templates.

Back up the directories by copying them to a location of your choice.

#### 3. Start the PFM - Web Console service.

For details on how to start the service, see [1.2.2 Starting services on the monitoring console server](#).

## (2) Restoring definition information for process monitoring definition templates

The following describes how to restore the directory structure that contains definition information for process monitoring definition templates. The example below assumes that the definition information is stored in the default location.

Storage directory for process monitoring definition templates:

- In Windows:

```
installation-folder\processMonitoringTemplates\system\  
installation-folder\processMonitoringTemplates\user\
```

- In UNIX:

```
/opt/jp1pcwebcon/processMonitoringTemplates/system/  
/opt/jp1pcwebcon/processMonitoringTemplates/user/
```

1. Stop the PFM - Web Console service.

For details on how to stop the service, see [1.3.2 Stopping services on the monitoring console server](#).

2. Copy the backed-up `system` and `user` directories to the storage directory for process monitoring definition templates.

3. Start the PFM - Web Console service.

For details on how to start the service, see [1.2.2 Starting services on the monitoring console server](#).

## 9.3 Backing up and restoring operation monitoring data

---

To back up the operation monitoring data, you can use the `jpctool db backup` command. You must execute the `jpctool db backup` command on a host where PFM - Manager is installed. You can also execute the command on a host where PFM - Agent or PFM - RM is installed, specifying the `-alone` or `-direct` option.

When using Store 2.0, you can perform a partial backup by specifying the `-partial` option.

To restore the operation monitoring data, use the `jpctool db restore` command. You must execute the `jpctool db restore` command on the PFM - Manager, PFM - Agent, or PFM - RM host where the database to be restored is backed up.

However, to execute the `jpctool db backup` and `jpctool db restore` commands, the following user permissions are required:

- In Windows: user with Administrator permissions or Backup Operator permissions
- In UNIX: root user permissions

Next are a couple cautionary notes on backing up and restoring the operation monitoring data:

Notes:

- If the data model version of the Store database that is backed up using the `jpctool db backup` command differs from the version of the Store database to be restored, the Store database cannot be restored.
- If a service key of the data to be restored differs from that of the data that is backed up using the `jpctool db backup` command, the Store database cannot be restored.
- The backup data for the Store database uses the character set of the host where the Store database is running. When you restore a Store database, make sure that the host to which you are restoring the data uses the same character set. If the character sets differ, double-byte characters and single-byte Katakana characters will not be set correctly, preventing the information in reports and event histories from displaying correctly.

### 9.3.1 Backup methods

In Performance Management, you can select the backup method according to the storage method used for the Store database. Store 1.0 allows for full backups only. Store 2.0 allows for partial backups as well as full backups. It also allows you to specify a backup directory. However, you can specify a backup directory only when backing up the data of the Agent Store or Remote Monitor Store service on the host where the backup command is being executed. For details on partial backups, see [9.3.4 Partially backing up performance data \(Store 2.0\)](#).

### 9.3.2 Backing up and restoring the event data

#### (1) Backing up the event data

1. Log on to the PFM - Manager host.
2. Execute the `jpctool service list` command, and make sure that the services have started.  
Make sure that the Name Server, Master Manager, and Master Store services are running.

For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool db backup` command.

When Running on a Non-Cluster System:

For example, to back up the event data for the Master Store service with the service ID PS1001 in the PFM - Manager Store database, execute the command as follows:

```
jpctool db backup -id PS1001
```

When Running on a Logical Host:

For example, to back up the event data for the Master Store service with the service ID PS1001 in the PFM - Manager Store database on a logical host, execute the command as follows:

```
jpctool db backup -id PS1001 -lhost logical-host-name
```

By default, executing this command creates the backup file named `PA.DB` in the backup directory.

**Table 9–33: Event data backup files**

Conditions			Files to be backed up
Non-cluster system	PFM - Manager host	In Windows	<i>installation-folder</i> \mgr\store\backup\generation-number#\PA.DB
		In UNIX	<i>/opt/jplpc/mgr/store/backup/generation-number#</i> /PA.DB
Cluster system	Shared disk	In Windows	<i>environment-directory</i> \jplpc\mgr\store\backup\generation-number#\PA.DB
		In UNIX	<i>environment-directory</i> /jplpc/mgr/store/backup/generation-number#/PA.DB

# The generation number is assigned in ascending order from 01. The maximum generation number is the value specified in the Backup Save in the `jpcto.ini` file. By default, the maximum generation number is 05.

For further details on the `jpctool db backup` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*. For details on service IDs, see the section that describes service naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

## (2) Restoring event data

1. Log on to the PFM - Manager host.

2. Execute the `jpccspm stop` command to stop the PFM - Manager service.

For details on how to stop the PFM - Manager service, see [1.3 Stopping services](#). For further details on the `jpccspm stop` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Check the storage location for the backup file.

For details on the default backup destinations for event data, see [Table 9-33 Event data backup files](#).

4. Execute the `jpctool db restore` command.

When Running on a Non-Cluster System:

For example, execute the following command to restore the event data in `installation-folder\mgr\store\backup\01`. (Manager indicates the service key for PFM - Manager):

```
jpctool db restore -key Manager -d "installation-folder\mgr\store\backup\01"
```

When Running on a Cluster System:

For example, execute the following command to restore the event data in *environment-directory\jp1pc\mgr\store\backup\01* on the logical host *jp1-ha1*. (*Manager* indicates the service key for PFM - Manager):

```
jpctool db restore -key Manager -d "environment-directory\jp1pc\mgr\store\backup\01" -lhost jp1-ha1
```

For further details on the `jpctool db restore` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

5. Execute the `jpccspm start` command to start the PFM - Manager services.

Start the PFM - Manager services.

For details on how to start the PFM - Manager services, see [1.2 Starting services](#). For further details on the `jpccspm start` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

Note:

Restoring event data sometimes causes a delay in restarting the services, because the index of the database has to be rebuilt when the services start up again.

### 9.3.3 Backing up and restoring the performance data

#### (1) Backing up the performance data

1. Log on to the PFM - Manager host.
2. Execute the `jpctool service list` command, and make sure that the services have started.  
Make sure that the Name Server, Master Manager, and Agent Store or Remote Monitor Store services, which manage the performance data to be backed up, have started.  
For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

3. Execute the `jpctool db backup` command.

When Running on a Non-Cluster System:

For example, execute the following command when you want the performance data in the Store database of PFM - Agent for Oracle on the *host02* host to be backed up:

```
jpctool db backup -id OS* -host host02
```

When Running on a Cluster System:

For example, execute the following command when you want the performance data in the Store database of PFM - Agent for Oracle on the *jp1-ha2* logical host to be backed up:

```
jpctool db backup -id OS* -lhost jp1-ha2
```

By default, executing the command creates a backup file named *database-ID . DB* in the backup directory.

Table 9–34: Performance data backup files

Conditions			Files to be backed up
Non-cluster system	PFM - Agent or PFM - RM host	In Windows	<i>installation-folder\xxx<sup>#1</sup>\store\instance-name<sup>#2</sup>\backup\generation-number<sup>#3</sup>\database-ID<sup>#4</sup>.DB</i>
		In UNIX	<i>/opt/jp1pc/xxx<sup>#1</sup>/store/instance-name<sup>#2</sup>/backup/generation-number<sup>#3</sup>/database-ID<sup>#4</sup>.DB</i>
Cluster system	Shared disk	In Windows	<i>environment-directory\jp1pc\xxx<sup>#1</sup>\store\instance-name<sup>#2</sup>\backup\generation-number<sup>#3</sup>\database-ID<sup>#4</sup>.DB</i>
		In UNIX	<i>environment-directory/jp1pc/xxx<sup>#1</sup>/store/instance-name<sup>#2</sup>/backup/generation-number<sup>#3</sup>/database-ID<sup>#4</sup>.DB</i>

#1

xxx indicates the service key of each PFM - Agent or PFM - RM. For details on the PFM - Agent or PFM - RM service keys, see the description of the naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

#2

Created when PFM - Agent or PFM - RM is in the instance environment.

#3

The generation number is assigned in ascending order from 01. The maximum generation number is the value specified in the Backup Save in the `jpcto.ini` file. By default, the maximum generation number is 05.

#4

The following are the database IDs:

- PI: Database for records of the PI record type
- PD: Database for records of the PD record type
- PL: Database for records of the PL record type

However, you can also back up the performance data on a host where PFM - Agent or PFM - RM is installed. To perform backup on a host where PFM - Agent or PFM - RM is installed, specify the `-alone` or `-direct` option in the `jpctool db backup` command.

For further details on the `jpctool db backup` command, see the chapter that describes the command in the manual *JPI/Performance Management Reference*.

Note:

If you execute the `jpctool db backup` command while any of the following commands or processes are underway, the `jpctool db backup` command might fail if it targets the same Master Store service, Agent Store service, or Remote Monitor Store service as the other command or process:

- `jpctool db backup`
- `jpctool db dump`
- `jpctool db clear`
- `jpctool db import`
- `jpctool db restore`
- Data storage by the Agent Store service or Remote Monitor Store service
- Displaying a historical report

In this scenario, try executing the `jpctool db backup` command again.

## (2) Restoring the performance data

1. Log on to the PFM - Agent or PFM - RM host that stores the backup file.
2. Execute the `jpcspm stop` command to stop the PFM - Agent or PFM - RM service.  
For details on how to stop the PFM - Agent or PFM - RM service, see [1.3 Stopping services](#). For further details on the `jpcspm stop` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.
3. Check the storage location for the backup file.  
For details on the default backup destinations for performance data, see [Table 9-34 Performance data backup files](#).
4. Execute the `jpctool db restore` command.

When Running on a Non-Cluster System:

For example, execute the following command when you want the performance data in the `oracleA` instance of PFM - Agent for Oracle on the `installation-folder\agto\store\oracleA\backup\01` to be restored: Oracle indicates the service key for PFM - Agent.

```
jpctool db restore -key Oracle -d "installation-folder\agto\store\oracleA\backup\01" -inst oracleA
```

When Running on a Cluster System:

For example, execute the following command when you want the performance data in the `oracleA` instance of PFM - Agent for Oracle on the `environment-directory\jplpc\agto\store\oracleA\backup\01` of the `jp1-ha2` logical host to be restored (Oracle indicates the service key for PFM - Agent):

```
jpctool db restore -key Oracle -d "installation-folder\agto\store\oracleA\backup\01" -lhost jp1-ha2 -inst oracleA
```

For further details on the `jpctool db restore` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*. For details on the service key for each PFM - Agent or PFM - RM instance, see the section that describes naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

5. Execute the `jpcspm start` command to start the PFM - Agent or PFM - RM service.  
For details on how to start the PFM - Agent or PFM - RM service, see [1.2 Starting services](#).  
For further details on the `jpcspm start` command, see the chapter that describes the command in the manual *JP1/Performance Management Reference*.

Note 1:

Restoring performance data sometimes causes a delay in restarting the services, because the index of the database has to be rebuilt when the services are started up again.

Note 2:

Backup data cannot be restored to a Store database that uses different Store version. You can only restore backup data acquired from a database set up to use Store 2.0 to a database that uses Store 2.0. Similarly, you can only restore backup data acquired from a database set up to use Store 1.0 to a database that uses Store version is 1.0.



## 9.3.4 Partially backing up performance data (Store 2.0)

With Store 2.0, you can partially back up performance data. Partial backup is available only while the Agent Store or Remote Monitor Store service is running. Partial backups allow you to accumulate differential data by specifying a past backup directory as the backup destination.

### (1) Range of data subjected to backup

When backing up data, you need to specify the beginning and end of the backup period based on local time as a number of days relative to the execution date of the backup command. In this case, the backup operation applies to the data from three days to one day prior to execution of the backup command. When the backup command is executed, the data from the specified backup period is backed up to the backup directory.

Because the PD and PL databases and the per-minute and hourly records in the PI database are stored in multiple files that each contains the performance data for a particular day, the unit databases for the specified dates are backed up. On the other hand, in the PI database, different records are stored in the following different files: daily and weekly records in the weekly file, monthly records in the monthly file, and yearly records in the yearly file. This means that the backed-up data contains even the data that falls outside the period defined by the start date and end date of records.

#:

Because the Store database runs on Greenwich Mean Time (GMT), when your system lies outside the GMT zone, you will notice the deviation of the collected data range from the specified date.

### (2) Creating a partial backup of data every $n$ day(s)

Because the Store database runs on GMT, data collection must start from  $n + 1$  days before, taking into account the difference between GMT and local time.

Example:

```
jpctool db backup -id ZS1inst1[host1] -d d:\backup01# -partial (n+1),1
```

# D:\backup01 indicates the backup directory.

### (3) Backing up the most recent data possible

To back up the latest database, use the following command:

Example: Backing up the latest version of the database

```
jpctool db backup -id ZS1inst1[host1] -d d:\backup01# -partial  
startday, endday
```

# D:\backup01 indicates the backup directory.

The recommended values to be specified for *startday* and *endday* of the `-partial` option vary depending on the local time setting.

For example, the table below shows the *startday* and *endday* values recommended for three different local time settings (namely, GMT, GMT-9:00, and GMT+9:00) as well as the actual backup data collection period in each case. This example assumes that you are executing the back up command on March 17 (Thursday) to back up data collected during a period from 0:00 to 23:59 on the previous day, March 16 (Wednesday).

Table 9–35: Recommended values for the -partial option

Local time setting	Recommended values to be specified for the -partial option		Actual backup data collection period (in local time)
	startday	endday	
GMT	1	1	From 0:00 on March 16 to 23:59 on March 16
GMT-09:00	1	0	From 15:00 on March 15 to the time at which the command is executed
GMT+09:00	2	0	From 9:00 on March 15 to the time at which the command is executed

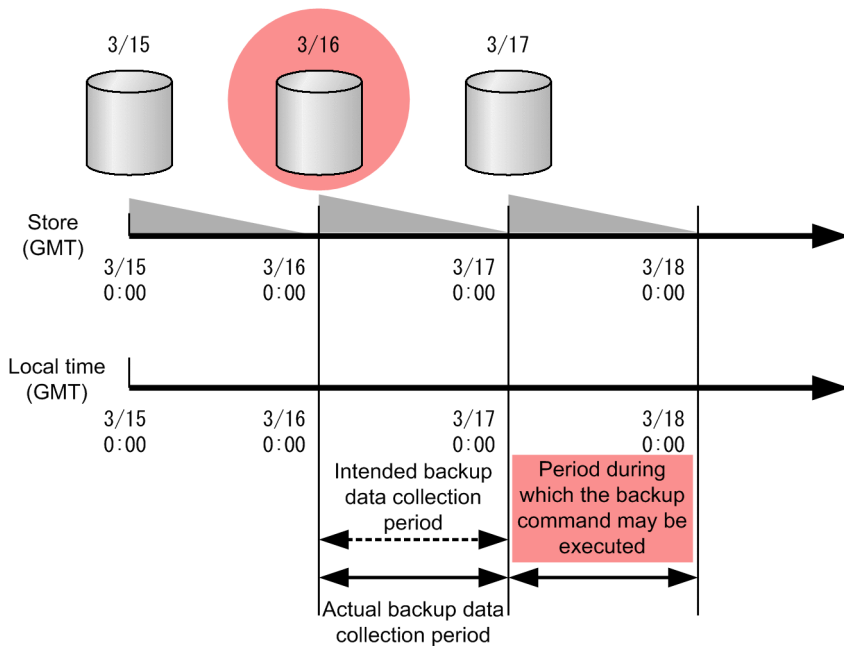
Depending on the time at which the backup command is executed, a backup might not be created. The period during which the backup command may be executed is described below.

**(a) When GMT is set as the local time**

Backup command to be executed:

```
jpctool backup ZSinst1[host1] -partial 1,1
```

Figure 9–2: Period during which the backup command may be executed (when GMT is set as the local time)

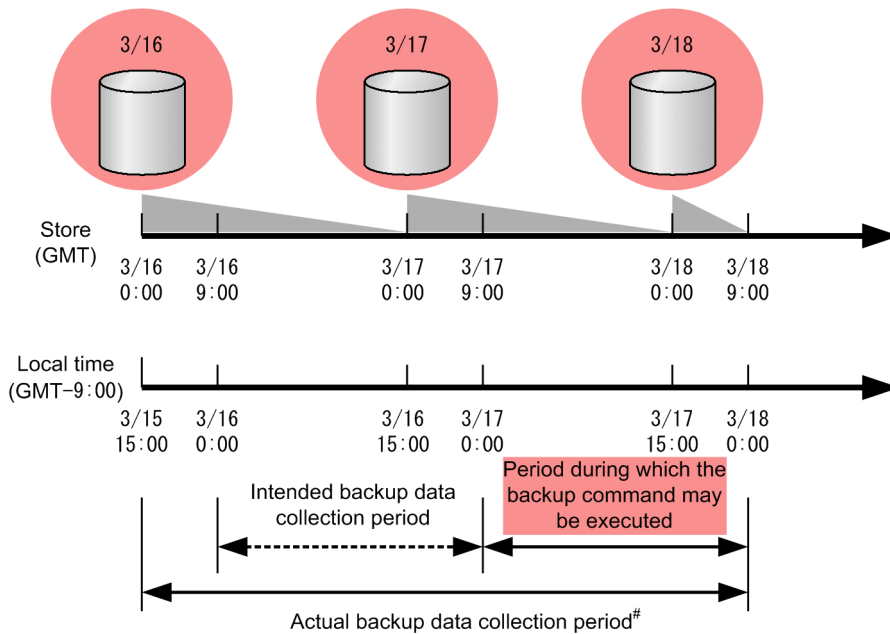


**(b) When GMT-09:00 is set as the local time**

Backup command to be executed:

```
jpctool backup ZSinst1[host1] -partial 1,0
```

Figure 9–3: Period during which the backup command may be executed (When GMT-09:00 is set as the local time)



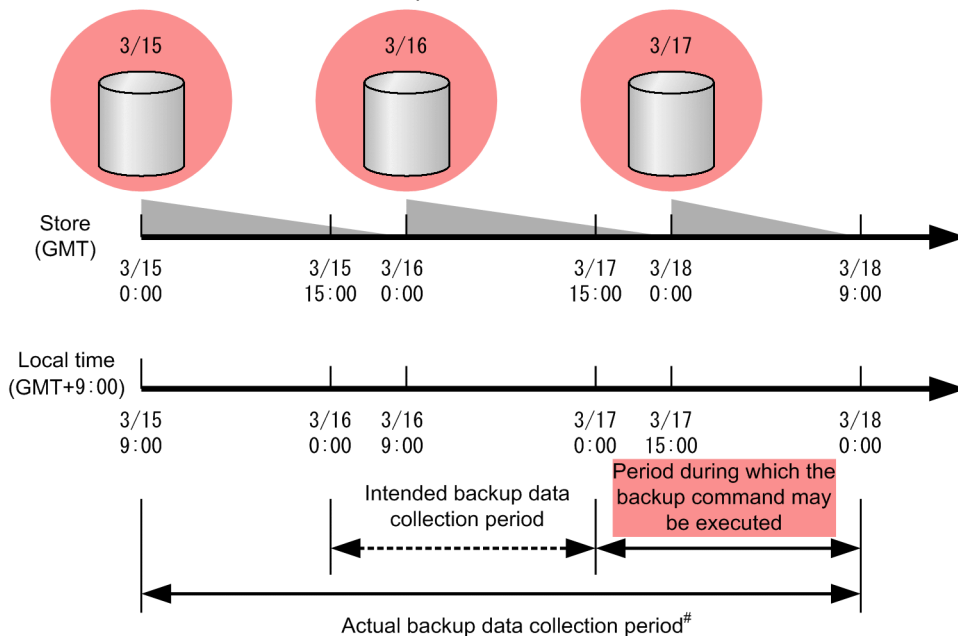
# Data collected during a period from 15:00 on March 15 to the time at which the backup command is executed (in local time) is actually backed up.

### (c) When GMT+09:00 is set as the local time

Backup command to be executed:

```
jpctool backup ZSinst1[host1] -partial 2,0
```

Figure 9–4: Period during which the backup command may be executed (When GMT+09:00 is set as the local time)



# Data collected during a period from 9:00 on March 15 to the time at which the backup command is executed (in local time) is actually backed up.

## (4) Location to which to store partial backups, and the directory and structure of the files to be stored

By default, the command creates backup files with the following names in the backup directory.

Table 9–36: Partial backup files for performance data

Conditions			Files to be backed up
Non-cluster system	PFM - Agent or PFM - RM host	In Windows	Contents of <i>installation-folder\xxx#1\store\instance-name#2\partial\stdatabase-ID#3</i>
		In UNIX	Contents of <i>/opt/jp1pc/xxx#1/store/instance-name#2/partial/stdatabase-ID#3</i>
Cluster system	Shared disk	In Windows	Contents of <i>environment-directory\jp1pc\ xxx#1\store\instance-name#2\partial\stdatabase-ID#3</i>
		In UNIX	Contents of <i>environment-directory/jp1pc/ xxx#1/store/instance-name#2/partial/stdatabase-ID#3</i>

#1

xxx indicates the service key of each PFM - Agent or PFM - RM. For details on the PFM - Agent or PFM - RM service keys, see the description of the naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

Created when PFM - Agent or PFM - RM is in the instance environment.

#3

The following are the database IDs:

PI: Database for records of the PI record type

PD: Database for records of the PD record type

PL: Database for records of the PL record type

The following table describes the directories and file structure used for the files produced by a partial backup:

Table 9–37: Directories and file structure for partial backups

Directory or file	Record type			Format	Min.	Max.	Description
	PI	PD	PL				
STXX	Y	Y	Y	n/a	n/a	n/a	n/a
Summary block	Y	N	N	<i>n</i>	1	6	Summary block (for PI records) 1: Minute 2: Hour 3: Day 4: Week 5: Month 6: Year
Year	Y	Y	Y	<i>YYYY</i>	1900	2027	Year
Month and day	Y	Y	Y	<i>MMDD</i>	0101	1231	Month and day
Generation number	Y	Y	Y	<i>nnn</i>	001	002	Generation number
<i>record-type.DB</i>	Y	Y	Y	n/a	n/a	n/a	Database file for each record type

Legend:

Y: Is an applicable file or directory.

N: Is not an applicable file or directory.

n/a: Not applicable

XX: Database ID

PI: Database for records of the PI record type

PD: Database for records of the PD record type

PL: Database for records of the PL record type

## 9.4 Migrating Performance Management data to another system

This section describes the steps required to migrate definition information and operation monitoring data from one Performance Management system to another system on a machine with a different host name.

### 9.4.1 Data that can be migrated

The following table lists the data that can be migrated between Performance Management systems.

Table 9–38: Data that can be migrated

Data requiring backup		Can be migrated
Definition information	Report definition information	Y
	Alarm definition information	Y
	Business group definition information	Y
	Service definition information	N
	Bookmark definition information	N
	Process monitoring definition template definition information	Y
Operation monitoring data	Event data	N
	Performance data	N

Legend:

Y: Can be migrated.

N: Cannot be migrated.

### 9.4.2 Migrating data from one Performance Management system to another

#### (1) Migrating report definitions

1. Export report definitions from an instance of PFM - Web Console that monitors the migration-source Performance Management system.
2. Import the exported report definitions into an instance of PFM - Web Console that monitors the migration-target Performance Management system.
3. Amend the imported report definitions to suit the monitoring conditions of the migration-target system.

For details about how to import and export report definitions, see [9.2.8 Backing up and restoring a report definition](#).

#### (2) Migrating alarm definitions

1. Export alarm definitions from PFM - Manager or PFM - Web Console in the migration-source Performance Management system.

2. Import the exported alarm definitions into a PFM - Manager or PFM - Web Console host in the migration-target Performance Management system.
3. Amend the imported alarm definitions to suit the monitoring conditions of the migration-target system.

For details about how to import and export alarm definitions, see [9.2.9 Backing up and restoring an alarm definition](#).

### **(3) Migrating business group definitions**

1. Export business group definitions from PFM - Manager in the migration-source Performance Management system.
2. Import the exported business group definitions into PFM - Manager in the migration-target Performance Management system.

For details about how to import and export business group definitions, see [9.2.10 Backing up and restoring a business group definition](#).

### **(4) Migrating process monitoring definition templates**

1. Back up the process monitoring template definitions used by PFM - Web Console to monitor the migration-source Performance Management system.
2. Restore the backed-up process monitoring template definitions to PFM - Web Console in the migration-target Performance Management system.

For details about how to import and export process monitoring definition templates, see [9.2.13 Backing up and restoring a process monitoring definition template](#).

# 10

## Cluster System Configuration and Operation

This chapter describes the installation and setup methods, as well as the flow of processing, for running Performance Management in a cluster system.



## 10.1 Overview and design of cluster systems

---

This section describes an overview of cluster systems and the architecture design for running Performance Management in a cluster system.

### 10.1.1 Overview of cluster systems

Cluster systems are used to link multiple servers and run them as a single system. Cluster systems can be generally classified in the following two types:

- HA (High Availability) cluster systems
- Load-balancing cluster systems

Note:

In this section, *cluster system* refers to an HA cluster system.

#### (1) HA cluster systems

The purpose of *HA cluster systems* is to enhance the availability of the entire system. HA cluster systems are often used in application servers and database servers for mission-critical systems that require high availability.

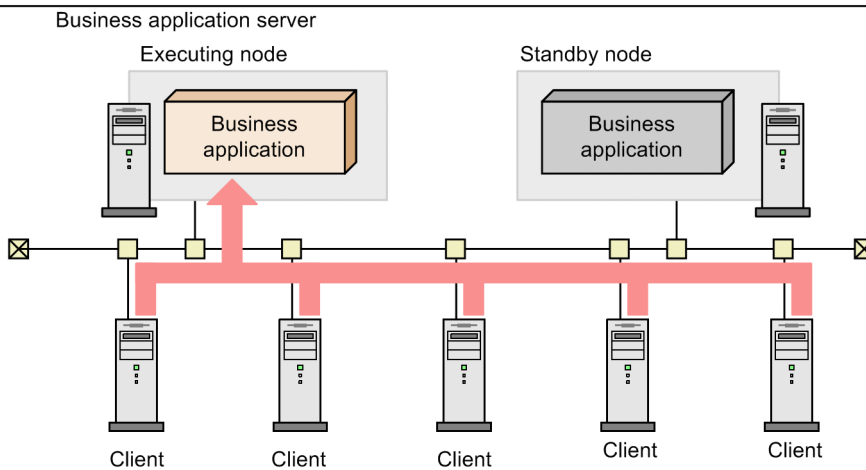
HA cluster systems include a redundant server for each server that makes up the system. In an HA cluster system, if problems occur in a server that is executing a job, a different server that has been standing by will continue the processing of the job. This is called *failover*.

Of the server systems in a cluster system, the system that is executing jobs is called the *executing node*, and the system that is standing by ready to take over processing when a problem occurs on the executing node is called the *standby node*.

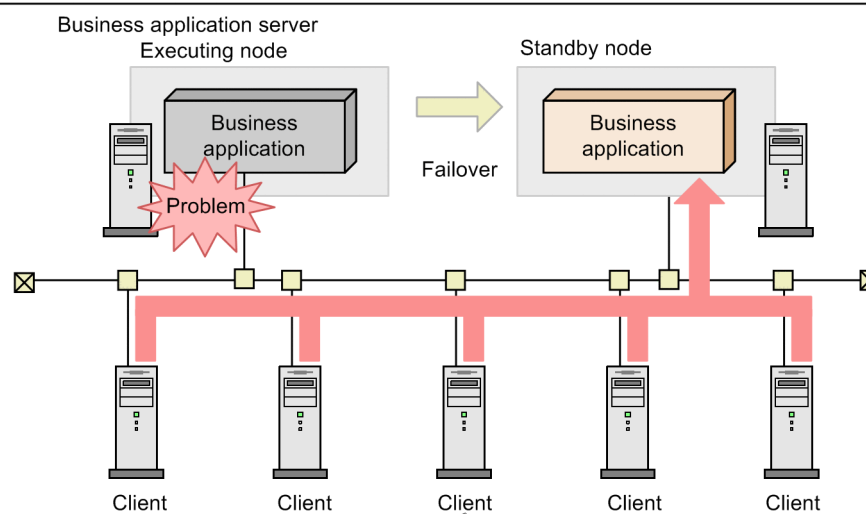
The following figure shows the flow of access when a problem occurs on the executing node.

Figure 10–1: Flow of access when a problem occurs on the executing node of an HA cluster system

Access when the executing node is normal



Access when there is a problem on the executing node



The client can access the business application at any time regardless of if there is a problem with the server.

- Legend:
- : Access flow
  - : Failover flow
  - : Applications being executed
  - : Applications in standby

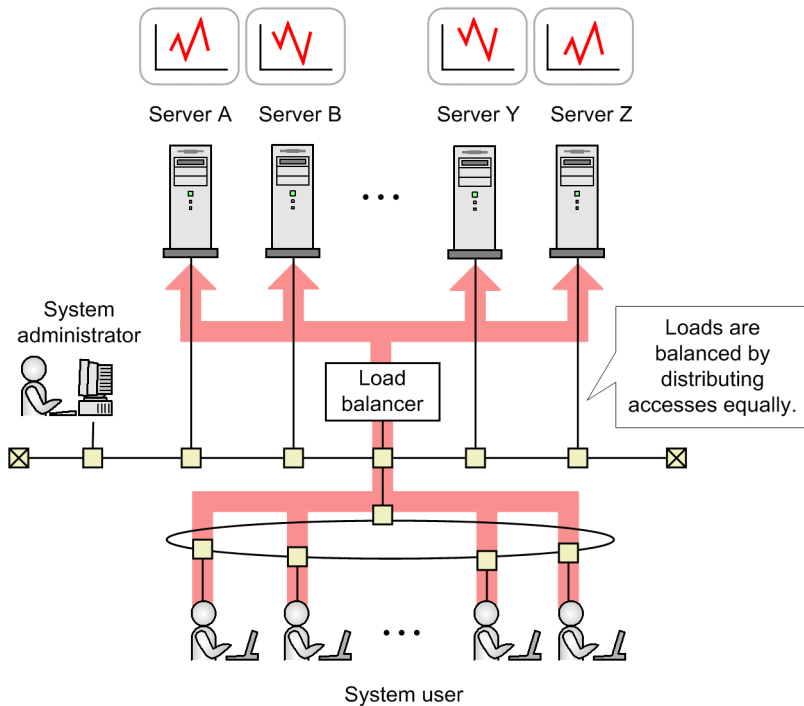
The software that controls the entire HA cluster system is called the *cluster software*. The cluster software always monitors the servers and, if a problem occurs, automatically switches the server for executing a job from that on the executing node to that on the standby node. Therefore, cluster systems are also called *node switching systems*.

## (2) Load-balancing cluster systems

*Load-balancing cluster systems* balance the processing load across multiple servers. They are often used in systems that require high processing performance.

Load-balancing cluster systems place multiple servers in parallel to balance processes, keep the load on any single server low, and increase the processing performance of the entire system. Even if a problem occurs on a server, switching processes to a different node can enhance the availability of the system.

Figure 10–2: Flow of access in a load-balancing cluster system



Supplemental information:

Examples of load-balancing cluster systems include systems that balance servers to receive requests, such as Web systems, and Oracle Real Application Cluster systems. In addition, business applications that run on load-balancing cluster systems require programs that can allocate processes to multiple nodes.

## 10.1.2 Designing a cluster configuration

Performance Management can monitor operations in a cluster system.

### (1) Examining the configuration in HA cluster systems

Running the Performance Management programs on the logical host environment of an HA cluster system is referred to as *logical host use*.

#### (a) Cluster configuration of PFM - Manager

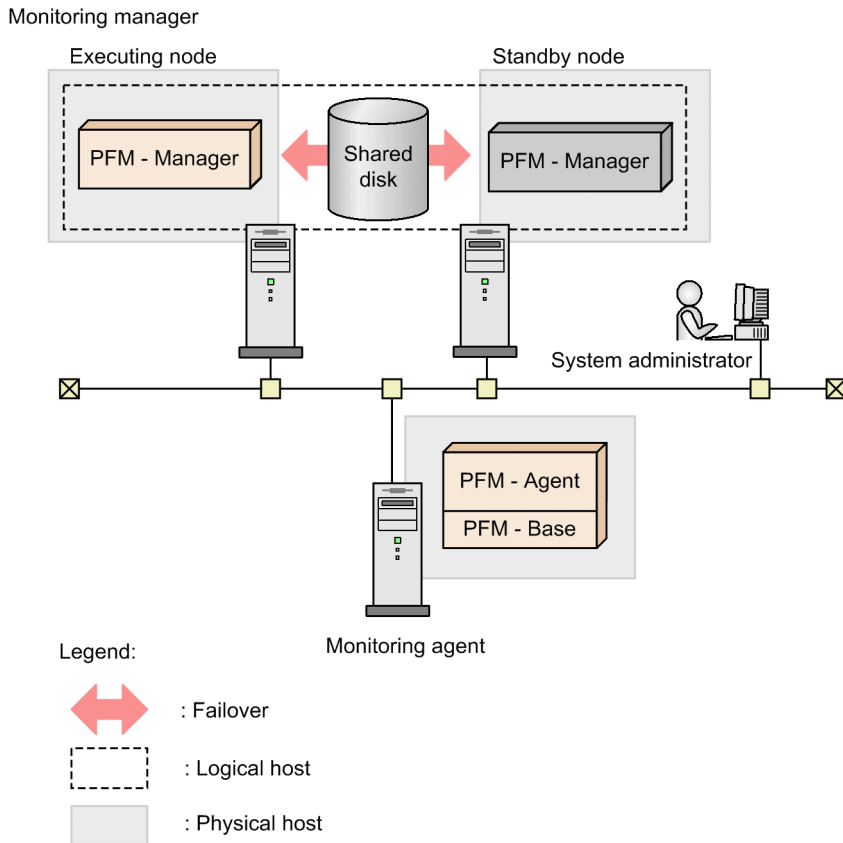
PFM - Manager can run on a logical host of a cluster system that has an active-standby configuration.

Even if a problem occurs on the executing node where PFM - Manager is executed, operation monitoring is continued by failing over to the standby node.

When PFM - Manager is used on a logical host, definition information and event data are stored on a shared disk and inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows the configuration when using PFM - Manager on a logical host.

Figure 10–3: Cluster configuration of PFM - Manager



Only a single instance of PFM - Manager can be executed at a time on a single node.

### (b) Cluster configuration of PFM - Web Console

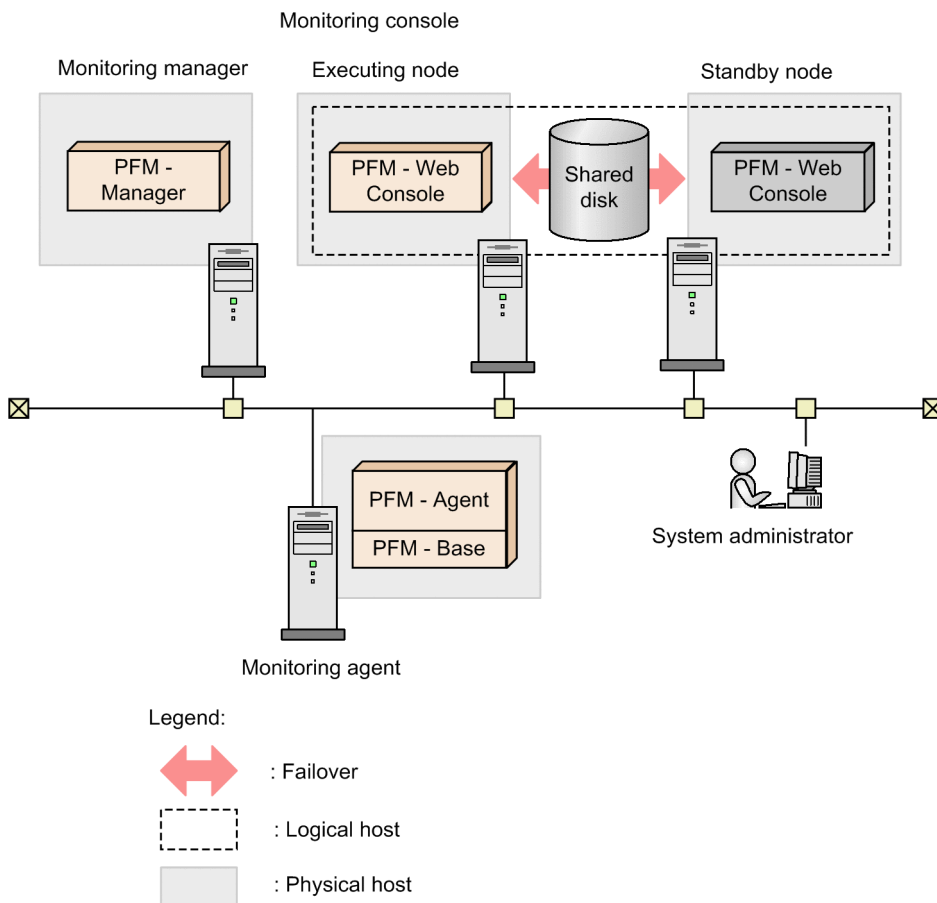
PFM - Web Console can run on a logical host of a cluster system that has an active-standby configuration.

Even if a problem occurs on the executing node where PFM - Web Console is executed, operation monitoring is continued by failing over to the standby node.

If PFM - Web Console is used on a logical host, bookmark definitions are stored on a shared disks so that such information can be inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows the configuration when using PFM - Web Console on a logical host.

Figure 10–4: Cluster configuration of PFM - Web Console



Only a single instance of PFM - Web Console can be executed at a time on a single node.

### (c) Cluster configuration of PFM - Base

PFM - Base is compatible with cluster systems that have an active-active configuration. PFM - Base can be used on a logical host if PFM - Agent or PFM - RM is installed on the same logical host.

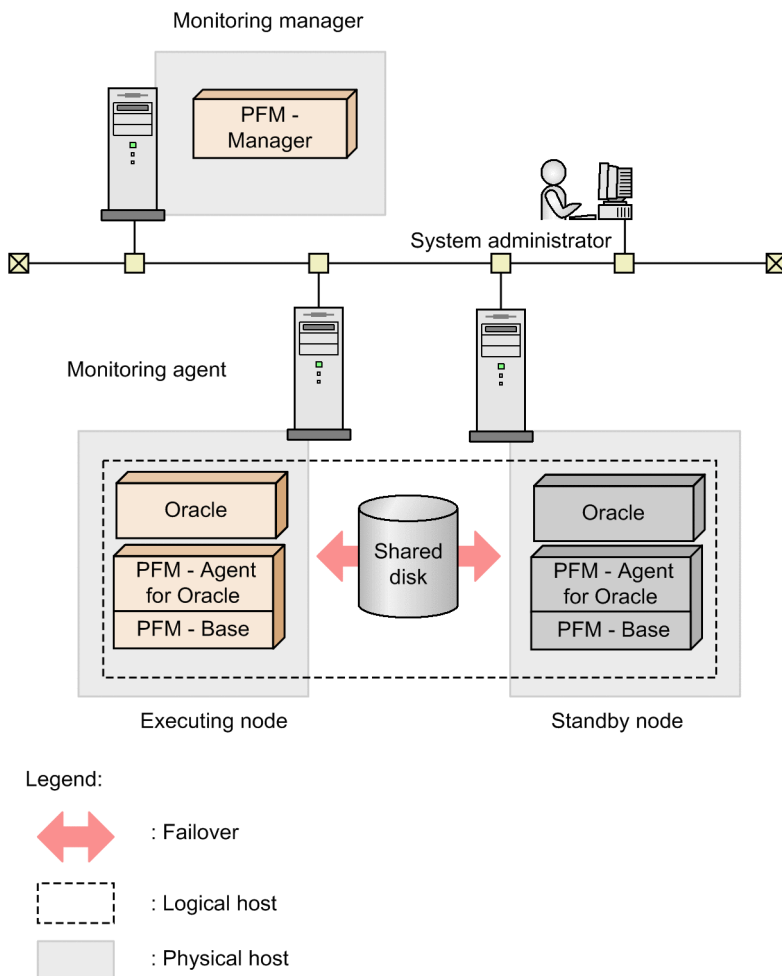
### (d) Cluster configuration of PFM - Agent

Different cluster systems support different PFM - Agents. When the program to be monitored is running in a logical host environment, only some types of PFM - Agents will be able to run in that logical host environment.

If PFM - Agent is used on a logical host, definition information and performance data are stored on shared disks so that they can be inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows an example of a configuration that monitors an Oracle cluster system with PFM - Agent for Oracle on a logical host.

Figure 10–5: Cluster configuration for PFM - Agent (PFM - Agent for Oracle)



Supplemental information:

PFM - Agent is used in a configuration that is compatible with the application that is being monitored. Therefore, there are some PFM - Agents that are used on a logical host and others that are used on a physical host. For example, PFM - Agent for Oracle is used on a logical host since PFM - Agent for Oracle monitors Oracle in a cluster configuration, on the other hand, PFM - Agent for Platform is used on a physical host to monitor the OSs on each node since PFM - Agent for Platform monitors OS performances. For details, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent manual.

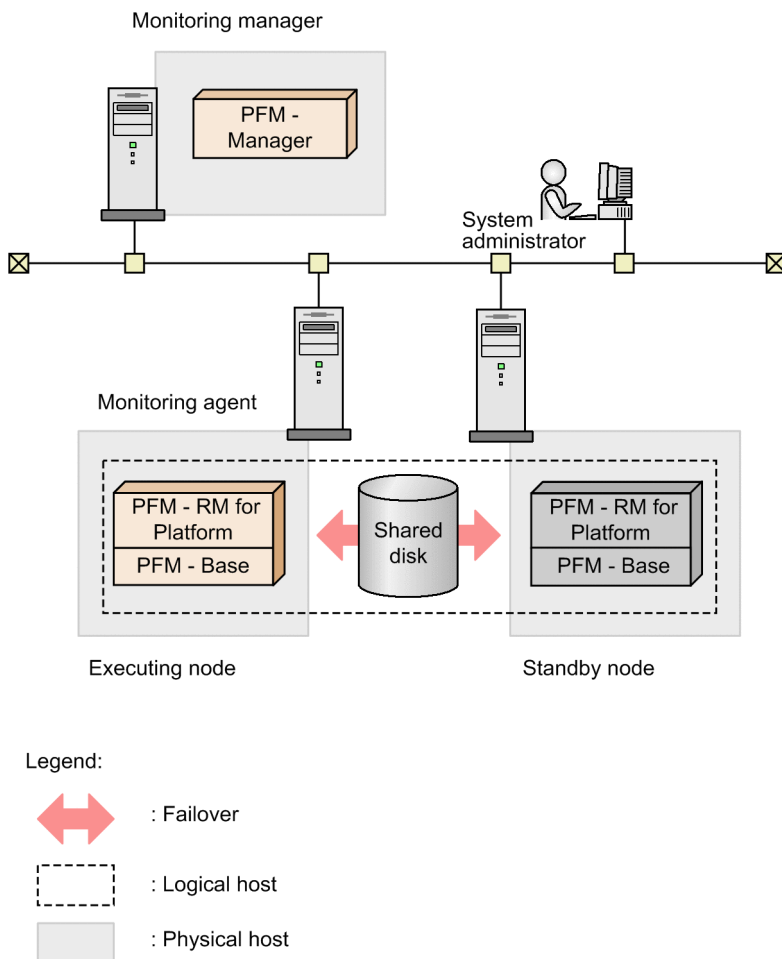
**(e) Cluster configuration of PFM - RM**

Different cluster systems support different PFM - RM products. Some PFM - RM products can also be used on a logical host. For details on whether the PFM - RM product you are using can be used in a cluster system, see the applicable PFM - RM manual.

If PFM - RM is used on a logical host, definition information and performance data are stored on the shared disks so that they can be inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows an example of the configuration when using PFM - RM for Platform on a logical host.

Figure 10–6: Cluster configuration of PFM - RM (PFM - RM for Platform)



## (2) Examining the configuration in load-balancing cluster systems

### (a) Cluster configuration of PFM - Manager

The PFM - Manager processing cannot be balanced across multiple nodes.

PFM - Manager must be used on a physical host or HA cluster system, rather than a load-balancing cluster system.

### (b) Cluster configuration of PFM - Web Console

The PFM - Web Console processing cannot be balanced across multiple nodes.

PFM - Web Console must be used on a physical host or HA cluster system, rather than a load-balancing cluster system.

### (c) Cluster configuration of PFM - Base

Conforms to the configuration of PFM - Agent or PFM - RM on the same host.

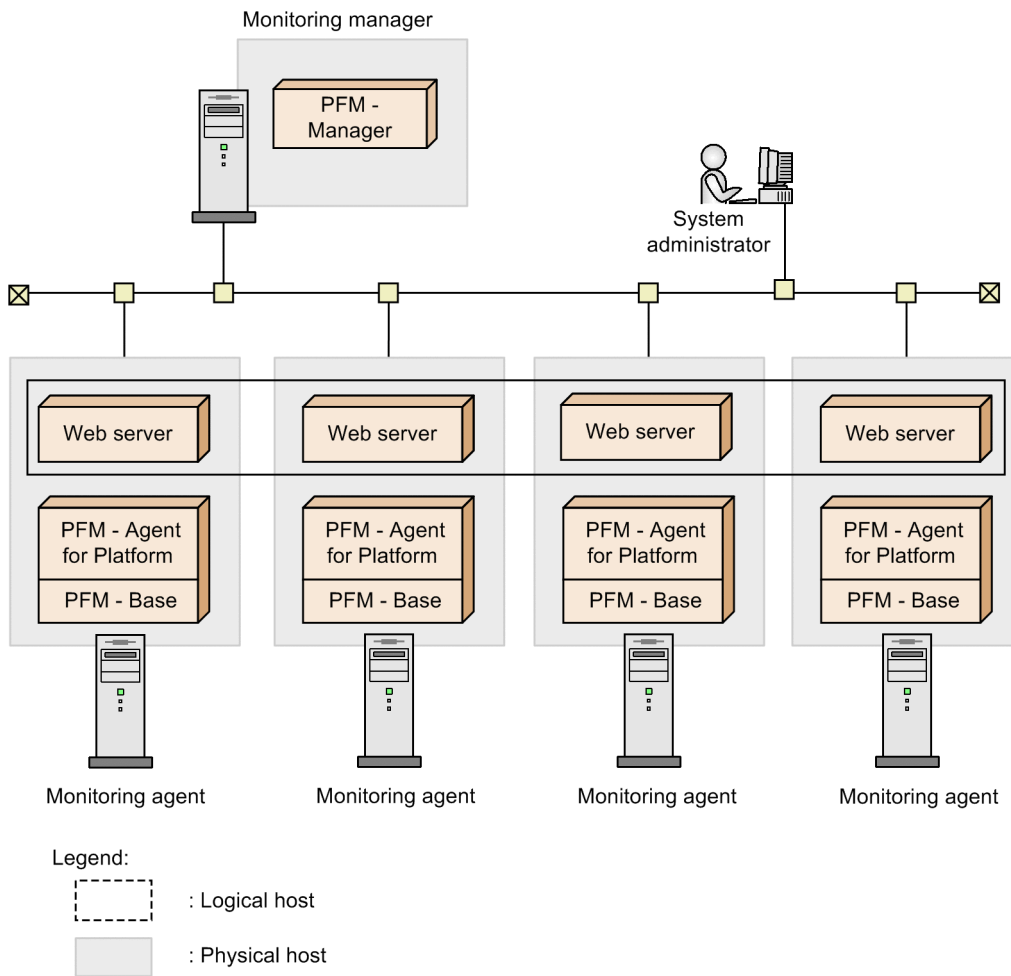
### (d) Cluster configuration of PFM - Agent

This subsection describes how PFM - Agent for Platform is used on each node of a load-balancing cluster system.

PFM - Agent for Platform monitors OS performances. Therefore, even in a cluster system, PFM - Agent for Platform is executed on physical hosts to monitor the OSs on each physical host. PFM - Agent for Platform must be used in the

same manner as a system that is not a cluster system. Even when used in a cluster system, PFM - Agent for Platform is not registered in the cluster software.

Figure 10–7: Cluster configuration of PFM - Agent (PFM - Agent for Platform)



For details on the cluster configuration of PFM - Agents, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent manual.

### (e) Cluster configuration of PFM - RM

Depending on the PFM - RM product you are using, it might not be possible to use PFM - RM in a load-balancing cluster system. For details, see the chapters that describe operations on cluster systems in the appropriate PFM - RM manual.

## 10.1.3 Planning the network configuration

When Performance Management is used on a logical host, it is necessary to configure a network so that communication is possible by using logical host names and logical IP addresses.

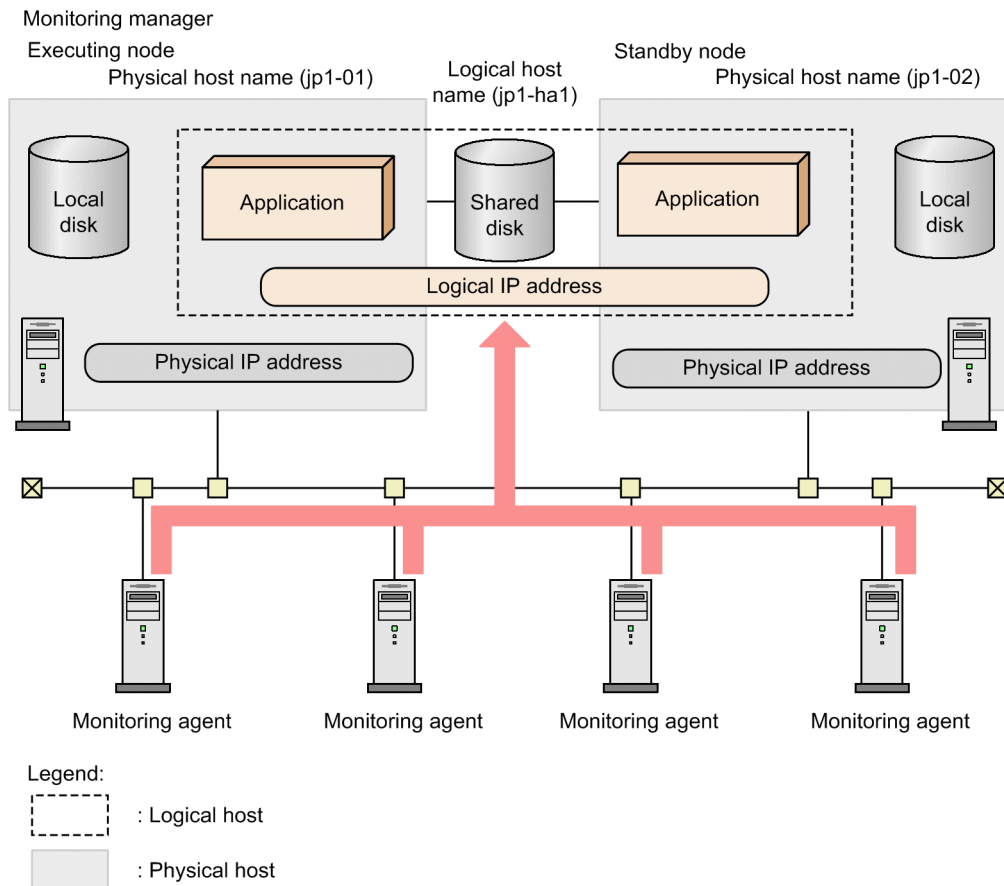
A *logical host* is a logical node that is controlled by cluster software and a unit of failover. A logical host has a *logical host name* and a *logical IP address*. Applications store data on shared disks and communicate via logical IP addresses, so that they are not dependant on physical nodes and can perform failover.



A *physical host* is a physical node. The host name used by a physical host (the host name displayed by the `hostname` command or `uname -n` command) is called the *physical host name*, and the IP address associated with the physical host name is called the *physical IP address*.

The following figure shows an overview of physical and logical hosts.

Figure 10–8: Overview of physical and logical hosts



## 10.1.4 Planning the data configuration

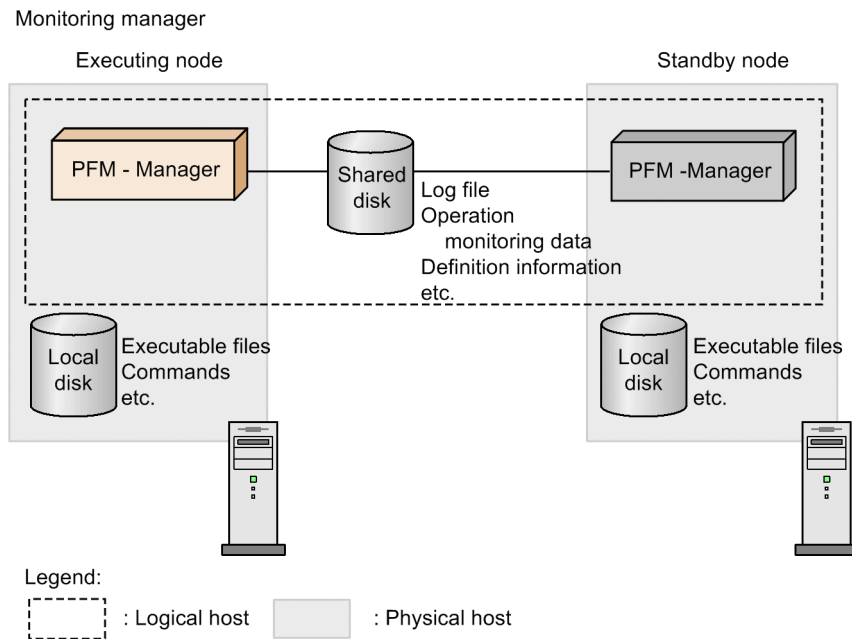
When you use Performance Management on a logical host, you need to consider the data requirements for the shared disk, over and above the data requirements for Performance Management in a non-cluster system.

Each cluster system has a *shared disk* that is shared between the executing node and standby node when a failover occurs. In addition, each executing node and standby node has *local disk* that are specific to each physical host and cannot be taken over by a different node.

With Performance Management, when a logical host environment is set up, an *environment directory* is created on the shared disk. This environment directory stores the definition files and operation monitoring data required for switching nodes when a failover occurs. The execution files and commands required to run Performance Management are stored on local disks.

The following figure shows the data configuration for Performance Management when used on a logical host.

Figure 10–9: Data configuration for Performance Management when using a logical host



Supplemental information:

Some definition information and log files are located on local disks.

For details on the formula used to calculate the disk capacity required for logical host operation with Performance Management, see the sections that describe the exclusively occupied disk space when running on a cluster system in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

### 10.1.5 Planning operation in a cluster system

Considerations for what security policy to use for managing Performance Management users and what items to monitor are the same as for non-cluster systems.

However, some naming rules for service names and process names, and some setting methods for executing actions on logical hosts when alarm events occur are different from those used in non-cluster systems. For details, see [10.6.1\(3\) Service names](#) and [10.6.6 Performing realtime operation monitoring by alarms in a cluster system](#).

### 10.1.6 Planning the failover method

When an error occurs in PFM - Agent or PFM - RM, and the node on which the program is running fails over, the business applications running on the logical host monitored by the PFM - Agent or PFM - RM might be affected. Therefore, you should decide whether nodes should fail over when a problem occurs in PFM - Agent or PFM - RM.

Supplemental information:

To avoid affecting business operations, you might use the following operation policy: "If a problem occurs in PFM - Agent or PFM - RM, the system will attempt to restart PFM - Agent or PFM - RM on that node, but the problem will not trigger a failover."

## 10.2 Configuration in a cluster system (in Windows)

---

### 10.2.1 Before installation and setup

#### (1) Prerequisite conditions

##### (a) Cluster system

Make sure that the following conditions are satisfied:

- The cluster system is controlled by cluster software.
- Settings are made so that the starting and stopping of Performance Management used on a logical host are controlled by cluster software.
- Reporting errors to Microsoft is disabled in the executing node and the standby node.  
If an application error occurs in Windows, a dialog box for reporting the error to Microsoft sometimes appears. If this dialog box is displayed, a failover might not be performed, therefore, you need to suppress such error notification. If error notification is not already disabled, specify the settings as follows.

In Windows Server 2008:

1. In the Control Panel, choose **System and Security**, **Action Center**, and then **Maintenance**.
2. Under **Check for solutions to problem reports**, click **Settings**.
3. In the Choose when to check for solutions to problem reports dialog box, select **Never check for solutions**.
4. Click **OK**.

In Windows Server 2012:

1. In the Control Panel, choose **System and Security**, **Action Center**, and then **Maintenance**.
2. Under **Check for solutions to problem reports**, click **Settings**.
3. In the **Windows Error Reporting Configuration** dialog box, select **I don't want to participate, and don't ask me again**.
4. Click **OK**.

In Windows Server 2016:

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**.

##### (b) Shared disks

Make sure that the following conditions are satisfied:

- Each logical host has a shared disk, and the disk can be taken over by from the executing node by the standby node.

- Shared disks are physically connected to each node via Fibre Channel or SCSI. Configurations in which the shared disk is a network drive or disk replicated over a network are not supported.
- When a failover occurs, if some processes are still using the shared disks, make sure it is still possible to force shared disks offline via cluster software or by other means and perform a failover.
- If multiple Performance Management programs are executed on a single logical host, make sure the directory names for the shared disks are the same. For Store databases, make sure the storage destination can be changed to allow storage in a different directory on the same shared disk.

### (c) Logical host name and logical IP address

Make sure that the following conditions are satisfied:

- There is a logical host name and corresponding logical IP address for each logical host, and switching from the executing node to the standby node can be performed.
- The logical host and logical IP address are set in the `hosts` file and on the name server.
- If using a DNS a logical host name is specified without a domain name, instead of by using a FQDN.
- Each physical host name and logical host name is unique within the system.

#### Important

Regarding logical host names:

- Do not use a physical host name (a host name displayed using the `hostname` command) for a logical host name. Otherwise, normal communication processing might be prevented.
- Logical host names must consist of from 1 to 32 bytes alphanumeric characters.
- `localhost`, an IP addresses, or a hyphen (-) cannot be used for a logical host name.

### (d) Configuring the language environment

In Windows, there are multiple locations where the language environment is configured. The configurations must be consistent on all executing nodes and standby nodes.

For details about how to set up a language environment, see the section on setting up a language environment in the *JP1/Performance Management Planning and Configuration Guide*.

## (2) Checking the setup environment

In addition to the environment information normally required to set up Performance Management, the following information is required to set up Performance Management used on a logical host.

Table 10–1: Information required to set up PFM - Manager to be used on a logical host (in Windows)

Item	Example
Logical host name	<code>jp1-ha1</code>
Logical IP address	<code>172.16.92.100</code>
Shared disk	<code>S:\jp1\</code>

If multiple instances of Performance Management that use a single logical host, each instance uses the directory of the same shared disk.

### **(3) Notes about upgrading when a logical host is used**

To upgrade PFM - Manager on a logical host, you must place a shared disk online on either an executing or a standby node.

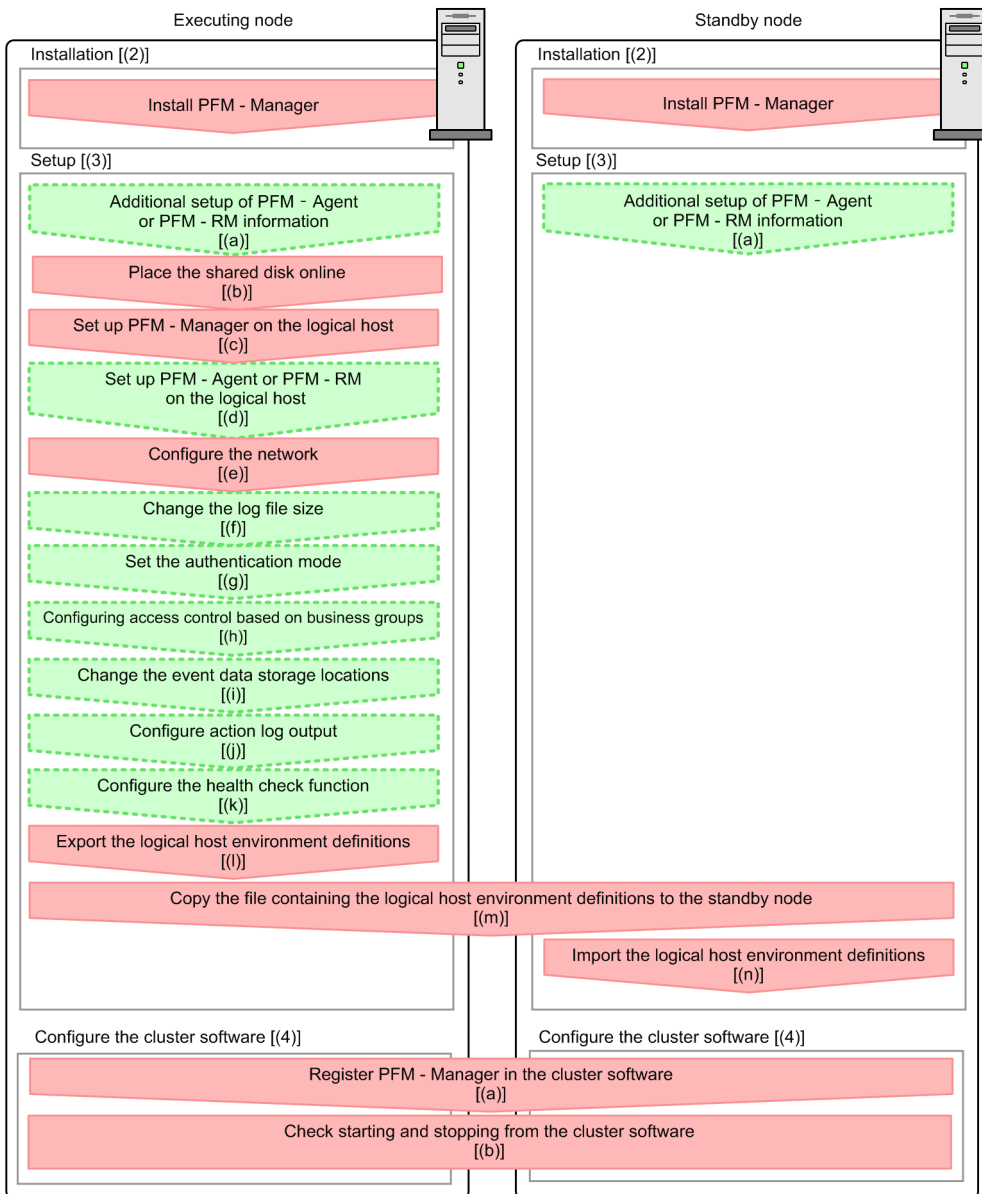
However, there is no need to place a shared disk online to upgrade PFM - Web Console in a cluster environment.

## **10.2.2 Installing and setting up PFM - Manager**

### **(1) Process flow for installation and setup**

The following figure shows the process flow for installation and setup of PFM - Manager used on a logical host.

Figure 10–10: Process flow for installation and setup of PFM - Manager used on a logical host (in Windows)



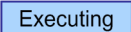

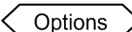
Legend:  
 : Mandatory step    : Optional step    [ ] : See the indicated section

### Important

- When PFM - Manager in a logical host environment is set up, PFM - Manager on the physical host environment can no longer be executed. However, the Action Handler service can still be executed, because it uses PFM - Agent or PFM - RM in the physical host environment.  
 When unsetup is performed on PFM - Manager in a logical host environment, PFM - Manager in the physical host environment can once again be executed.
- When PFM - Manager is set up in a logical host environment, the logical host environment inherits the PFM - Manager definitions from the physical host environment. However, the content of the Store database is not inherited. If unsetup is performed on PFM - Manager in the logical host environment, the definitions for the logical host environment and the Store database are deleted, and therefore switching to the physical host environment is not possible.

- Do not manually set `JPC_HOSTNAME` as an environment variable, because `JPC_HOSTNAME` is used by Performance Management as an environment variable. If you specify this setting, Performance Management will not run correctly.
- When you set up a new instance of PFM - Manager version 09-00 or later in a logical host environment, it inherits the health check settings of the physical host environment. Modify the settings as needed.
- In a logical host environment, the function for setting monitoring-host names cannot be used. The `jpccomm.ini` file on a logical host is ignored, and the host name for the logical host is used.
- If the monitoring suspension function is enabled, monitoring for all the hosts and agents must be resumed before setup.

The installation and setup procedures for PFM - Manager and the setting procedures for the cluster software are explained below.

In the procedure explanation, the image  indicates items to be performed on the executing node, and the image  indicates items to be performed on the standby node. In addition, the image  indicates setup items that are either required depending on the environment or can be performed if you want to set a value other than the default settings.

## (2) Installation procedure

Perform a new installation of PFM - Manager on the executing node and the standby node. The installation procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

Note:

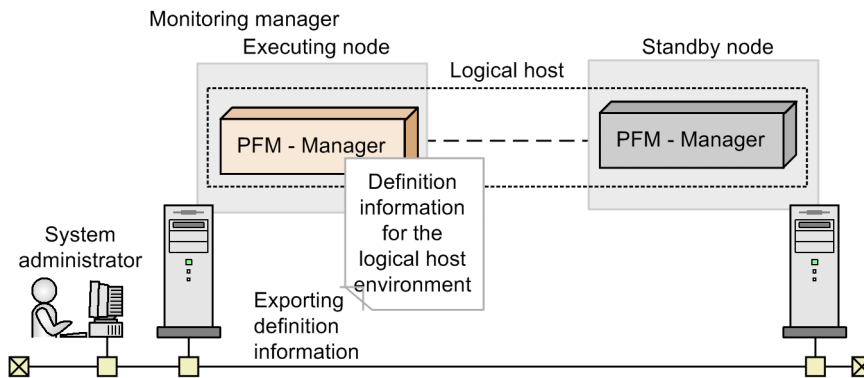
The installation destination is the local disk. Do not install PFM - Manager on the shared disk.

## (3) Setup procedure

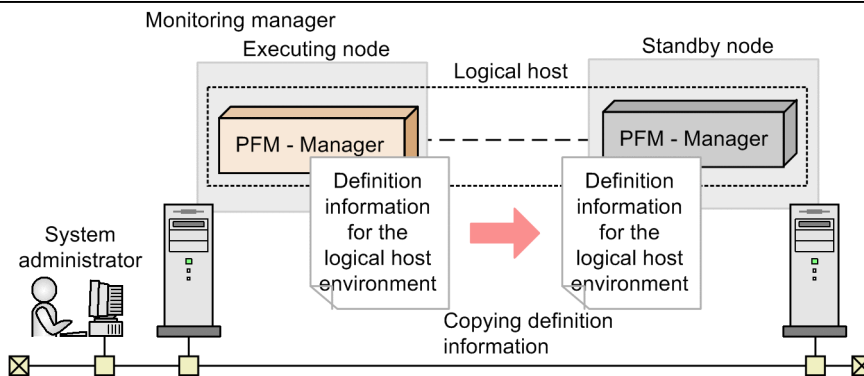
Perform PFM - Manager setup on the executing node first. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the setup content from the executing node to the standby node.

Figure 10–11: Method for applying the content set up on the executing node to the standby node

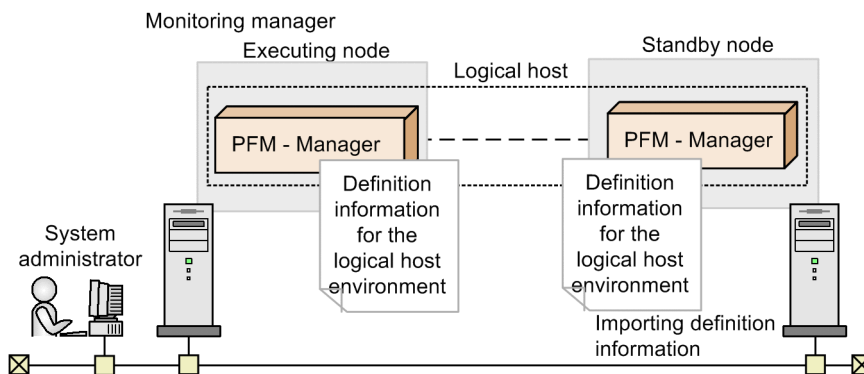
[Step 1] Set up the executing node.



[Step 2] Copy definition information from the executing node to the standby node.



[Step 3] Set up the standby node.



Each setup procedure is explained below.

**(a) Performing an additional setup for PFM - Agent or PFM - RM information** Executing

Standby Options

To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Manager for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.



The setup procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

Note:

If you add another PFM - Agent or PFM - RM to the same host as PFM - Manager, an additional setup is not required.

## (b) Making sure the shared disk is online Executing

Make sure that the shared disk is online on the executing node. If the shared disk is not online, place it online by using the cluster software and the volume manager.

## (c) Setting up the logical host environment for PFM - Manager Executing

Set up the logical host environment for PFM - Manager on the executing node. Before performing setup, stop all the Performance Management programs and services throughout the entire system.

### 1. Create a logical host environment.

Execute the `jpccconf ha setup` command to create a logical host environment for PFM - Manager.

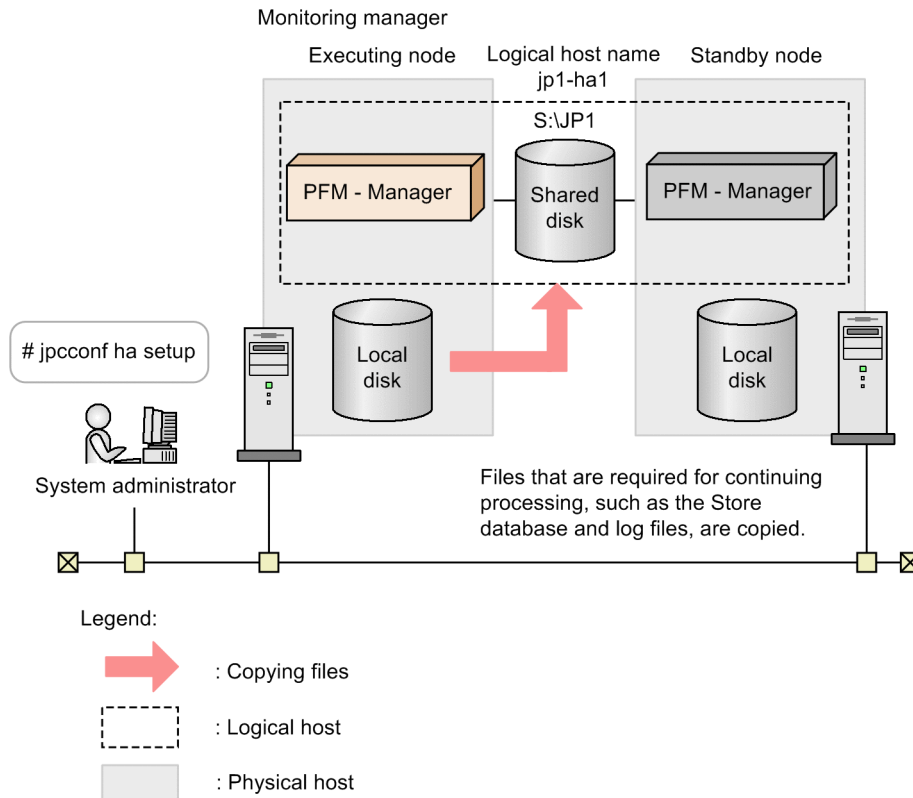
Use `-lhost` to specify the logical host name. For DNS operations, specify a logical host name that does not include a domain name. Specify the `-d` environment directory name for the directory name of the shared disk.

For example, execute the following command to set up a logical host with `jp1-ha1` as the logical host name and `S:\jp1` as the environment directory.

```
jpccconf ha setup -key Manager -lhost jp1-ha1 -d S:\jp1
```

When this command is executed, the `jp1pc` directory is created under `S:\jp1`, and the files required in the logical environment are copied to the environment directory. The following figure shows an example.

Figure 10–12: Execution example of the `jpccconf ha setup` command



When the command is executed, the required data is copied from the local disk of the executing node to the shared disk, and the settings required for use on the logical host are performed.

If you set up a logical host for PFM - Manager, the connection-target PFM - Manager in the physical host environment is renamed to the specified logical host name.

For details on the `jpccconf ha setup` command, see the chapters that describes commands in the manual *JP1/Performance Management Reference*.

## 2. Check the settings for the logical host environment.

Execute the `jpccconf ha list` command to check the settings for the logical host, and make sure that the logical host environment that has been created is correct.

```
jpccconf ha list -key all
```

An example of executing this command is as follows:

```
C:\>jpchasetup list all
```

Logical Host Name	Key	Environment Directory	[Instance Name]
jp1-ha1	mgr	"S:\jp1\jp1pc"	

KAVE05136-I The logical host startup information listing ended normally.

For details on the `jpccconf ha list` command, see the chapters that describes commands in the manual *JP1/Performance Management Reference*.

## (d) Performing a setup for a logical host of PFM - Agent or PFM - RM Executing

Options

This procedure is required only when PFM - Agent or PFM - RM needs to be set up on the same logical host as PFM - Manager.

For details on the setup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

## (e) Specifying network settings Executing

To use logical host names or logical IP addresses for communication among PFM - Manager and PFM - Web Console, add the following line to the *environment-directory\jp1pc\mgr\viewsvr\jpcvsvr.ini* file.

```
java.rmi.server.hostname=logical-host-name-or-logical-IP-address
```

For details on the host names used for communication between PFM - Manager, PFM - Web Console, and JP1/SLM, see the description of port numbers in the appendixes of the manual *JP1/Performance Management Reference*.

If you need to change the IP address and port number to connect to another instance of PFM- Manager, use the following procedure:

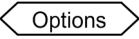
- Setting up IPv6 communication

When using Performance Management in an IPv6 environment, enable IPv6 support by executing the `jpccconf ipv6 enable` command on the PFM - Agent, PFM - RM, and PFM - Manager hosts.

In a cluster system, execute the command on the executing and standby nodes.

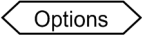
Note that only IPv4 communication is supported between PFM - Manager and PFM - Web Console.

For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

• Setting the IP address 

To set the IP addresses, directly edit the content of the `jpchosts` file. If you have edited the `jpchosts` file, copy the file from the executing node to the standby node.

For details on setting IP addresses, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

• Setting port numbers 

This procedure is necessary only when running Performance Management in a network environment with a firewall. For Performance Management communications via a firewall, use the `jpccconf port define` command to set a port number.

For example, execute the following command to set all port numbers for services that exist on the host with the logical host name `jp1-ha1` specified in the fixed values.

```
jpccconf port define -key all -lhost jp1-ha1
```

When this command is executed, definitions of the port numbers and service names (TCP service name beginning with `jp1pc` by default) for Performance Management are added to the services file.

In this example, the `jpccconf port define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on setting port numbers, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

For details on the `jpccconf port define` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

• Setting the host name or IP address used for communication with PFM - Web Console and JP1/SLM

In the following situations, define the host name or IP address of PFM - Manager in the `jpccsvr.ini` file on the PFM - Manager host.

- IP address translation (NAT translation) takes place between the PFM - Manager host and the PFM - Web Console host.
- Multiple IP addresses are used between the PFM - Manager host and the PFM - Web Console host.
- When linking with JP1/SLM, IP address translation (NAT translation) takes place between the PFM - Manager host and the JP1/SLM host.
- When linking with JP1/SLM, Multiple IP addresses are used between the PFM - Manager host and the JP1/SLM host.

For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

**(f) Changing the log file size**  

The operating status of Performance Management is output to a dedicated log file called the *common message log*. This setting is required if you want to change this file size.

For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

**(g) Specifying settings for the authentication mode**  

This setting is required only if you want to change the authentication mode of Performance Management from PFM authentication mode to JP1 authentication mode.

For details, see *2. Managing User Accounts and Business Groups*.

## (h) Specifying settings for access control based on business groups Executing

Options

This setting is required if you want to use business groups to manage users in Performance Management. You can enable or disable access control based on business groups by entering a setting in the startup information file (`jpccomm.ini`).

For details, see *2. Managing User Accounts and Business Groups*.

## (i) Changing the storage locations of event data Executing Options

The settings below are required if you want to change the storage destination, backup destination, or export destination of the event data managed by PFM - Manager.

By default, event data is stored in the following locations:

- Data storage folder: `environment-directory\jplpc\mgr\store\`
- Backup folder: `environment-directory\jplpc\mgr\store\backup\`
- Export folder: `environment-directory\jplpc\mgr\store\dump\`

For details on how to change a destination, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

## (j) Specifying settings for action log output Executing Options

This setting is required if you want to output an action log when an alarm is issued. An action log is log information output in conjunction with the alarm function, when an aspect of the system (such as the system load) exceeds a threshold. For details on how to set this option, see the section describing action log output in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

## (k) Configuring the health check function Executing Options

To configure the health check function:

1. Check the settings of the health check function.

Execute the following command on the PFM - Manager host on the executing node to display the setting of the health check function.

```
jpccconf hc display
```

When the command is executed, the setting for the health check function appears as follows:

- If the health check function is enabled: `available`
- If the health check function is disabled: `unavailable`

For details on the `jpccconf hc display` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

2. Change the setting of the health check function.

Execute the following command on the PFM - Manager host on the executing node to set up the health check function, if necessary.

- To enable the health check function:

```
jpccconf hc enable
```

- To disable the health check function:

```
jpccconf hc disable
```

For details on the `jpccconf hc enable` and `jpccconf hc disable` commands, see the chapter explaining the commands in the manual *JP1/Performance Management Reference*.

## (l) Exporting the logical host environment definitions Executing

When a logical host environment for PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file. To set up a different instance of Performance Management on the same logical host, perform an export after all setup procedures are completed.

1. Execute the `jpccconf ha export` command.

Export the logical host environment definitions to the desired file.

For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file.

```
jpccconf ha export -f lhostexp.conf
```

If the health check function is enabled for the PFM - Manager in the logical host environment you are exporting, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be exported.

In this example, the `jpccconf ha export` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha export` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

## (m) Copying the file containing the logical host environment definitions to the standby node Executing   Standby

Copy the file that has been exported in step (l) from the executing node to the standby node, so that it will be applied on the standby node.

Next, use operations of the cluster software or volume manager software to place the shared disk online, and finish the operations on the executing node. If this shared disk will continue to be used, it is not necessary to take it offline.

## (n) Importing the file containing the logical host environment definitions Standby

Import the exported file copied from the executing node to the standby node.

1. Execute the `jpccconf ha import` command.

Import the logical host environment definitions to the standby node.

For example, execute the following command if the export file name is `lhostexp.conf`.

```
jpccconf ha import -f lhostexp.conf
```

When the `jpccconf ha import` command is executed, the environment settings for the standby node are changed to the same environment as for the executing node. Therefore, the necessary settings are made to use PFM - Manager on a logical host.

If the health check function is enabled for the PFM - Manager in the logical host environment you are importing, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be imported.

In this example, the `jpccconf ha import` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha import` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## 2. Check the settings for the logical host environment.

Execute the `jpccconf ha list` command in the same manner as for the executing node, to check the settings of the logical host.

Execute the command as follows:

```
jpccconf ha list -key all
```

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (4) Cluster software setting procedure

Cluster software settings are required for both the executing node and the standby node.

### (a) Registering PFM - Manager in the cluster software Executing Standby

To use PFM - Manager on a logical host, register it in the cluster software, and set the cluster software to control the starting and stopping of PFM - Manager.

For details on how to register PFM - Agents or PFM - RM in the cluster software, see the chapters that describe operations in cluster systems in the appropriate PFM - Agent or PFM - RM manual.

The setting contents for registering PFM - Manager in the cluster software are described below by using items for registration in Windows WSFC as examples.

For example, when running PFM - Manager in standalone mode on a logical host, register the services listed in the following table in the cluster software.

Table 10–2: PFM - Manager services to register in the cluster software (standalone mode)

No.	Name	Service name	Dependencies
1	PFM - Name Server [LHOST]	JP1PCMGR_PN [LHOST]	IP address resources Physical disk resources <sup>#</sup>
2	PFM - Master Manager [LHOST]	JP1PCMGR_PM [LHOST]	#1 cluster resources
3	PFM - Master Store [LHOST]	JP1PCMGR_PS [LHOST]	#2 cluster resources
4	PFM - Correlator [LHOST]	JP1PCMGR_PE [LHOST]	#3 cluster resources
5	PFM - Trap Generator [LHOST]	JP1PCMGR_PC [LHOST]	#4 cluster resources
6	PFM - View Server [LHOST]	JP1PCMGR_PP [LHOST]	#5 cluster resources
7	PFM - Action Handler [LHOST]	JP1PCMGR_PH [LHOST]	#6 cluster resources
8	PFM - Agent Store for HealthCheck [LHOST]	JP1PCAGT_0S [LHOST]	#7 cluster resources
9	PFM - Agent for HealthCheck [LHOST]	JP1PCAGT_0A [LHOST]	#8 cluster resources

<sup>#</sup>: The shared disk drive that hosts the logical host environment directory created according to (c) in (3) above.

When running PFM - Manager on the same logical host as PFM - Agent or PFM - RM, register the services listed in the table below in the cluster software. In this example, the system is running PFM - RM for Platform and PFM - Agent for Oracle.

Table 10–3: PFM - Manager services to register in the cluster software (on a host with PFM - Manager, PFM - RM for Platform, and PFM - Agent for Oracle installed)

No.	Name	Service name	Dependencies
1	PFM - Name Server [ <i>LHOST</i> ]	JP1PCMGR_PN [ <i>LHOST</i> ]	IP address resources Physical disk resources <sup>#1</sup>
2	PFM - Master Manager [ <i>LHOST</i> ]	JP1PCMGR_PM [ <i>LHOST</i> ]	#1 cluster resources
3	PFM - Master Store [ <i>LHOST</i> ]	JP1PCMGR_PS [ <i>LHOST</i> ]	#2 cluster resources
4	PFM - Correlator [ <i>LHOST</i> ]	JP1PCMGR_PE [ <i>LHOST</i> ]	#3 cluster resources
5	PFM - Trap Generator [ <i>LHOST</i> ]	JP1PCMGR_PC [ <i>LHOST</i> ]	#4 cluster resources
6	PFM - View Server [ <i>LHOST</i> ]	JP1PCMGR_PP [ <i>LHOST</i> ]	#5 cluster resources
7	PFM - Action Handler [ <i>LHOST</i> ]	JP1PCMGR_PH [ <i>LHOST</i> ]	#6 cluster resources
8	PFM - Agent Store for HealthCheck [ <i>LHOST</i> ]	JP1PCAGT_OS [ <i>LHOST</i> ]	#7 cluster resources
9	PFM - Agent for HealthCheck [ <i>LHOST</i> ]	JP1PCAGT_OA [ <i>LHOST</i> ]	#8 cluster resources
10	PFM - RM Store for Platform <i>instance-name</i> [ <i>LHOST</i> ]	JP1PCAGT_7S_ <i>instance-name</i> [ <i>LHOST</i> ]	#7 cluster resources <sup>#2</sup>
11	PFM - RM for Platform <i>instance-name</i> [ <i>LHOST</i> ]	JP1PCAGT_7A_ <i>instance-name</i> [ <i>LHOST</i> ]	#10 cluster resources <sup>#2</sup>
12	PFM - RM Store for Oracle <i>instance-name</i> [ <i>LHOST</i> ]	JP1PCAGT_1S_ <i>instance-name</i> [ <i>LHOST</i> ]	#7 cluster resources <sup>#2</sup>
13	PFM - RM for Oracle <i>instance-name</i> [ <i>LHOST</i> ]	JP1PCAGT_1A_ <i>instance-name</i> [ <i>LHOST</i> ]	#12 cluster resources <sup>#2</sup>

#1  
The shared disk drive that hosts the logical host environment directory created according to (c) in (3) above.

#2  
For details on the Agent-specific dependencies you need to set, see the documentation for PFM - Agent or PFM - RM.

Place the logical host name wherever [*LHOST*] appears. The following is an example for a Name Server service for which the logical host name is `jp1-ha1`:

- Name  
PFM - Name Server [`jp1-ha1`]
- Service name  
JP1PCMGR\_PN [`jp1-ha1`]

For WSFC, these services are registered as WSFC resources. The settings for each resource are as follows. The setting items for WSFC are indicated by [ ].

- [**Resource Type**] is registered as `General-Purpose Service`.



- See *Table 10-2 PFM - Manager services to register in the cluster software (standalone mode)* and *Table 10-3 PFM - Manager services to register in the cluster software (on a host with PFM - Manager, PFM - RM for Platform, and PFM - Agent for Oracle installed)* and specify **Dependencies**.

For example, if the PFM - Master Store [*LHOST*] service is to be registered into cluster software, specify the service in such a manner that it is in a dependency with PFM - Master Manager [*LHOST*] service because a dependency with cluster resource 2 is required.

- **Startup Parameters** and **Registry Replication** are not specified.
- Specify the settings for the **Policies** tab in Properties according to whether a failover is performed when a problem occurs in Performance Management.

For example, if you want to perform a failover in the event of a PFM - Manager failure, specify as follows:

- Select the **If resource fails, attempt restart on current node** check box.
- Select the **If restart is unsuccessful, fail over all resources in this service or application** check box.<sup>#</sup>
- As a guideline, specify 3 in **Maximum restarts in the specified period**.

#

These options correspond to **If restart is unsuccessful, fail over all resources in this Role** in Windows Server 2012 or later.

### Important

- Starting and stopping of services registered on a cluster are controlled by the cluster software. Therefore, set [**Startup Type**] to [**Manual**] so that automatic startup is not performed when the OS starts up on the executing node and the standby node. Services are set to [**Manual**] immediately after setup by the `jpccconf ha setup` command. In addition, do not use the following command to perform a forced stop.

```
jpccspm stop -key all -lhost logical-host-name -kill immediate
```

- When PFM - Manager links to integrated management products (JP1/IM), specify their dependency relationship so that the PFM - Manager services stop before the JP1/Base services stop.

## (b) Checking starting and stopping from the cluster software

Executing

Standby

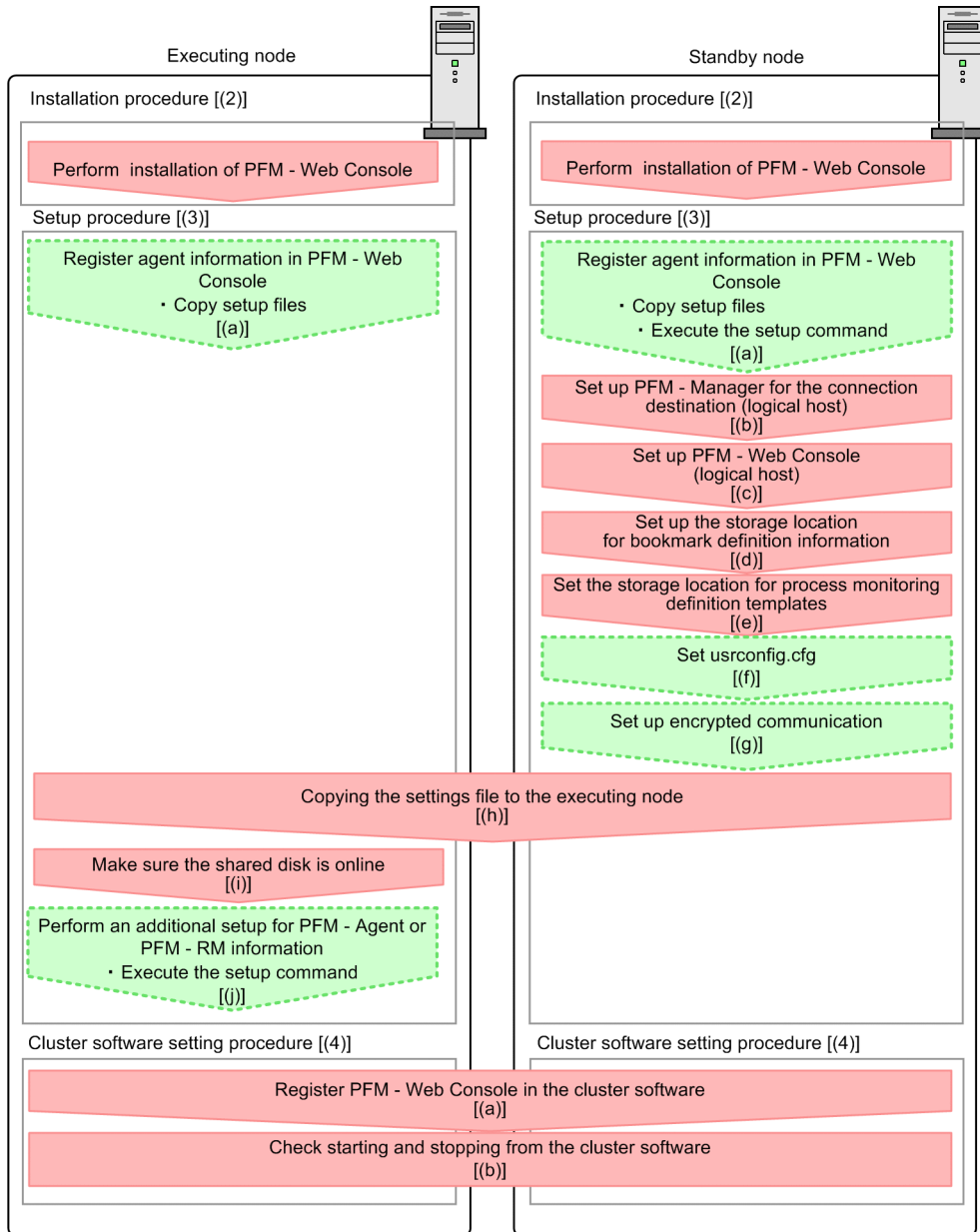
Perform operations to start and stop PFM - Manager from the cluster software in each node, and make sure that the operations are normal.

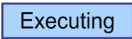

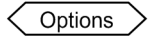


## 10.2.3 Installing and setting up PFM - Web Console

### (1) Process flow for installation and setup

Figure 10–13: Process flow for installation and setup of PFM - Web Console used on a logical host



In the procedure explanation, the image  indicates the items to be performed on the executing node, and the image  indicates the items to be performed on the standby node. In addition, the image  indicates the setup items required depending on the environment, and the optional setup items for when changing the default settings.

### (2) Installation procedure

Perform a new installation of PFM - Web Console on the executing node and the standby node. The installation procedure is the same as for a non-cluster system.

For details on the installation procedure, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

Notes:

- The installation destination is the local disk. Do not perform installation on the shared disk.
- Install each PFM - Web Console for both the executing node and the standby node in a location with the same path.

### (3) Setup procedure

When using PFM - Web Console on a logical host, the environment configurations on the executing node and the standby node have to be the same.

#### (a) Registering agent information in PFM - Web Console

Executing

Standby

Options

To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Web Console for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Notes:

- You do not need to register PFM - Agent or PFM - RM if you add the same version of PFM - Agent or PFM - RM with the same product ID to a Performance Management system in which the PFM - Agent or PFM - RM information has already been registered.
- Set up the latest version of PFM - Agent or PFM - RM if you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host.

The additional setup for agent information in PFM - Web Console takes place where shown in [Figure 10-13 Process flow for installation and setup of PFM - Web Console used on a logical host](#).

To register the agent information in PFM - Web Console:

1. Copy the setup file. 

Executing

Standby

Copy the PFM - Agent or PFM - RM setup files to the following locations on the PFM - Web Console executing and standby nodes.

`pfm - web console-installation-folder\setup\`

The setup file to be copied and the relevant procedure are the same as for when an additional setup is performed for PFM - Manager. For details, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

2. Execute the setup command on the standby node. 

Standby

Execute the `jpcwagtsetup` command on the standby node, and register the agent information.

Execute the command as follows:

```
jpcwagtsetup
```

For details on the `jpccwagtsetup` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

Supplemental information:

When you register the agent information of PFM - Agent or PFM - RM in PFM - Web Console, you must restart PFM - Web Console. However, the restart after step 2 is not required because PFM - Web Console restarts when a failover occurs.

## **(b) Setting up PFM - Manager for the connection destination (logical host)** Standby

On the standby node, set the IP address and host name for PFM - Manager to which PFM - Web Console connects in the Windows initialization file (`config.xml`).

Specify the IP address or the host name of the PFM - Manager to connect to in `host` in the `<vserver-connection>` tag under the `<vsa>` tag. If the PFM - Manager to connect to is running on a cluster system, specify the logical IP address or the logical host name.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

## **(c) Setting up PFM - Web Console (logical host)** Standby

Set the logical IP address or logical host name for PFM - Web Console in the Windows initialization file (`config.xml`) on the standby node.

Specify the logical IP address or the logical host name of the PFM - Web Console host in `host` in the `<vserver-connection>` tag under the `<vsa>` tag.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

## **(d) Setting up the storage location for bookmark definition information** Standby

Set the folder to store the bookmark definition information in the Windows initialization file (`config.xml`) on the standby node.

Specify the folder for storing bookmark definition information in `bookmarkRepository` in the `<bookmark>` tag under the `<vsa>` tag. Specify a folder on the shared disk to ensure that the information is inherited if a failover occurs.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

## **(e) Setting the storage location for process monitoring definition templates**

Standby

Set the storage folder for process monitoring definition templates in the initialization file (`config.xml`) on the standby node.

Specify the folder for storing bookmark definition information in `processMonitoringTemplatesRepository` in the `<process-monitoring>` tag under the `<vsa>` tag. Specify a folder on the shared disk to ensure that the information is inherited if a failover occurs.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

## (f) Setting `usrconf.cfg` Standby

If the language setting of the system locale differs from that of the `usrconf.cfg` file, change the setting of the `usrconf.cfg` file on the standby node.

If the system locale has been changed since passwords were set, check and, if necessary, revise the settings in the `usrconf.cfg` file.

For details about the option definition file (`usrconf.cfg`), see the chapter that describes definition files in the manual *JP1/Performance Management Reference*.

## (g) Setting encrypted communication between a web browser and the monitoring console server Standby

If you will be using encrypted communication between a web browser and the monitoring console server, specify the settings in both PFM - Web Console and the web browser. For details, see the section on changing the settings for encrypted communication between a web browser and the monitoring console server in the *JP1/Performance Management Planning and Configuration Guide*.

## (h) Copying the settings file to the executing node Standby Executing

Copy the Windows initialization file (`config.xml`) edited in (b), (c), (d), and (e) to the executing node.

Copy the file to the following location on the executing node:

```
installation-folder\conf
```

If the settings of the `usrconf.cfg` file on the standby node were changed in (f), you need to copy the file to the executing node. Copy the file to the following location on the executing node:

```
Installation folder\CPSB\CC\web\containers\PFMWebConsole\usrconf
```

## (i) Make sure the shared disk is online Executing

Make sure that the shared disk is online on the execution node. If the shared disk is not online, place it online through the operation of the cluster software and the volume manager.

## (j) Performing an additional setup for PFM - Agent or PFM - RM information Executing

Options

Use the setup files copied in (a) to perform an additional setup of the agent information for PFM - Agent or PFM - RM on the execution node.

1. Stop the PFM - Web Console services on the executing node.

Use the `jpcwstop` command to stop the services if the PFM - Web Console services are not registered with the cluster software.

When making changes to the Performance Management configuration such as adding PFM - Agent or PFM - RM after the services are registered with the cluster software, use the cluster software to stop the services. For details on changing the configuration of the cluster system, see [10.3 Changing the cluster system configuration \(in Windows\)](#).

2. Execute the setup command on the executing node.

Execute the command as follows:

```
jpcwagtsetup
```

For details on the `jpcwagtsetup` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

- 3. Start the PFM - Web Console service on the executing node.  
Start the PFM - Web Console services stopped in step 1.

### (4) Cluster software setting procedure

Set PFM - Web Console in the cluster software. Perform this setting in both the executing node and the standby node.

#### (a) Registering PFM - Web Console in the cluster software Executing Standby

To use PFM - Web Console in a logical host environment, register it in the cluster software, and then set the cluster software to control the starting and stopping of PFM - Web Console.

The setting contents for registering PFM - Web Console in the cluster software are described below by using items for registration in Windows WSFC as examples. For PFM - Web Console, perform an additional registration of the services listed in the following table in the same cluster group as for PFM - Manager.

Table 10–4: PFM - Web Console services to be registered in the cluster software

No.	Name	Service name	Dependencies
1	PFM - Web Console	PFM-WebConsole	IP address resources Physical disk resources <sup>#</sup>
2	PFM - Web Service	PFM-WebService	#1-1 cluster resources (PFM - Web Console)

<sup>#</sup>: The shared disk drive that hosts the logical host environment directory created according to (d) and (e) in (3) above.

For WSFC, these services are registered as WSFC resources. The settings for each resource are as follows. The setting items for WSFC are indicated by [ ].

- Register resources as `General-Purpose Service`.
- Set [Name], [Service Name], and [Dependency] with reference to [Table 10-4 PFM - Web Console services to be registered in the cluster software](#).  
[Name] is the name for displaying the service, and [Service Name] is the name for specifying the service to be controlled by WSFC.
- Starting and stopping a service that is registered in the cluster are controlled by the cluster software. To prevent services from being started automatically when the OS starts, set **Startup type** to **Manual** on both the executing node and the standby node.
- Do not set [Duplicate Registry].
- On the **Policies** tab in Properties, select the **If resource fails, attempt restart on current node** check box. As a guideline, specify 3 in **Maximum restarts in the specified period**.

#### Important

- When you configure WSFC, use **Failover Cluster Management** and the `cluster` command provided by the cluster software. For details, see the documentation provided by Microsoft.
  1. Create the clustered PFM - Web Service service.

Choose **Failover Cluster Management** in the Start menu to start the cluster software, and then create a clustered PFM - Web Service. Add the generic service (the PFM - Web Service), a client access point (Name, IP address), storage, and other resources to move between nodes when a failover occurs. Display the properties for each item, and set the resource dependencies and other cluster-related settings.

2. Execute the `cluster` command.

Open the command prompt as an administrator, and execute the following command:

```
cluster /res "resource-name" /priv /StartupParameters=""
```

`Δ` represents a space. As *resource-name*, specify the resource name of the generic PFM - Web Service service. You can find out the resource name of the generic service in the Failover Cluster Management tool.

3. Check the value in **Setup parameters**.

From **Failover Cluster Management**, open the Properties page for the generic PFM - Web Service service, and make sure that the **Setup parameters** field is empty.

## (b) Checking starting and stopping from the cluster software

Executing

Standby

Perform operations to start and stop PFM - Web Console in each node from the cluster software, and make sure that the operations are normal.

## 10.2.4 Installing an upgrade for PFM - Agent or PFM - RM

To install an upgrade for PFM - Agent or PFM - RM in a physical host environment where PFM - Agent, PFM - RM, or PFM - Manager is running in a logical host environment:

1. Use the cluster software to stop all of the PFM services on each logical host.
2. Use the `jpcspm stop -key jplpc` command to stop all of the PFM services on both the executing and standby physical hosts.
3. Place the shared disk online from the executing node.
4. Install PFM - Agent or PFM - RM on each applicable executing host by overwriting the previous installation.
5. Install PFM - Agent or PFM - RM on each applicable standby host by overwriting the previous installation.
6. Set up Performance Management so that it can run.
7. Use the cluster software to start all of the PFM services on each logical host.
8. Use the cluster software to start all of the PFM services on both the executing and standby physical hosts.

For details on PFM - Agent-specific or PFM - RM-specific considerations, see the corresponding PFM - Agent or PFM - RM manual and the *Release Notes*.

## 10.2.5 Unsetup and uninstallation of PFM - Manager

### (1) Before unsetup and uninstallation

Notes regarding the order of unsetup:

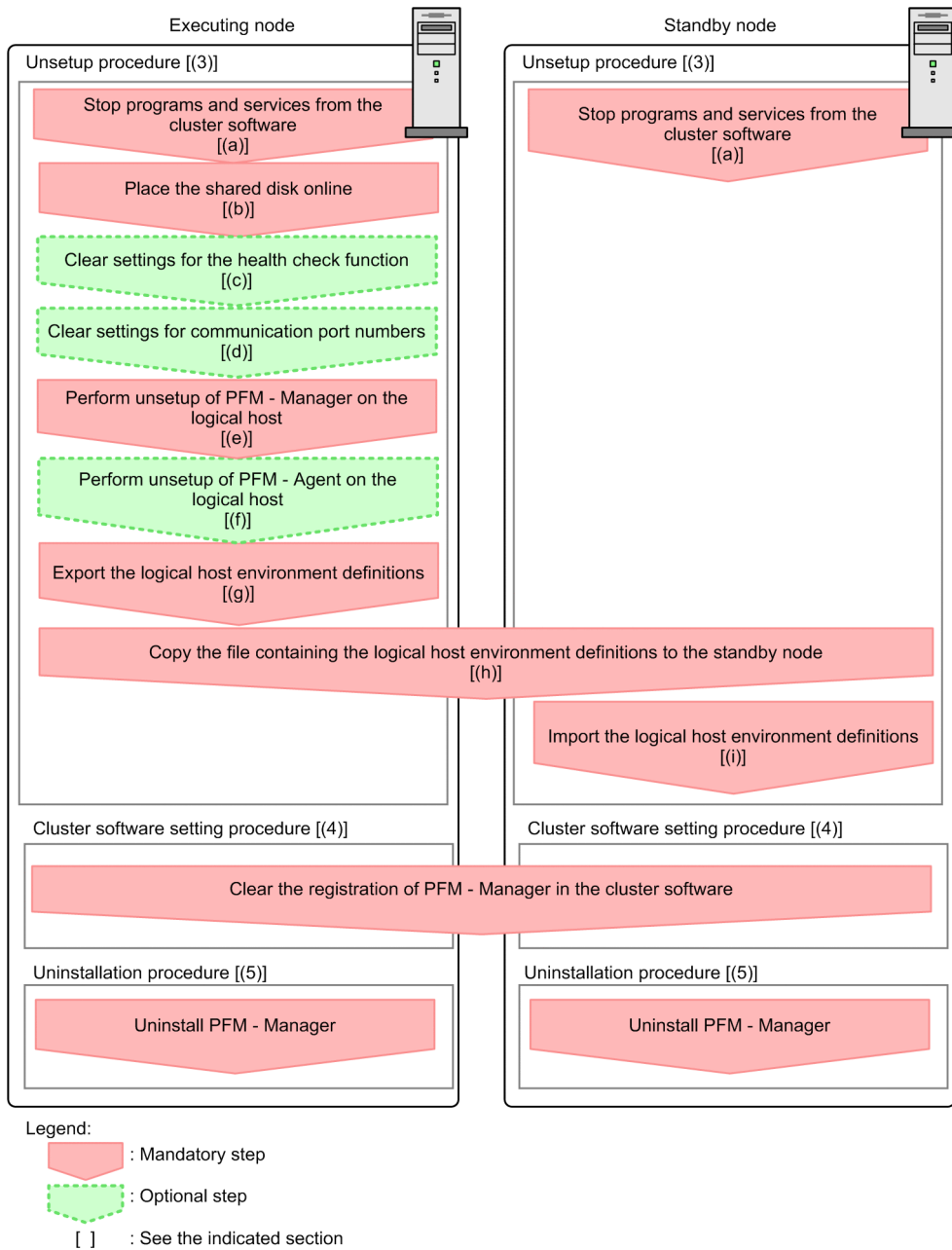
PFM - Manager is required to execute PFM - Agent or PFM - RM. Therefore, when performing unsetup on PFM - Manager, it is necessary to consider its relationship with PFM - Agent or PFM - RM in the system and determine the work order for unsetup. The work order when unsetup is required is the same as the order for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

Notes on stopping of services:

Stop all Performance Management programs and services running on the executing nodes and standby nodes on which unsetup is to be performed. Also, stop all PFM - Agent services across the Performance Management system connected to the PFM - Manager for which unsetup will be performed. For details on how to stop services, see *1. Starting and Stopping Performance Management*.

## (2) Process flow for unsetup and uninstallation

Figure 10–14: Process flow for unsetup and uninstallation of PFM - Manager used on a logical host (in Windows)



In the procedure explanation, the image indicates the items to be performed on the executing node, and the image indicates the items to be performed on the standby node. In addition, the image indicates the setup items required depending on the environment, and the optional setup items for when changing the default settings.

## (3) Unsetup procedure

First, perform unsetup on the executing node. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the unsetup content from the executing node to the standby node.



## (a) Stopping from the cluster software Executing Standby

Use operations from the cluster software to stop all Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

## (b) Making sure the shared disk is online Executing

Make sure that the shared disk is online on the executing node. If the shared disk is not online, place it online through the operation of cluster software and the volume manager.

## (c) Clearing settings for the health check function Executing Options

Execute the following command on the PFM - Manager host on the executing node to clear the settings for the health check function.

```
jpccconf hc disable
```

For details on the `jpccconf hc disable` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (d) Clearing settings for communication port numbers Executing Options

This procedure is required only when port numbers have been set using the `jpccconf port define` command during the setup in an environment with a firewall.

1. Clear the settings for communication port numbers.

Execute the `jpccconf port define` command to clear the settings for communication port numbers.

For example, execute the following command to clear all the settings for port numbers for services that exist on the host with the logical host name `jp1-hal`.

```
jpccconf port define -key all -lhost jp1-hal
```

In this example, the `jpccconf port define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode.

The `jpccconf port define` command is used to set the port numbers that are used for communications by PFM - Manager on the logical host or by other Performance Management programs. When entering a port number, a value of 0 will clear the setting. In addition, when this command is executed, the port numbers and service names (service names starting with `jp1pc` by default) for Performance Management defined in the services file are deleted.

For details on the `jpccconf port define` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (e) Performing unsetup of a logical host for PFM - Manager Executing

1. Check the logical host settings.

Check the current settings before performing unsetup on the logical host environment. Check the logical host name and shared disk path.

Execute the command as follows:

```
jpccconf ha list -key all
```

An example of executing this command is as follows:

```
C:\>jpchasetup list all
```

Logical Host Name	Key	Environment Directory	[Instance Name]
jp1-ha1	mgr	"S:\jp1\jp1pc"	

KAVE05136-I The logical host startup information listing ended normally.

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

## 2. Delete the logical host environment for PFM - Manager.

When the `jpccconf ha unsetup` command is executed, the settings for starting PFM - Manager on the logical host are deleted. In addition, the files for the logical host on the shared disk are also deleted. Execute the command as follows:

```
jpccconf ha unsetup -key Manager -lhost jp1-ha1
```

For details on the `jpccconf ha unsetup` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

Note:

If the shared disk is offline, only the logical host settings will be deleted. The directories and files on the shared disk will not be deleted.

## 3. Check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all
```

Make sure that PFM - Manager has been deleted from the logical host environment.

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

## (f) Performing unsetup for a logical host of PFM - Agent or PFM - RM Executing

Options

This procedure is required only when there is PFM - Agent or PFM - RM on the same logical host from which unsetup will also be performed for PFM - Manager.

Perform unsetup of PFM - Agent or PFM - RM. For details on the unsetup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

## (g) Exporting the logical host environment definitions Executing

When a logical host environment to perform unsetup of PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file.

Note:

To perform unsetup of a different instance of Performance Management from the same logical host, perform the export after all unsetup procedures are completed.

### 1. Export the logical host environment definitions.

For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file. The export file allows an arbitrary file name.

```
jpccconf ha export -f lhostexp.conf
```

In this example, the `jpccconf ha export` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha export` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (h) Copying the file containing the logical host environment definitions to the standby node

Executing

Standby

Copy the file that has been exported in step (f) from the executing node to the standby node, so that it will be applied on the standby node.

Next, use operations of the cluster software or volume manager software to place the shared disk online, and finish the operations on the executing node. If this shared disk will continue to be used, it is not necessary to take it offline.

## (i) Importing the file containing the logical host environment definitions

Standby

Import the export file copied from the executing node to the standby node, so that it will be applied to the standby node.

Use the `jpccconf ha import` command to apply the Performance Management settings for the logical host created on the executing node to the standby node. If multiple instances of Performance Management have been set up on a single logical host, import all of the instances as one group.

### 1. Import the logical host environment definitions.

Use the `jpccconf ha import` command to import the exported file of logical host environment definitions copied from the executing node to the standby node.

For example, execute the following command when the exported file name is `lhostexp.conf`.

```
jpccconf ha import -f lhostexp.conf
```

When the command is executed, the environment settings for the standby node are changed to the same environment settings specified for the executing node that has been exported. Therefore, the settings for running PFM - Manager on a logical host are deleted. If you perform unsetup of Performance Management on another logical host, the relevant settings are also deleted.

In this example, the `jpccconf ha import` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha import` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

### 2. Check the settings for the logical host environment.

Execute the `jpccconf ha list` command in the same manner as for the executing node, to check the settings of the logical host.

Execute the command as follows:

```
jpccconf ha list -key all
```

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (4) Clearing the registration of PFM - Manager in the cluster software

Executing

Standby

Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

## (5) Performing uninstallation of PFM - Manager

Executing

Standby

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure is the same as for a non-cluster system.

For details, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

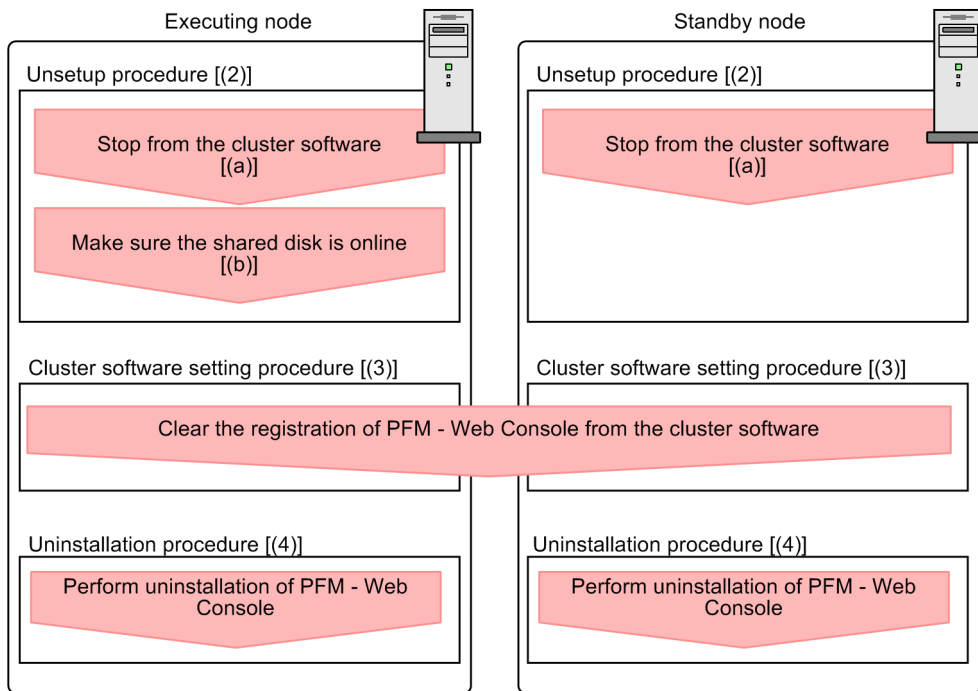
Notes:

- When performing uninstallation of PFM - Manager, stop all Performance Management programs and services on the node where uninstallation is to be performed.
- If uninstallation is performed on Performance Management without deleting the logical host environment, the environment directory might remain. When this happens, delete the environment directory.


## 10.2.6 Unsetup and uninstallation of PFM - Web Console

### (1) Process flow for unsetup and uninstallation

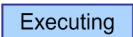
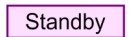
Figure 10–15: Process flow for unsetup and uninstallation of PFM - Web Console used on a logical host (in Windows)



Legend:

 : Required item

[ ] : See the indicated step.

The image  indicates the items to be performed on the executing node, and the image  indicates the items to be performed on the standby node.

### (2) Unsetup procedure

#### (a) Stopping from the cluster software

Use operations from the cluster software to stop all Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

#### (b) Making sure the shared disk is online

Make sure that the shared disk is online. If the shared disk is not online, place it online through the operation of the cluster software and volume manager.

### (3) Clearing the registration of PFM - Web Console from the cluster software

Executing

Standby

Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

### (4) Performing uninstallation of PFM - Web Console

Executing

Standby

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure of PFM - Web Console is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

#### Note:

If the installation folder for the bookmark definition information has been changed from the default setting, it will not be deleted when performing uninstallation of PFM - Web Console. You need to delete it manually after performing the uninstallation.

## 10.3 Changing the cluster system configuration (in Windows)

---

After a system is configured and the operation started, as the business expands and processed data volume increases, the system's cluster configuration might need to be changed with the addition of servers or introduction of new applications.

For this reason, the following the Performance Management configuration changes need to be studied in response to changes in the cluster configuration of the monitoring target system:

- Addition of PFM - Agent or PFM - RM due to the addition of a monitored system
- Removal of PFM - Agent or PFM - RM due to the removal of a monitored system
- Changing the logical host name of a machine after operation begins
- Changing the logical host environment after operation begins

This section describes the procedures for making changes to the Performance Management configuration when using a cluster system on a logical host.

### 10.3.1 Adding PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be added in order to monitor the performance of servers or applications that are newly added to a system.

When you add PFM - Agent or PFM - RM with a new product ID that has not previously been used in the Performance Management system, you need to set up the agent information in PFM - Manager and PFM - Web Console.

For details on product IDs, see the appropriate PFM - Agent or PFM - RM manual.



#### Tip

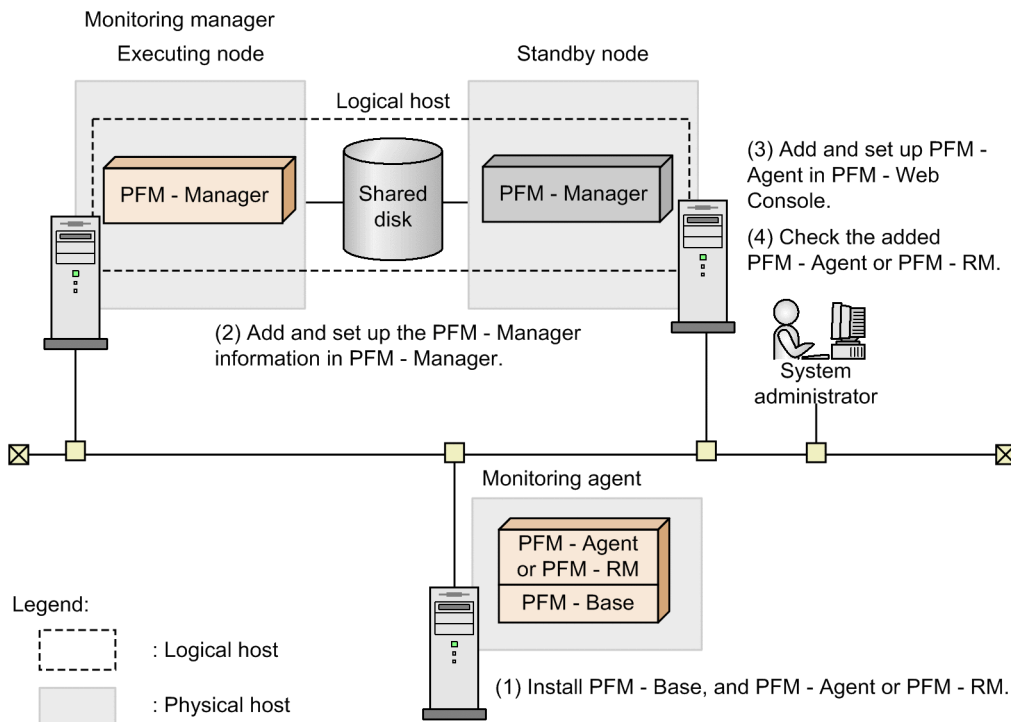
Agent information is a kind of information used by PFM - Manager and PFM - Web Console to manage and display PFM - Agent or PFM - RM.

Notes:

- Stop PFM - Manager and all Performance Management programs and services on that node before adding PFM - Agent or PFM - RM. For details on how to stop services, see [1. Starting and Stopping Performance Management](#).
- It is also necessary to stop PFM - Manager used on a logical host if work is being performed. An error might occur if you execute the `jpccconf agent setup` command or the `jpccwagtsetup` command to add PFM - Agent or PFM - RM before the Performance Management programs and services are completely stopped. In such a case, first make sure that all services have been completely stopped, and then re-execute the `jpccconf agent setup` command or the `jpccwagtsetup` command.

The following figure shows the process flow for adding PFM - Agent or PFM - RM to a Performance Management system in a logical host environment.

Figure 10–16: Process flow for adding PFM - Agent or PFM - RM to a Performance Management system in a logical host environment



The procedure is as follows:

## (1) Installing PFM - Base and either PFM - Agent or PFM - RM

Perform a new installation of PFM - Base and either PFM - Agent or PFM - RM on the host where Performance Management will be used to monitor performances.

For details on the installation procedure, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

## (2) Performing an additional setup for PFM - Agent or PFM - RM information in PFM - Manager

### (a) Process flow of additional PFM - Agent or PFM - RM information setup in PFM - Manager

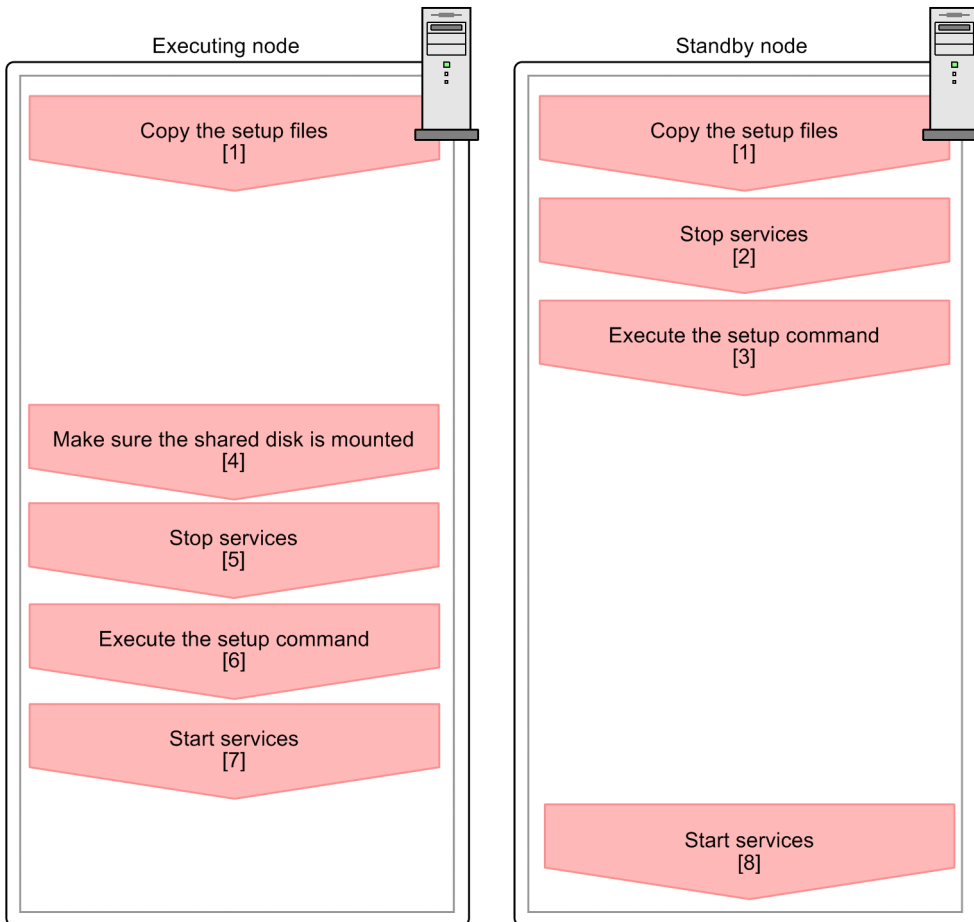
The process flow for performing an additional setup for the agent information of PFM - Agent or PFM - RM into PFM - Manager used on a logical host in a cluster system is described below.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Perform the addition and setup of agent information on the standby node first. When the addition and setup are completed on the standby node, next perform setup on the executing node.



Figure 10–17: Additional PFM - Agent or PFM - RM information setup in PFM - Manager



Legend:



: Required setup item



: See the indicated step.

Notes:

- If you add PFM - Agent or PFM - RM to the same host as PFM - Manager and PFM - Web Console, an additional setup is not required.
- If you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host, first set up the older version of PFM - Agent or PFM - RM, and then set up the newer version of PFM - Agent or PFM - RM.

## (b) Additional PFM - Agent or PFM - RM information setup procedure in PFM - Manager

The procedure for performing an additional setup for PFM - Agent or PFM - RM agent information is explained below.

To add and set up the PFM - Agent information in PFM - Manager:

The image Executing means the procedure used on the executing node, and the image Standby means the procedure used on the standby node.

1. Copying the setup files Executing Standby

Copy the PFM - Agent or PFM - RM setup files to the executing and standby nodes of PFM - Manager.

For details, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

## 2. Stopping services on the standby node Standby

Stop all physical host services on the standby node.

## 3. Executing the setup command Standby

Execute the `jpccconf agent setup` command on the standby node to add and set up the new agent.

Execute the command as follows:

```
jpccconf agent setup -key xxxx
```

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

For example, execute the following command to set up PFM - Agent for Oracle:

```
jpccconf agent setup -key Oracle
```

In this example, the `jpccconf agent setup` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf agent setup` command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

## 4. Making sure the shared disk is online Executing

Make sure that the shared disk is online on the execution node. With the additional setup procedure, write the agent information to the shared disk. Use either operations from the cluster software or the volume manager to check if the shared disk is online.

## 5. Stopping services Executing

Stop all Performance Management programs and services in the physical and logical host environments on the standby node. Use the cluster software to stop the programs and services.

## 6. Executing setup commands Executing

Execute the `jpccconf agent setup` command on the executing node in the same manner as for the standby node in order to add and set up the new agent.

```
jpccconf agent setup -key xxxx
```

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

For example, execute the following command to set up PFM - Agent for Oracle:

```
jpccconf agent setup -key Oracle
```

In this example, the `jpccconf agent setup` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf agent setup` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## 7. Starting services Executing

Start the Performance Management programs and services that were stopped on the executing node.

## 8. Starting services on the standby node Standby

On the standby node, start the Performance Management programs and services that you stopped earlier.

### (3) Performing an additional setup for PFM - Agent or PFM - RM in PFM - Web Console

Perform an additional setup for PFM - Agent or PFM - RM information in instances of PFM - Web Console that are used on a logical host in a cluster system.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

For details on the additional setup procedure, see [10.2.3\(3\)\(a\) Registering agent information in PFM - Web Console](#).

### (4) Checking PFM - Agent or PFM - RM that was added and set up

1. Start the services on the PFM - Agent or PFM - RM nodes.

Start the Performance Management programs and services on the nodes of the newly added PFM - Agent or PFM - RM.

2. Check if PFM - Agent or PFM - RM has been added correctly.

Execute the `jpctool service list` command to check if PFM - Manager has been connected correctly.

Execute the command as follows:

```
jpctool service list -id *
```

For details on the `jpctool service list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## 10.3.2 Deleting PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be deleted when a monitored system is removed from the entire system due to changes in the system configuration.

Delete PFM - Agent or PFM - RM from the Performance Management system used by the logical host. The programs must be deleted from both the PFM - Manager and PFM - Web Console hosts.

Note:

Stop all programs and services associated with the instance of PFM - Agent or PFM - RM you are deleting.

### (1) Deleting PFM - Agent or PFM - RM from PFM - Manager

1. Unbind the alarm tables.

If any alarm tables are bound to the instance of PFM - Agent or PFM - RM you are deleting, unbind the alarm tables in PFM - Web Console or by using the `jpctool alarm unbind` command. For details on how to unbind alarm tables in PFM - Web Console, see [6.6.1\(2\)\(b\) Unbinding an alarm table bound to a monitoring agent](#). For details on how to unbind alarm tables using the `jpctool alarm unbind` command, see [6.8.2 Unbinding an alarm table bound to a monitoring agent](#).

2. Delete the agent information.

Delete the agent information managed by PFM - Manager.

Execute the command as follows:

```
jpctool service delete -id xxxx -host host-name -lhost logical-host-name
```

xxxx indicates the service ID for each PFM - Agent or PFM - RM.

For example, execute the following command to delete the agent information for PFM - Agent for Oracle in the logical host environment with the host name `jp1` and the logical host name `jp1-ha1`.

```
jpctool service delete -id O* -host jp1 -lhost jp1-ha1
```

For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

### 3. Perform unsetup and uninstall PFM - Agent or PFM - RM.

Perform unsetup and uninstall PFM - Agent or PFM - RM. For details on how to perform unsetup and how to uninstall PFM - Agents or PFM - RM, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

If the instance of PFM - Agent or PFM - RM that will be deleted is on the same node as PFM - Manager, it is necessary to restart PFM - Manager after the unsetup and uninstallation have been performed. Go to step 3.

### 4. Apply the agent information to PFM - Manager.

Synchronize the agent information between PFM - Manager and PFM - Web Console so that the deletion takes effect in PFM - Web Console. To synchronize the agent information, use the `jpctool service sync` command.

The time when the agent information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console. For details about the `jpctool service sync` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

Note: When performing unsetup of the PFM - RM remote agent

Because the service information is deleted automatically when you unset up the PFM - RM remote agent (by using the `jpccconf target unsetup` command), you do not need to execute the `jpctool service delete` command.

However, you do need to execute the `jpctool service sync` command to apply the changes to PFM - Web Console after the unsetup process.

The following describes when the service information is deleted.

- If PFM - Manager and the PFM - RM you are deleting are running  
When you execute the `jpccconf target unsetup` command, PFM - RM issues a request to PFM - Manager to delete the service information. PFM - Manager then deletes the service information.
- If PFM - Manager or the PFM - RM service you are deleting is stopped  
PFM - Manager deletes the service information when the PFM - RM service starts and connects to PFM - Manager after the `jpccconf target unsetup` command is executed.

## (2) Deleting PFM - Agent or PFM - RM from PFM - Web Console

### 1. Close and re-open PFM - Web Console on the executing node.

Apply the changes made by the deleted PFM - Agent or PFM - RM information to PFM - Web Console.

After executing the `jpctool service sync` command, close and re-open PFM - Web Console on the executing node.

### 2. Delete agents from the Agents tree.

Delete agents that are no longer required from the **User Agents** node in the Agents tree, as needed.

For details on how to delete agents from the Agents tree, see [3.2 Creating and editing an Agents tree in a Web browser](#) or [3.3 Using commands to create and edit an Agents tree](#).

3. Delete the alarm definition information and report definition information.

Delete the unnecessary alarm definition information and report definition information as necessary.

For details on deleting alarm definition information, see [6.4.9\(2\) Deleting an alarm](#) or [6.7.6 Deleting an alarm](#). For details on deleting report definition information, see [5.3.12\(2\) Deleting a report](#) or [5.5.2 Deleting an unnecessary report](#).

### 10.3.3 Changing logical host names after starting operation

This subsection describes the procedures (performed on the Performance Management system) necessary for changing the host names of the PFM - Manager host, PFM - Agent host, or PFM - RM host after the Performance Management system has been configured.

To change a logical host name, you must first use the `jpccconf host hostname` command to change the monitoring host name.

If you execute the `jpccconf host hostname` command, all existing information, including definition and performance information, is inherited. For details on the `jpccconf host hostname` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

#### (1) Changing the PFM - Manager logical host name

##### (a) Overview of changing the PFM - Manager logical host name

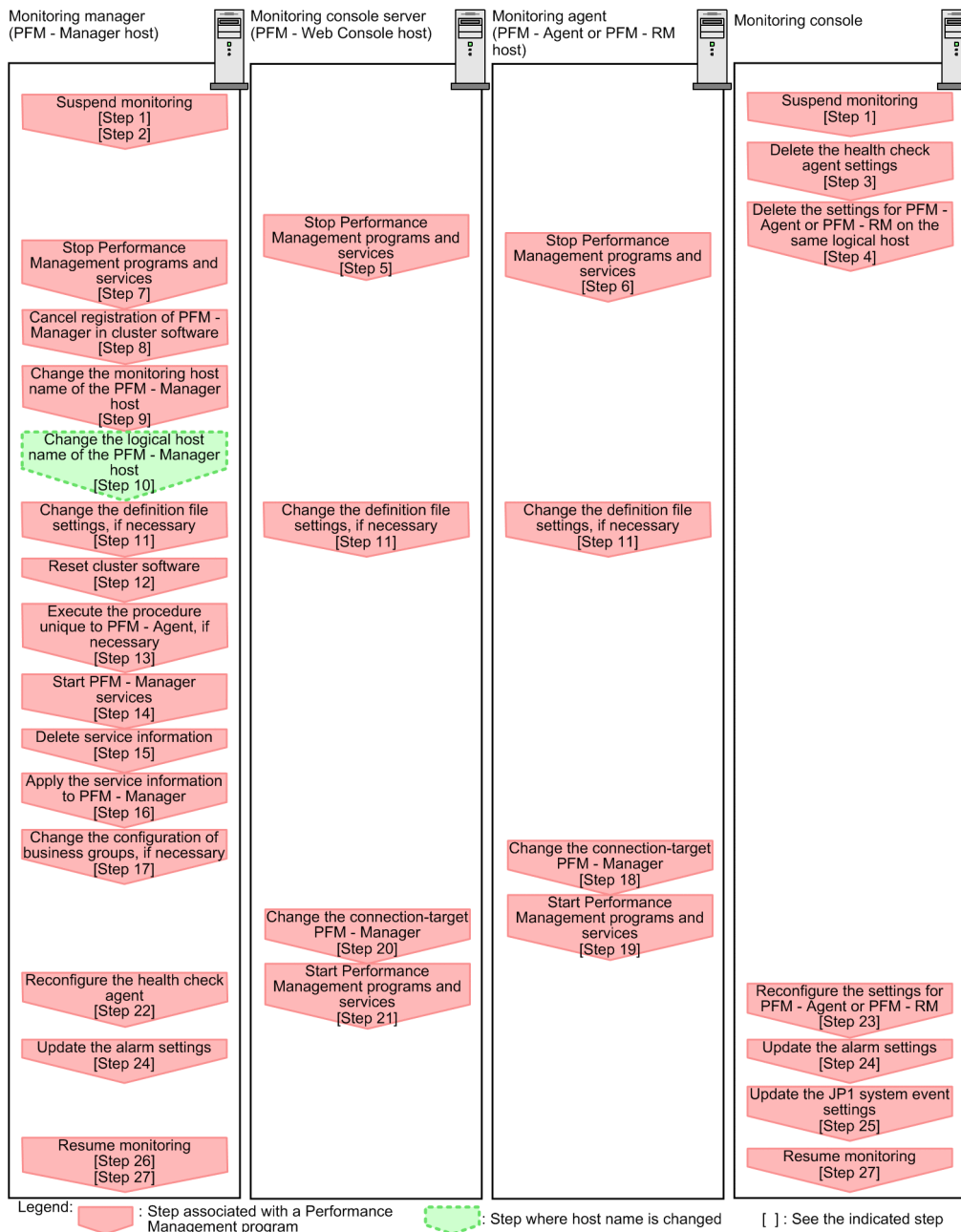
You must work on the following hosts when changing the PFM - Manager logical host name:

- PFM - Manager host
- PFM - Web Console host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Before performing this task in a system that links with JP1/SLM, refer to [13.4.1 Changing host names after linking with JP1/SLM](#).

Figure 10–18: Changing the PFM - Manager logical host name



## (b) Procedure for changing the PFM - Manager logical host name

Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Suspend monitoring for the PFM - Manager host whose host name is to be changed.  
If you do not want health check events to occur while changing the host name, suspend monitoring for the host whose name is to be changed. You can do so by using the `jpctool monitor suspend` command of the PFM - Manager host or from the monitoring console.  
For details on suspending monitoring, see [8. Suspending and Resuming Monitoring](#).
2. Suspend monitoring with the new host name specified.  
If you suspend monitoring in step 1, you also need to suspend monitoring with the new host name specified.  
In this case, use the `-force` option of the `jpctool monitor suspend` command of the PFM - Manager host.

3. Delete the settings for the health check agent.

If you are using the health check function, you can delete the agent definitions for the health check agent using your PFM - Web Console (by deleting the definitions from the management folder in the Agents tree and removing the association between the alarm tables and the definitions). For details on how to change the agent definition, see [6. Monitoring Operations with Alarms](#).

4. Delete the settings for PFM - Agent or PFM - RM.

You can use the PFM - Web Console to delete the agent definitions for the logical PFM - Agent host or logical PFM - RM host installed on the same host as the PFM - Manager whose logical host name is to be changed. This involves deleting the definitions from the management folder in the Agents tree. For details about how to change agent definitions, see [3. Monitoring Agents](#).

5. Stop services on the PFM - Web Console host.

On the PFM - Web Console host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcwstop` command.

6. Stop services on the PFM - Agent or PFM - RM host.

On the PFM - Agent or PFM - RM host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcspm stop` command.

7. Stop services on the PFM - Manager host.

Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

8. Cancel the registration of PFM - Manager from the cluster software.

Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

9. Change the monitoring host name of PFM - Manager host.

Execute the `jpcconf host hostname` command to change the monitoring host name.

In the following example, the logical host name is changed from `lhostA` to `lhostB`.

```
jpcconf host hostname -lhost lhostA -newhost lhostB -d d:\backup -
dbconvert convert
```

For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

 **Note**

As a general rule, the directory specified in the `-d` option of the `jpcconf host hostname` command requires disk space equivalent to the total size of the PFM - Agent and PFM - RM Store databases and the import directory on the specified host. If you have made changes to the storage directory or import directory of the Store database, calculate the disk space requirements with reference to the size of the database in the new location.

For example, if PFM - Agent for HiRDB and PFM - Agent for Oracle are located in the environment directory, the directory must have free disk space equivalent to the size of the Store databases in the environment directory plus the size of the database in the import directory. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

10. Change the PFM - Manager logical host name.



Change the PFM - Manager logical host name.

11. Edit the settings in the `hosts` and `jpchosts` files so that the new host name can be resolved to an IP address in the Performance Management system, if necessary.

12. Reconfigure the cluster software

For details, see [10.2.2\(4\) Cluster software setting procedure](#).

13. Perform any PFM - Agent-specific steps, if necessary.

If PFM - Agent has been installed on the PFM - Manager host, the PFM - Agent-specific procedure might be necessary. The following table describes whether the PFM - Agent-specific procedure is necessary.

**Table 10–5: Whether the PFM - Agent-specific procedure is necessary**

Configuration		Necessity and reference
The version of PFM - Agent installed on the PFM - Manager host is 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The version of PFM - Agent installed on the PFM - Manager host is earlier than 09-00.	The following PFM - Agents: <ul style="list-style-type: none"> <li>• PFM - Agent for Cosminexus</li> <li>• PFM - Agent for Domino</li> <li>• PFM - Agent for Enterprise Applications</li> <li>• PFM - Agent for Microsoft SQL Server</li> </ul>	The PFM - Agent-specific procedure is necessary. For details about the procedure, see <a href="#">10.3.3(4) Optional PFM - Agent-specific steps for host name changes</a> .
	Other than the above	The PFM - Agent-specific procedure is not necessary.

If a PFM - Agent-specific step is to be performed, complete the reference step shown in this table before proceeding to the next step.

14. Start services on the PFM - Manager host.

Use the cluster software to start all PFM - Manager services.

15. Delete service information on the PFM - Manager host.

Even though the PFM - Manager host name is changed, the service information of the Performance Management programs with the old host name remains the same. Therefore, you need to delete unnecessary information.

The types of service information that you need to delete and the method of checking the service information are described as follows:

*Service information on the host with the old host name*

All the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id * -host old-host-name -lhost new-host-name
```

*Service information whose service ID contains the old host name*

Items whose Service ID column contains the old host name of the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id * -lhost new-host-name
```

Service information can be deleted by using the `jpctool service delete` command.

Delete service information on the host with the old host name by using the following command:



```
jpctool service delete -id * -host old-host-name -lhost new-host-name
```

Additionally, delete service information whose service ID contains the old host name by using the following command:

```
jpctool service delete -id ???old-host-name -host new-host-name -lhost  
new-host-name
```

If the message KAVE05233-W is issued during command execution because of a service information deletion error, re-execute the command as follows:

```
jpctool service delete -id * -host old-host-name -lhost new-host-name -  
force  
jpctool service delete -id ???old-host-name -host new-host-name -lhost  
new-host-name -force
```

#### Note

Even though you execute the `jpctool service list` command, old service information that contains the old host name might not be displayed. Because such service information also needs to be deleted from the database, you must execute the `jpctool service delete` command shown above.

For details on the commands, see the chapter that describes the commands in the manual *JPI/Performance Management Reference*.

#### 16. Apply the service information to PFM - Manager.

Synchronize the service information between PFM - Manager and PFM - Web Console so that the deletion takes effect in PFM - Web Console. To synchronize the service information, use the `jpctool service sync` command.

The time when the service information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console. For details about the `jpctool service sync` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

#### 17. Change the business group configuration if needed.

If the PFM - Manager host whose logical host name you changed is assigned to a business group, you need to change the configuration of the business group. For details on how to do this, see [2. Managing User Accounts and Business Groups](#).

#### 18. Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host.

Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the logical host name. Use the `jpccconf mgrhost define` command to change the settings for PFM - Manager for the connection destination.

(Specify the same settings on the physical host of both the executing and standby nodes of the PFM - Manager environment.)

For example, if the host name of PFM - Manager for the connection destination is changed to `host01`, specify and execute the command as follows:

```
jpccconf mgrhost define -host lhostB
```

In this example, the `jpccconf mgrhost define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf mgrhost define` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

#### 19. Start services on the PFM - Agent or PFM - RM host.

Start the Performance Management programs and services on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the logical host name. To start services, use `jpcspm start` command.

20. Change PFM - Manager for the connection destination on the PFM - Web Console host.

Change the settings for PFM - Manager for the connection destination on the PFM - Web Console host connected to PFM - Manager for which you have changed the logical host name. Change the information in the Windows initialization file (`config.xml`) to change the settings for PFM - Manager for the connection destination. For details, see the chapter describing installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

21. Start services on the PFM - Web Console host.

Start the Performance Management programs and services on the PFM - Agent host connected to PFM - Manager for which you have changed the logical host name. To start services, use the `jpcwstart` command.

22. Reconfigure the definition for the health check agent.

If you have been using the health check function, reconfigure the definition (that was deleted in step 3) of the health check agent after changing the host name.

23. Reconfigure the definition of PFM - Agent or PFM - RM.

Reconfigure the definition (that was deleted in step 4) of the logical PFM - Agent or logical PFM - RM installed on the same host as PFM - Manager for which the logical host name was changed.

24. Update the alarm settings.

In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

- The action handler of the PFM - Manager host is specified for the action handler that executes actions.  
Edit the alarm to set `PH1<new-pfm-manager-host-name>` for the action handler that executes actions.
- JP1 events are issued by actions.  
Set the JP1 event settings in the action again.

For details on how to edit alarms, see *6. Monitoring Operations with Alarms*.

25. Update the JP1 system event settings.

If either of the following conditions is met, use your PFM - Web Console to update the JP1 system event settings:

- The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
- The old host name is specified as the name of the monitoring console host for JP1 system events.

For details on the JP1 system events, see *12.2 JP1 events issued from Performance Management to JP1/IM*.

26. Resume monitoring with the old host name specified.

If you suspend monitoring in step 1, you need to resume monitoring with the old host name specified to delete the settings information of monitoring suspension for the old host name.

In this case, use the `-force` option of the `jpctool monitor resume` command of the PFM - Manager host.

27. Resume monitoring for the PFM - Manager host whose host name was changed.

If you suspend monitoring in step 2, use the `jpctool monitor resume` command of the PFM - Manager host or use the monitoring console to resume monitoring on the PFM - Manager host.

28. Check whether the JP1 system event settings are properly updated.

Check the following items after changing the logical host name:

- Collection of performance data  
Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).
- Execution of the `jpcrept` command  
Make sure that there is no problem in outputting the collected performance data.
- The report definitions and alarm definitions  
Make sure that there are no problems with the report definitions and alarm definitions created from the Web browser.
- The actions  
Make sure that there is no problem in executing the created actions.

## **(2) Changing the PFM - Agent or PFM - RM logical host name**

### **(a) Overview of changing the PFM - Agent or PFM - RM logical host name**

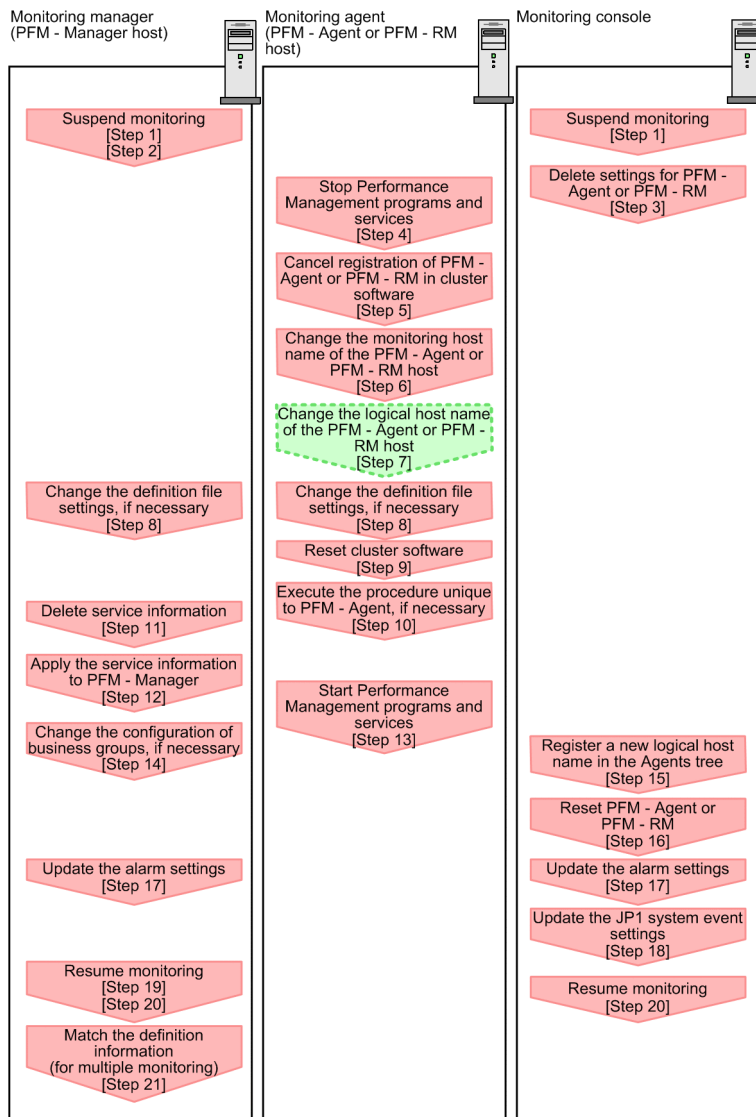
You must work on the following hosts when changing the PFM - Manager or PFM - RM logical host name:

- PFM - Manager host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Before performing this task in a system that links with JP1/SLM, refer to *13.4.1 Changing host names after linking with JP1/SLM*.

Figure 10–19: Changing the logical host name of PFM - Agent or PFM - RM



## (b) Procedure for changing the PFM - Agent or PFM - RM logical host name

Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Suspend monitoring for the PFM - Agent or PFM - RM host whose host name is to be changed.
 

If you do not want health check events to occur while changing the host name, suspend monitoring for the host whose name is to be changed. You can do so by using the `jpctool monitor suspend` command of the PFM - Manager host or from the monitoring console.

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on suspending monitoring, see [8. Suspending and Resuming Monitoring](#).
2. Suspend monitoring with the new host name specified.
 

If you suspend monitoring in step 1, you also need to suspend monitoring with the new host name specified.

In this case, use the `-force` option of the `jpctool monitor suspend` command of the PFM - Manager host.

In a multiple-monitoring configuration, perform this step on the primary manager.

3. Delete the PFM - Agent or PFM - RM information.

Use the PFM - Web Console to delete the agent definitions from the PFM - Agent or PFM - RM host whose logical host name will be changed (by deleting the definitions from the management folder in the Agents tree and removing the association between the alarm tables and the definitions).

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on how to change agent definitions, see [3. Monitoring Agents](#) or [6. Monitoring Operations with Alarms](#).

4. Stop the services on the PFM - Agent or PFM - RM host.

Stop all Performance Management programs and services on the PFM - Agent or PFM - RM host for which you intend to change the logical host name. Use operations from the cluster software to stop Performance Management programs and the services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

5. Unregister PFM - Agent or PFM - RM from the cluster software.

Delete the settings related to PFM - Agent or PFM - RM on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

6. Change the monitoring host name for the PFM - Agent or PFM - RM host.

Execute the `jpccconf host hostname` command to change the monitoring host name.

In the following example, the logical host name is changed from `lhostA` to `lhostB`.

```
jpccconf host hostname -lhost lhostA -newhost lhostB -d d:\backup -
dbconvert convert
```

Note:

After executing the above command, do not execute any other Performance Management commands until you change the host name in the next step.

For details on the `jpccconf host hostname` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

 **Note**

As a general rule, the directory specified in the `-d` option of the `jpccconf host hostname` command requires disk space equivalent to the total size of the PFM - Agent and PFM - RM Store databases and the import directory on the specified host. If you have made changes to the storage directory or import directory of the Store database, calculate the disk space requirements with reference to the size of the database in the new location.

For example, if PFM - Agent for HiRDB and PFM - Agent for Oracle are located in the environment directory, the directory must have free disk space equivalent to the size of the Store databases in the environment directory plus the size of the database in the import directory. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

7. Change the PFM - Agent or PFM - RM logical host name.

Change the PFM - Agent or PFM - RM logical host name.

8. Edit the settings in the `hosts` and `jpchosts` files so that the new host name can be resolved to an IP address in the Performance Management system, if necessary.

9. Configure the cluster software.

For details, see [10.2.2\(4\) Cluster software setting procedure](#).

10. Perform any PFM - Agent-specific steps, if necessary.

The following table describes whether the PFM - Agent-specific procedure is necessary.

**Table 10–6: Whether the PFM - Agent-specific procedure is necessary**

Configuration		Necessity and reference
The monitoring host name to be changed is PFM - Agent version 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary, depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The monitoring host name to be changed is PFM - Agent for versions earlier than 09-00.	The following PFM - Agents: <ul style="list-style-type: none"> <li>• PFM - Agent for Cosminexus</li> <li>• PFM - Agent for Domino</li> <li>• PFM - Agent for Enterprise Applications</li> <li>• PFM - Agent for Microsoft SQL Server</li> </ul>	The PFM - Agent-specific procedure is necessary. For details about the procedure, see <a href="#">10.3.3(4) Optional PFM - Agent-specific steps for host name changes</a> .
	Other than the above	The PFM - Agent-specific procedure is not necessary.

If a PFM - Agent-specific step is to be performed, complete the reference step shown in this table before proceeding to the next step.

11. Delete service information on the PFM - Manager host.

Even though the PFM - Agent or PFM - RM host name is changed, the service information of the Performance Management programs with the old host name remains the same. Therefore, you need to delete unnecessary information from the PFM - Manager host. In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

The types of service information that you need to delete and the method of checking the service information are described as follows:

*Service information on the host with the old host name*

All the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id * -host old-host-name
```

*Service information whose service ID contains the old host name*

Items whose Service ID column contains the old host name of the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id *
```

Service information can be deleted by using the `jpctool service delete` command.

Delete service information on the host with the old host name by using the following command:

```
jpctool service delete -id * -host old-host-name
```

Additionally, delete service information whose service ID contains the old host name by using the following command:

```
jpctool service delete -id ???old-host-name -host new-host-name
```

If the message KAVE05233-W is issued during command execution because of a service information deletion error, re-execute the command as follows:

```
jpctool service delete -id * -host old-host-name -force
jpctool service delete -id ???old-host-name -host new-host-name -force
```

#### Note

Even though you execute the `jpctool service list` command, old service information that contains the old host name might not be displayed. Because such service information also needs to be deleted from the database, you must execute the `jpctool service delete` command shown above.

For details on the commands, see the chapter that describes the commands in the manual *JP1/Performance Management Reference*.

#### 12. Apply the service information to PFM - Manager.

Synchronize the service information between PFM - Manager and PFM - Web Console so that the deletion takes effect in PFM - Web Console. To synchronize the service information, use the `jpctool service sync` command.

In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

The time when the service information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console. For details about the `jpctool service sync` command, see the chapter that describes commands in the manual *JP1/Performance Management Reference*.

#### 13. Start services on the PFM - Agent or PFM - RM host.

Start Performance Management programs and services from the cluster software on the PFM - Agent or PFM - RM host for which you have changed the logical host name.

#### 14. Change the business group configuration if needed.

If the PFM - Agent host or PFM - RM host whose logical host name you changed is assigned to a business group, you need to change the configuration of the business group.

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on how to do so, see [2. Managing User Accounts and Business Groups](#).

#### 15. Register the new logical host name in the management folder in the Agents tree as needed.

Register the PFM - Agent or PFM - RM host whose logical host name you changed in the management folder in the Agents tree of PFM - Web Console. For details on how to register a host in the management folder, see [3. Monitoring Agents](#).

#### 16. Reconfigure the definition of step 3 as needed.

Reconfigure the definitions (that were deleted in step 3) of the PFM - Agent or PFM - RM for which the logical host name was changed.

In a multiple-monitoring configuration, perform this step on the primary manager.

#### 17. Update the alarm settings.

In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

In a multiple-monitoring configuration, perform this step on the primary manager.

- When the action handler of the PFM - Agent or PFM - RM host is specified for the action handler that executes actions.

Edit the alarm to set `PH1<new-pfm-agent-or-pfm-rm-host-name>` for the action handler that executes actions.

For details on how to edit alarms, see [6. Monitoring Operations with Alarms](#).

#### 18. Update the JP1 system event settings.

If either of the following conditions is met, use your PFM - Web Console to update the JP1 system event settings:



In a multiple-monitoring configuration, perform this step on the primary manager.

- The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
- The old host name is specified as the name of the monitoring console host for JP1 system events.

For details on the JP1 system events, see *12.2 JP1 events issued from Performance Management to JP1/IM*.

#### 19. Resume monitoring with the old host name specified.

If you suspend monitoring in step 1, you need to resume monitoring with the old host name specified to delete the settings information of monitoring suspension for the old host name.

In this case, use the `-force` option of the `jpctool monitor resume` command of the PFM - Manager host.

In a multiple-monitoring configuration, perform this step on the primary manager.

#### 20. Resume monitoring for the PFM - Agent or PFM - RM host whose host name was changed.

If you suspend monitoring in step 2, use the `jpctool monitor resume` command of the PFM - Manager host or use the monitoring console to resume monitoring for the PFM - Agent or PFM - RM host.

In a multiple-monitoring configuration, perform this step on the primary manager.

#### 21. Match the definitions on the primary manager and the secondary manager (in a multiple-monitoring configuration).

Export the definitions for the multiple-monitoring configuration from the primary manager and import them to the secondary manager so that the primary manager and the secondary manager have the same definitions.

For details about how to match the definition information, see *11.5 Duplicating definition information*.

#### 22. Check whether the JP1 system event settings are properly updated.

Check the following items after changed the settings:

- Collection of the performance data  
Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).
- Execution of the `jpcrept` command  
Make sure that there is no problem in outputting the collected performance data.
- The report definitions and alarm definitions  
Make sure that there are no problems with the report definitions and alarm definitions created from the Web browser.
- The actions  
Make sure that there is no problem in executing the created actions.

### (3) Changing the PFM - Web Console logical host name

To change the PFM - Web Console logical host name:

Before performing this task in a system that links with JP1/SLM, refer to *13.4.1 Changing host names after linking with JP1/SLM*.

#### 1. Stop services on the PFM - Web Console host.

Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

#### 2. Cancel the registration of PFM - Web Console from the cluster software.



Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

3. Edit the PFM - Web Console host information in the Windows initialization file (`config.xml`) to refer to the new logical host name.

This step is necessary when the logical host name has been set for the `ownHost` parameter in the `<vsa>` - `<vserver-connection>` tag of the Windows initialization file (`config.xml`).

For details on how to edit the host information, see [10.2.3\(3\)\(c\) Setting up PFM - Web Console \(logical host\)](#) and [10.2.3\(3\)\(h\) Copying the settings file to the executing node](#).

4. If the integrated management product (JP1/IM) is linked for operation monitoring, change the host name specified in each applicable definition file or in the property value for each service.

- If a JP1 user event is used:  
Change the host name in the definition files for the tool launcher and for opening monitor windows. For details, see [12.3.2\(4\) Editing and copying the definition files for linkage](#).
- If a JP1 system event is used:  
Change the host name in the Monitoring Console Host property value for each service. For details, see [12.3.2\(1\) Configuring so that JP1 events are issued](#).
- If the setting is specified to display Performance Management reports from events in the integrated console:  
Change the PFM - Web Console host name specified in the performance report definition file (`performance.conf`).

For details on an integrated management product (JP1/IM), see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

5. If the job management product (JP1/AJS3) is linked for operation monitoring, change the host name.

Change the PFM - Web Console host name specified in the JP1/AJS3 - Web Console environment-settings file (`ajs3web.conf`).

6. Change the PFM - Web Console logical host name.

7. If encrypted communication between a web browser and the monitoring console server is enabled, re-obtain certificates.

You must re-obtain certificates under the new host name.

For details, see the section on changing the settings for encrypted communication between a web browser and the monitoring console server in the *JP1/Performance Management Planning and Configuration Guide*.

8. Reconfigure the cluster software.

For details on the setting procedure, see [10.2.3\(4\) Cluster software setting procedure](#).

9. Start services on the PFM - Web Console host.

Use operations from the cluster software to start the PFM - Web Console services.

10. If the integrated management product (JP1/IM) is linked, restart the product (JP1/IM).

You can also apply the settings by executing the JP1/IM `jco_spmd_reload` command. For details about this command, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

11. If the job management product (JP1/AJS3) is linked for operation monitoring, restart the services of JP1/AJS3.

## (4) Optional PFM - Agent-specific steps for host name changes

This subsection describes the PFM - Agent-specific steps necessary to perform the following operations for each product:

- Changing the PFM - Manager logical host name
- Changing the PFM - Agent or PFM - RM logical host name

For details on when it is necessary to perform these steps, see [10.3.3\(1\) Changing the PFM - Manager logical host name](#) and [10.3.3\(2\) Changing the PFM - Agent or PFM - RM logical host name](#).

### (a) PFM - Agent for Cosminexus

Edit the definition files in all of the existing instance environments.

- Definition file  
`environment-directory\agtc\agent\instance-name\jpcagt.ini`
- What to edit  
Specify a new host name as the value of the `COSMI_HOST` entry in the `[Agent]` section.

### (b) PFM - Agent for Domino

*Note:*

Perform the following procedure only if you use the health check function provided by PFM - Agent for Domino.

Edit the definition files in all of the existing instance environments.

- Definition file  
`environment-directory\agt1\agent\instance-name\jpcagt.ini`
- What to edit  
Specify a new host name as the value of the following entries in the `[Health Check Options]` section:
  - Host entry in the `[[HTTP Port Check]]` subsection
  - Host entry in the `[[SMTP Port Check]]` subsection
  - Host entry in the `[[POP3 Port Check]]` subsection
  - Host entry in the `[[LDAP Port Check]]` subsection
  - Host entry in the `[[NNTP Port Check]]` subsection

### (c) In PFM - Agent for Enterprise Applications

Execute the `jpcconf inst setup` command for all created instance environments. For example, if an instance environment `o246bcisD500` exists in PFM - Agent for Enterprise Applications, execute the following command:

```
jpcconf inst setup -key agtm -inst o246bcisD500 -lhost jp1-halr3
```

The `jpcconf inst setup` command is an interactive command that returns a command prompt when executed.

At the `ASHOST` prompt, enter the new host name, and press the **Enter** key when the other prompts come up. If you press the **Enter** key at a prompt without entering a value, the existing value is assumed.

## (d) In PFM - Agent for Microsoft SQL Server

Execute the `jpccconf inst setup` command for all created instance environments. For example, if an instance environment `default` exists in PFM - Agent for Microsoft SQL Server, execute the following command:

```
jpccconf inst setup -key agtq -inst default -lhost jp1-halSQL
```

In this example, the `jpccconf inst setup` command is executed in interactive mode. However, the command can also be executed in non-interactive mode.

When you execute the `jpccconf inst setup` command, specify the new host name at the `SQL_HOST` prompt. The other items are optional. Items for which you do not specify a value retain the existing setting.

## 10.3.4 Changing the logical host environment after starting operation

This subsection describes how to perform operations such as modifying the `jpchosts` file and changing port numbers or the environment directory path when Performance Management is running in a logical host environment.

These settings are required if you want to start PFM - Manager in a logical host environment.

### (1) Modifying the `jpchosts` file

If you are already using Performance Management in a logical host environment, use the following procedure to modify the `jpchosts` file:

1. Edit the `jpchosts` file on the executing node.
2. Copy the `jpchosts` file from the executing node to the standby node.

### (2) Changing or adding port numbers

To change or add a port number when you are already using Performance Management in a logical host environment:

1. Set the port numbers by executing the `jpccconf port define` command on the executing node.

Place the shared disk online before you execute the command.

For example, execute the following command to set all of the port numbers for the services on the logical host `jp1-hal` to the default values.

```
jpccconf port define -key all -lhost jp1-hal
```

When you execute the `jpccconf port define` command, the port numbers and service names of Performance Management (by default, TCP services whose names start with `jp1pc`) are defined in the `services` file.

For details on how to set port numbers, see the chapter describing installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

For details on the `jpccconf port define` command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

2. Execute the `jpccconf ha export` command on the executing node.

The settings for Performance Management in the logical host environment are exported to a file you specify.

For example, execute the command as follows to export the settings for the logical host environment to the file `lhostexp.conf`:

```
jpccconf ha export -f lhostexp.conf
```

3. Copy the file you exported using the `jpccconf ha export` command from the executing node to the standby node.

4. Execute the `jpccconf ha import` command to import the exported file into the standby node.

The shared disk does not need to be online on the standby node during this step.

The environment definition file exported from the executing node is imported into the standby node.

For example, execute the command as follows to import the file `lhostexp.conf`:

```
jpccconf ha import -f lhostexp.conf
```

When you execute the `jpccconf ha import` command, the environment of the standby node becomes the same environment as the executing node.

### (3) Changing the environment directory path

To change the environment directory path when you are already using Performance Management in a logical host environment:

- For PFM - Manager, PFM - Base, PFM - Agent, and PFM - RM

The logical host must be set up again. Use the following procedure to perform migration. For details about how to unset up and set up PFM - Agent or PFM - RM as described in steps 2 and 3, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

1. Back up the definition information or operation monitoring data.
2. Unset up the logical host environment.
3. Set up the logical host with a new environment directory path specified.
4. Restore the definition information or operation monitoring data.

- For PFM - Web Console

1. Stop PFM - Web Console.
2. Change the environment directory path.

For details, see *10.2.3(3)(d) Setting up the storage location for bookmark definition information* and *10.2.3(3)(e) Setting the storage location for process monitoring definition templates*.

When you want to inherit the bookmark definition information and process monitoring definition templates, copy the appropriate folder beforehand.

3. Start PFM - Web Console.

## 10.4 Configuration in a cluster system (in UNIX)

---

### 10.4.1 Before installation and setup

#### (1) Prerequisite conditions

##### (a) Cluster system

Make sure that the following conditions are satisfied:

- The cluster system is controlled by cluster software.
- Settings are made so that the starting and stopping of Performance Management used on a logical host are controlled by cluster software.

##### (b) Shared disk

Make sure that the following conditions are satisfied:

- Each logical host has a shared disk, and the disk can be taken over from the executing node by the standby node.
- Shared disks are physically connected to each node via Fibre Channel or SCSI. Configurations in which the shared disk is a network drive or disk replicated over a network is used are not supported.
- When a failover occurs, if some processes are still using the shared disks, make sure it is still possible to force shared disks offline via cluster software or by other means and perform a failover.
- If multiple Performance Management programs are executed on a single logical host, make sure the directory names for the shared disks are the same. For Store databases, make sure the storage destination can be changed to allow storage in a different directory on the same shared disk.

##### (c) Logical host name and logical IP address

Make sure that the following conditions are satisfied:

- There is a logical host name and corresponding logical IP address for each logical host, and switching from the executing node to the standby node can be performed.
- The logical host and logical IP address are set in the `hosts` file and on the name server.
- If using a DNS, a logical host name is specified without a domain name, instead of by using a FQDN.
- Each physical host name and logical host name is unique within the system.

#### Important

Notes regarding logical host names:

- Do not use a physical host name (a host name displayed using the `uname -n` command) for a logical host name. Otherwise, normal communication processing might be prevented.
- Logical host names must consist of from 1 to 32 bytes alphanumeric characters.
- `localhost`, an IP address, or a string that begins with a hyphen (-) cannot be used for a logical host name.

### (d) Other prerequisite conditions

Make sure that the following conditions are satisfied:

- Kernel parameters have been optimized.

## (2) Checking the setup environment

In addition to the environment information normally required to set up Performance Management, the following information is required to set up Performance Management used on a logical host.

Table 10–7: Information required to set up PFM - Manager to be used on a logical host (in UNIX)

Item	Example
Logical host name	jp1-ha1
Logical IP address	172.16.92.100
Shared disk	/usr/jp1

If multiple instances of Performance Management use a single logical host, each instance uses the directory of the same shared disk.

## (3) Notes about upgrading when a logical host is used

To upgrade PFM - Manager on a logical host, you must place a shared disk online on either an executing or a standby node.

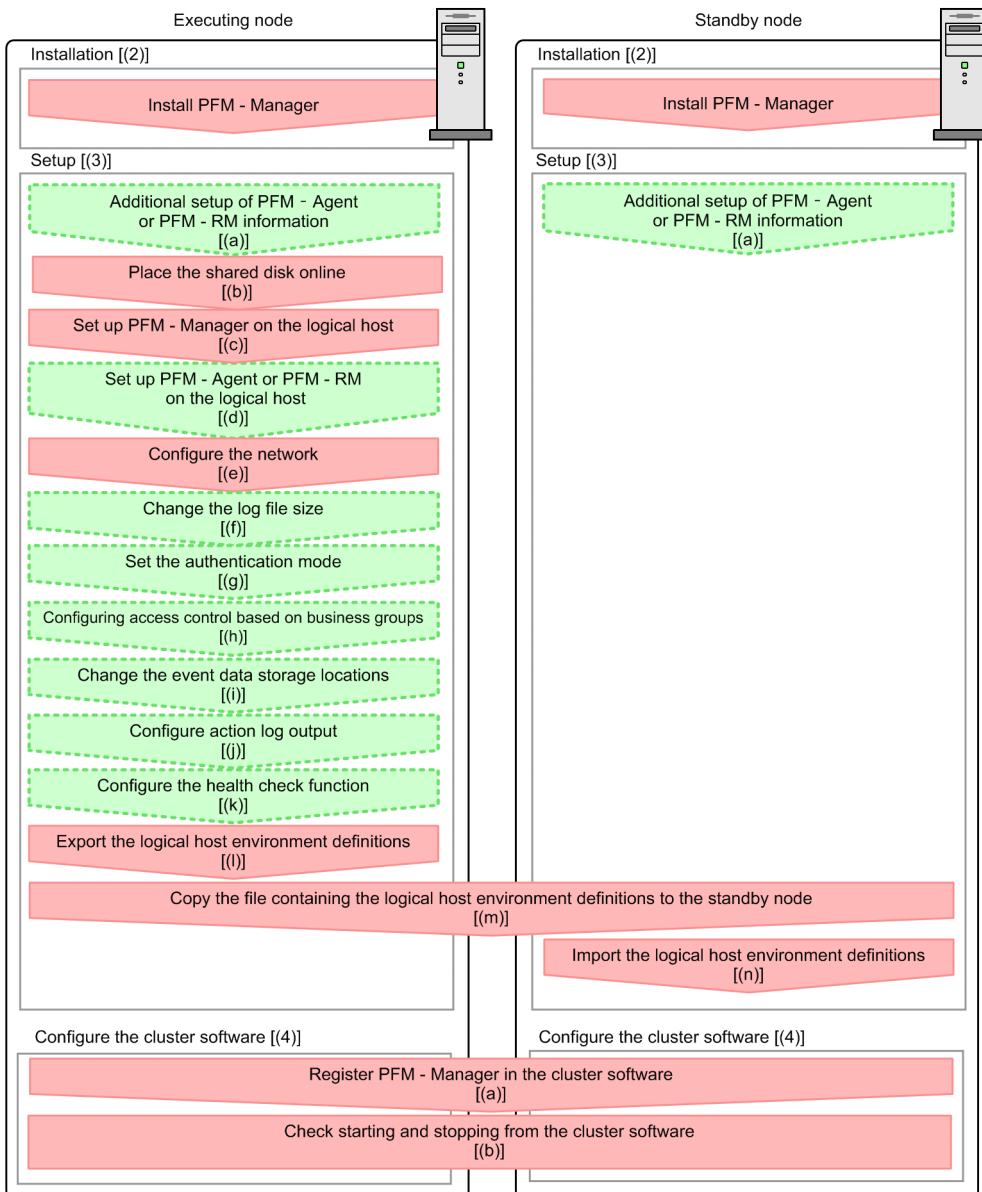
However, there is no need to place a shared disk online to upgrade PFM - Web Console in a cluster environment.

## 10.4.2 Installing and setting up PFM - Manager

### (1) Process flow for installation and setup

The following figure shows the process flow for installation and setup of PFM - Manager used on a logical host.

Figure 10–20: Process flow for installation and setup of PFM - Manager used on a logical host (in UNIX)

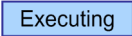
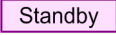
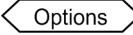


Legend:  
 : Mandatory step   
 : Optional step   
 [ ] : See the indicated section

### Important

- When PFM - Manager in a logical host environment is set up, PFM - Manager for the physical host environment can no longer be executed. However, the Action Handler service can still be executed, because it uses PFM - Agent or PFM - RM in the physical host environment.  
 When unsetup is performed on PFM - Manager in a logical host environment, PFM - Manager in the physical host environment can once again be executed.
- When PFM - Manager in a logical host environment is set up, the definitions for PFM - Manager in the physical host environment are inherited by the logical host environment. However, the content of the Store database is not inherited. If unsetup is performed on PFM - Manager in the logical host environment, the definitions for the logical host environment and the Store database are deleted, and therefore switching to the physical host environment is not possible.

- Do not manually set `JPC_HOSTNAME` as an environment variable because it is used for Performance Management as an environment variable. If you specify this setting, Performance Management will not run correctly.
- For PFM - Manager of the version 09-00 or later, when you set up a new instance of PFM - Manager in a logical host environment, the settings of the health check function in the physical host environment are inherited by the logical host environment. You must modify the settings of the health check function, if necessary.
- In a logical host environment, the function for setting monitoring-host names cannot be used. The `jpccomm.ini` file on a logical host is ignored and the host name for the logical host is used.
- If the monitoring suspension function is enabled, monitoring for all the hosts and agents must be resumed before setup.

In the procedure explanation, the image  indicates items to be performed on the executing node, and the image  indicates items to be performed on the standby node. In addition, the image  indicates setup items that are either required depending on the environment or can be performed if you want to set a value other than the default settings.

## (2) Installation procedure

Perform a new installation of PFM - Manager on the executing node and the standby node. The installation procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

Note:

The installation destination is the local disk. Do not install PFM - Manager on the shared disk.

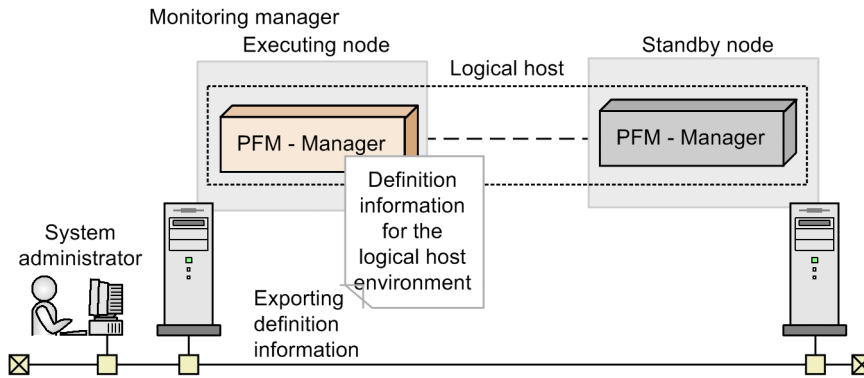
## (3) Setup procedure

Perform PFM - Manager setup on the executing node first. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the setup content from the executing node to the standby node.

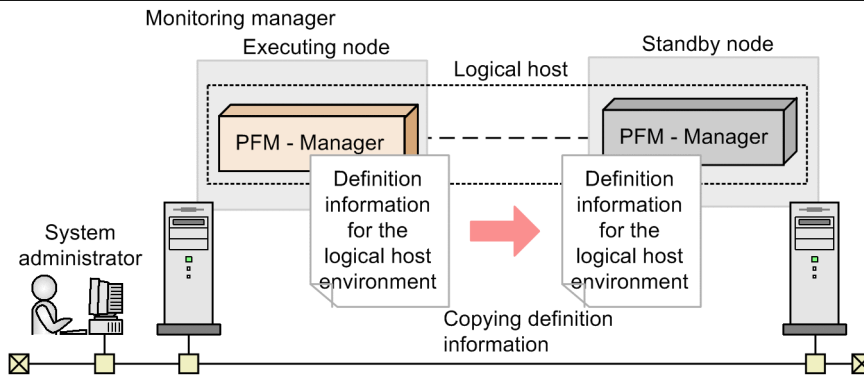


Figure 10–21: Method for applying the content set up on the executing node to the standby node

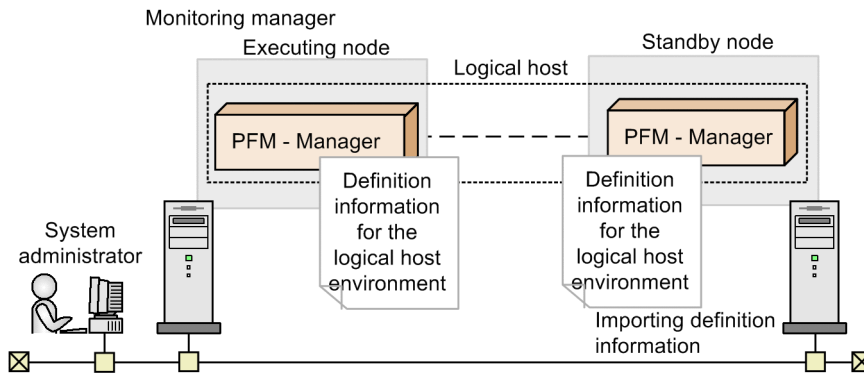
[Step 1] Set up the executing node.



[Step 2] Copy definition information from the executing node to the standby node.



[Step 3] Set up the standby node.



Each setup procedure is explained below.

**(a) Specifying the LANG environment variable** Executing Standby

Specify the LANG environment variable on the executing node and the standby node.

For details about how to specify the LANG environment variable, see the section on setting the LANG environment variable in the *JP1/Performance Management Planning and Configuration Guide*.

**(b) Performing an additional setup for PFM - Agent or PFM - RM information** Executing

Standby Options

To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Manager for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

The setup procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

Note:

If you add another PFM - Agent or PFM - RM to the same host as PFM - Manager, an additional setup is not required.

### (c) Making sure the shared disk is mounted Executing

Make sure that the shared disk is mounted. If the shared disk is not mounted, execute the `mount` command to mount the file system.

Note:

If setup is performed without mounting the shared disk, files might be created on the local disk.

### (d) Setting up a logical host for PFM - Manager Executing

Set up the logical host environment for PFM - Manager on the executing node. Before performing setup, stop all the Performance Management programs and services throughout the entire system.

#### 1. Create a logical host environment.

Execute the `jpccconf ha setup` command to create a logical host environment for PFM - Manager.

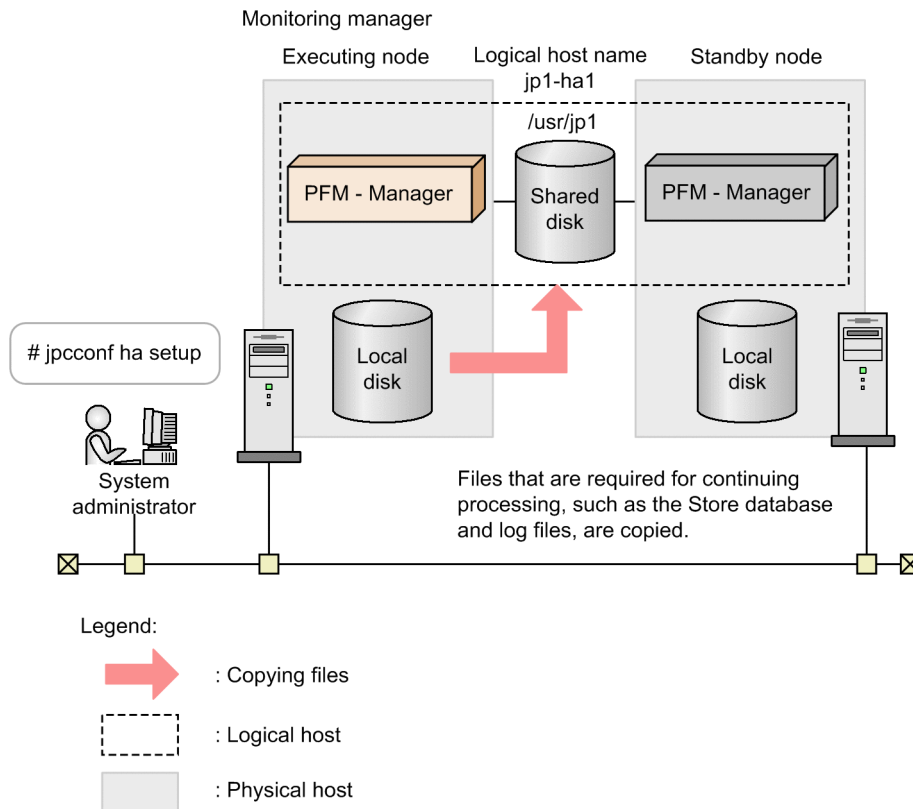
Use `-lhost` to specify the logical host name. For DNS operation, specify a logical host name that does not include a domain name. Specify the `-d` environment directory name for the directory name of the shared disk.

For example, execute the following command to set up a logical host with `jp1-ha1` as the logical host name and `/usr/jp1` as the environment directory.

```
jpccconf ha setup -key Manager -lhost jp1-ha1 -d /usr/jp1
```

When this command is executed, the `jp1pc` directory is created under `/usr/jp1`, and the files required in the logical host environment are copied to the environment directory. The following figure shows an example.

Figure 10–22: Execution example of the `jpccconf ha setup` command



When the command is executed, the required data is copied from the local disk of the executing node to the shared disk, and the settings required for use on the logical host are performed.

When the PFM-Manager's logical host is set up, the connection-target PFM - Manager in the physical host environment is renamed to the specified logical host name.

For details on the `jpccconf ha setup` command, see the chapters that describes commands in the manual *JPI/Performance Management Reference*.

## 2. Check the settings for the logical host environment.

Execute the `jpccconf ha list` command to check the settings for the logical host, and make sure that the logical host environment that has been created is correct.

```
jpccconf ha list -key all
```

An example of executing this command is as follows:

```
# jpccconf ha list -key all
```

Logical Host Name	Key	Environment Directory	[Instance Name]
jp1-ha1	mgr	"/usr/jp1/jp1pc"	

KAVE05136-I The logical host startup information listing ended normally.

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (e) Performing a setup for a logical host of PFM - Agent or PFM - RM Executing

Options

This procedure is required only when there is a PFM - Agent or PFM - RM to set up in the same logical host in addition to PFM - Manager.

For details on the setup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

## (f) Specifying network settings Executing

To allow communication between PFM - Manager and PFM - Web Console using a logical host name or logical IP address, add the following line to `jpcvsvr.ini` (*environment-directory/jp1pc/mgr/viewsvr/jpcvsvr.ini*):

```
java.rmi.server.hostname=logical-host-name-or-logical-IP-address
```

For details on the host names used for communication between PFM - Manager, PFM - Web Console, and JP1/SLM, see the sections that describe port numbers in the manual *JP1/Performance Management Reference*.

In addition, use the following procedure when changing IP addresses and port numbers according to the network configuration.

- Setting up IPv6 communication

When using Performance Management in an IPv6 environment, enable IPv6 support by executing the `jpccconf ipv6 enable` command on the PFM - Agent, PFM - RM, and PFM - Manager hosts.

In a cluster system, execute the command on the executing and standby nodes.

Note that only IPv4 communication is supported between PFM - Manager and PFM - Web Console.

For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

- Setting the IP address Options

To set the IP addresses, directly edit the content of the `jpchosts` file. If you have edited the `jpchosts` file, copy the file from the executing node to the standby node.

For details on setting IP addresses, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

- Setting port numbers Options

This procedure is necessary only when running Performance Management in a network environment with a firewall. For Performance Management communications via a firewall, use the `jpccconf port define port` command to set a port number.

For example, execute the following command to set all port numbers for services that exist on the host with the logical host name `jp1-ha1` specified in the fixed values.

```
jpccconf port define -key all -lhost jp1-ha1
```

When this command is executed, definitions of the port number and service name (TCP service name beginning with `jp1pc` by default) for Performance Management are added to the services file.

For details on setting port numbers, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

In this example, the `jpccconf port define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf port define` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

- Setting the host name or IP address used for communication with PFM - Web Console and JP1/SLM

In the following situations, define the host name or IP address of PFM - Manager in the `jpccsvr.ini` file on the PFM - Manager host.

- IP address translation (NAT translation) takes place between the PFM - Manager host and the PFM - Web Console host.
- Multiple IP addresses are used between the PFM - Manager host and the PFM - Web Console host.
- When linking with JP1/SLM, IP address translation (NAT translation) takes place between the PFM - Manager host and the JP1/SLM host.
- When linking with JP1/SLM, multiple IP addresses are used between the PFM - Manager host and the JP1/SLM host.

For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

### (g) Changing the log file size Executing Options

The operating status of Performance Management is output to a dedicated log file called the *common message log*. This setting is required when if you want change this file size.

For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

### (h) Specifying settings for the authentication mode Executing Options

This setting is required only if you want to change the authentication mode of Performance Management from PFM authentication mode to JP1 authentication mode.

For details, see *2. Managing User Accounts and Business Groups*.

### (i) Specifying settings for access control based on business groups Executing

Options

This setting is required if you want to use business groups to manage users in Performance Management. You can enable or disable access control based on business groups by entering a setting in the startup information file (`jpccomm.ini`).

For details, see *2. Managing User Accounts and Business Groups*.

### (j) Changing the storage locations of event data Executing Options

The settings below are required if you want to change the storage destination, backup destination, or export destination of the event data managed by PFM - Manager.

By default, event data is stored in the following locations:

- Data storage folder: `environment-directory/jp1pc/mgr/store/`
- Backup folder: `environment-directory/jp1pc/mgr/store/backup/`
- Export folder: `environment-directory/jp1pc/mgr/store/dump/`

For details on how to change a destination, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

## (k) Specifying settings for action log output Executing Options

This setting is required if you want to output an action log when an alarm is issued. An action log is log information output in conjunction with the alarm function, when an aspect of the system (such as the system load) exceeds a threshold. For details on how to set this option, see the section describing action log output in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

## (l) Configuring the health check function Executing Options

1. Check the settings of the health check function.

Execute the following command on the PFM - Manager host on the executing node to display the setting of the health check function.

```
jpccconf hc display
```

When the command is executed, the setting for the health check function appears as follows:

- If the health check function is enabled: `available`
- If the health check function is disabled: `unavailable`

For details on the `jpccconf hc display` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

2. Change the setting of the health check function.

Execute the following command on the PFM - Manager host on the executing node to set up the health check function, if necessary.

- To enable the health check function:

```
jpccconf hc enable
```

- To disable the health check function:

```
jpccconf hc disable
```

For details on the `jpccconf hc enable` and `jpccconf hc disable` commands, see the chapter explaining the commands in the manual *JPI/Performance Management Reference*.

## (m) Exporting the logical host environment definitions Executing

When a logical host environment for PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file. To set up a different instance of Performance Management on the same logical host, perform an export after all setup procedures are completed.

1. Execute the `jpccconf ha export` command.

Export the logical host environment definitions to the desired file.

For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file.

```
jpccconf ha export -f lhostexp.conf
```

If the health check function is enabled for the PFM - Manager in the logical host environment you are exporting, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be exported.

In this example, the `jpccconf ha export` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha export` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (n) Copying the file containing the logical host environment definitions to the standby node

Executing

Standby

Copy the file that has been exported in step (m) from the executing node to the standby node, so that it will be applied on the standby node.

Next, unmount the file system to complete the work. If this shared disk will continue to be used, it is not necessary to unmount the file system.

Note:

Even if the shared disk is unmounted, if there is a `jp1pc` directory and associated files in the specified environment directory, setup is performed without mounting the shared disk. If that is the case, use the following procedure:

1. Use the `tar` command to archive the `jp1pc` directories in the environment directory specified on the local disk.
2. Mount the shared disk.
3. If the specified environment directory does not exist on the shared disk, create an environment directory.
4. Expand the `tar` file in the environment directory on the shared disk.
5. Unmount the shared disk.
6. Delete the `jp1pc` directory and associated files in the environment directory specified on the local disk.

## (o) Importing the file containing the logical host environment definitions

Standby

Import the export file copied from the executing node into the standby node.

1. Execute the `jpccconf ha import` command.

Import the logical host environment definitions into the standby node.

For example, execute the following command if the export file name is `lhostexp.conf`.

```
jpccconf ha import -f lhostexp.conf
```

When the `jpccconf ha import` command is executed, the environment settings for the standby node are changed to the same environment as for the executing node. Therefore, settings are made to use PFM - Manager on a logical host.

If the health check function is enabled for the PFM - Manager in the logical host environment you are importing, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be imported.

In this example, the `jpccconf ha import` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha import` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

2. Check the settings for the logical host environment.

Execute the `jpccconf ha list` command in the same manner as for the executing node to check the settings of the logical host.



Execute the command as follows:

```
jpccconf ha list -key all
```

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (4) Cluster software setting procedure

Cluster software settings are required for both the executing node and the standby node.

### (a) Registering PFM - Manager in the cluster software Executing Standby

To use PFM - Manager on a logical host, register it in the cluster software, and set the cluster software to control the starting and stopping of PFM - Manager.

For details on how to register PFM - Agents or PFM - RM in the cluster software, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

Generally, the following four command items are required when registering an application in the UNIX cluster software: *Start*, *Stop*, *Monitor operations*, and *Forced stop*.

The following table lists and describes the settings in PFM - Manager.

Table 10–8: Control commands for PFM - Manager registered in the cluster software

Command	Description
Start	Execute the following commands in order, and then start PFM - Manager: <code>/opt/jplpc/tools/jpcspm start -key Manager -lhost <i>logical-host-name</i></code> <code>/opt/jplpc/tools/jpcspm start -key AH -lhost <i>logical-host-name</i></code> Perform this action after a condition has been reached in which the shared disk and logical IP address can be used.
Stop	Execute the following commands in order, and then stop PFM - Manager: <code>/opt/jplpc/tools/jpcspm stop -key AH -lhost <i>logical-host-name</i></code> <code>/opt/jplpc/tools/jpcspm stop -key Manager -lhost <i>logical-host-name</i></code> Perform this action before a condition is reached in which the shared disk and logical IP address cannot be used. When a service is stopped due to a problem, the return value for the <code>jpcspm stop</code> command is 3. If this is the case, it can be considered a normal termination since the services have been stopped. For the cluster software that determines execution results by return values, the recovery value can be set to 0.
Monitor operations	Use the <code>ps</code> command to check if the following process is running. <code>ps -ef   grep "<i>process-name logical-host-name</i>"   grep -v "grep process monitored"</code> For details on process names, see <a href="#">10.6.1(3) Service names</a> . Hitachi recommends that you prepare a command for suppressing operation monitoring (for example, a command to stop monitoring when there is a file that is under maintenance) in anticipation of a temporary stop in Performance Management due to maintenance during the operation.
Forced stop	Execute the following command when a forced stop is required: <code>/opt/jplpc/tools/jpcspm stop -key all -lhost <i>logical-host-name</i> -kill immediate</code> Only <code>all</code> can be set to the service key for the first argument.



Command	Description
Forced stop	<p>Note:</p> <p>If this command is executed, SIGKILL is sent to perform a forced stop of all Performance Management processes in the specified logical host environment. At this time, the forced stop is performed on Performance Management not for each service, but for each logical host.</p> <p>Set this item to perform a forced stop only when the system cannot be stopped by executing a normal stop command.</p>

Notes:

- Do not make automatic startup settings for OS startups, since the starting and stopping of the Performance Management registered in the cluster are controlled by the cluster.
- When running Performance Management in a Japanese or Chinese language environment, configure the cluster software to run a script that sets the LANG environment variable before executing any Performance Management commands. In an environment where the LC\_ALL environment variable is set to a different value from the LANG environment variable, either unset the LC\_ALL environment variable or change its value to match the LANG environment variable. You can unset LC\_ALL by adding the following setting:  

```
unset LC_ALL
```
- If the cluster software determines execution results on the basis of the return values from commands, configure the cluster software to convert the return values from Performance Management commands to what the cluster software expects. For details about the return values from Performance Management commands, see the reference documentation for each command.
- Before using the ps command for monitoring operations, execute the ps command to confirm that a character string that is a combination of the logical host name and the instance name is correctly displayed. If part of the character string is not displayed, shorten the instance name.  

When you use the ps command to identify the process name and logical host name, the command sometimes fails to acquire the information, in which case the information might appear in square brackets. Read the manual page for the ps command in your operating system and execute the command again.
- When PFM - Manager links to integrated management products (JP1/IM), specify their dependency relationship so that the PFM - Manager services stop before the JP1/Base services stop.

**(b) Checking starting and stopping from the cluster software**

Executing

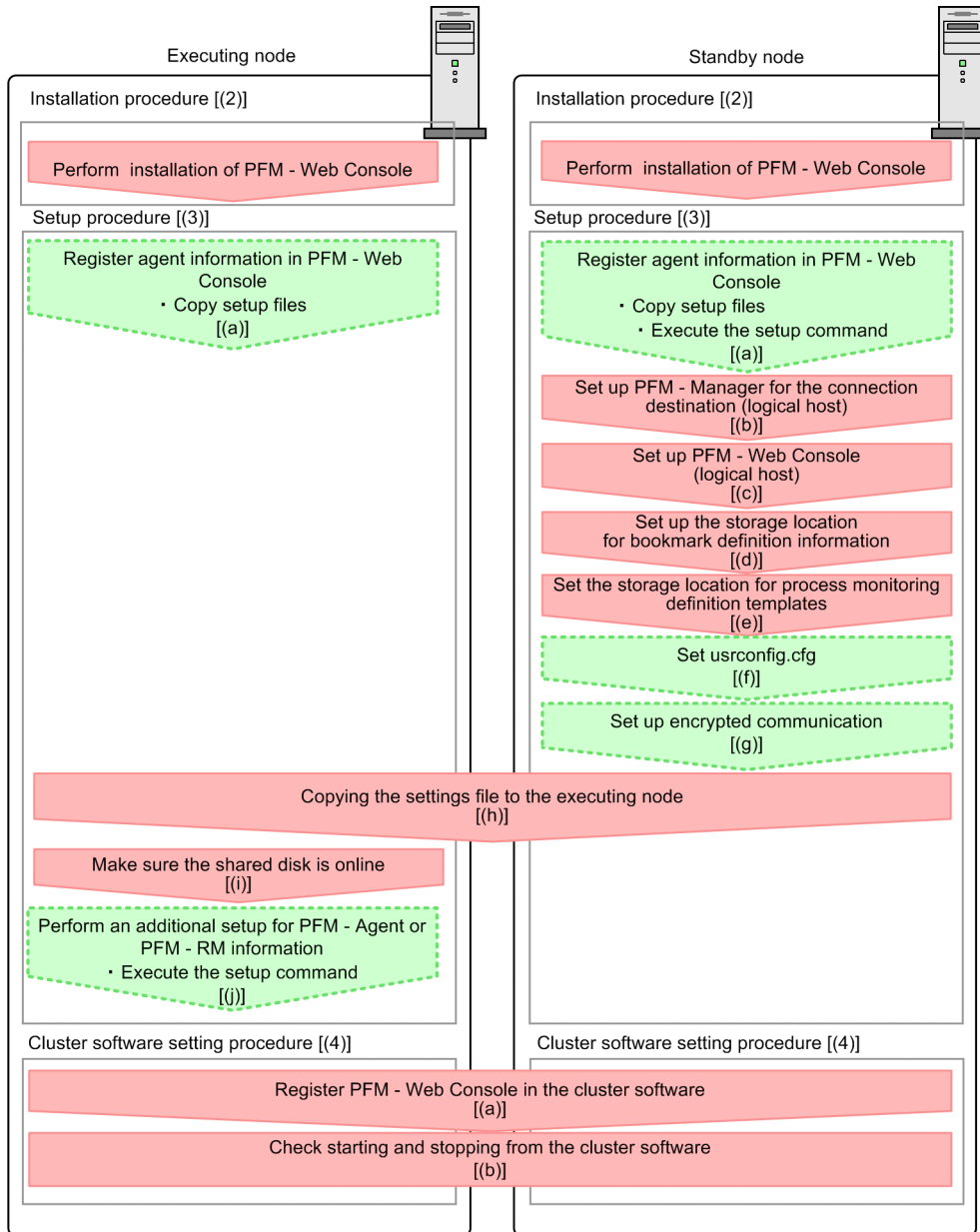
Standby

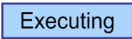

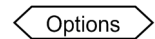
Check whether the cluster software is operating correctly by using it to issue start and stop requests to PFM - Manager or PFM - Web Console on each node.

## 10.4.3 Installing and setting up PFM - Web Console

### (1) Process flow for installation and setup

Figure 10–23: Process flow for installation and setup of PFM - Web Console used on a logical host



In the procedure explanation, the image  indicates the tasks to be performed on the executing node, and the image  indicates the tasks to be performed on the standby node. In addition, the image  indicates the setup items required for specific environments, and optional setup items for when you want to change the default settings.

### (2) Installation procedure

Perform a new installation of PFM - Web Console on the executing node and the standby node. The installation procedure is the same as for a non-cluster system.

For details on the installation procedure, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

Notes:

- Install PFM - Web Console on the local disk, not the shared disk.
- Install each PFM - Web Console for both the executing node and the standby node in a location with the same path.

### (3) Setup procedure

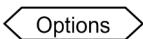
When using PFM - Web Console on a logical host, the environment configurations on the executing node and the standby node have to be the same.

#### (a) Specifying the LANG environment variable Executing Standby

Specify the LANG environment variable on the executing node and the standby node.

For details about how to specify the LANG environment variable, see the section on setting the LANG environment variable in the *JPI/Performance Management Planning and Configuration Guide*.

#### (b) Registering agent information in PFM - Web Console Executing Standby



To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Web Console for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Notes:

- You do not need to register PFM - Agent or PFM - RM when you add the same version of PFM - Agent or PFM - RM with the same product ID to a Performance Management system in which the PFM - Agent or PFM - RM information has been already registered.
- Set up the latest version of PFM - Agent or PFM - RM if you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host.

To perform an additional setup of agent information in PFM - Web Console, see the process flow shown in [Figure 10-23](#).

##### 1. Copy the setup files. Executing Standby

Copy the PFM - Agent or PFM - RM setup file to the following locations on the PFM - Web Console executing node and standby node.

```
/opt/jp1pcwebcon/setup/
```

The files to copy and the procedure for copying the files are the same as when performing an additional setup for PFM - Manager. For details, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

##### 2. Execute the setup command on the standby node. Standby

Execute the `jp1pcwagtsetup` command on the standby node to register the agent information.

Execute the command as follows:

```
jpcwagtsetup
```

For details on the `jpcwagtsetup` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

Supplemental information:

When you register the agent information of PFM - Agent or PFM - RM in PFM - Web Console, you must restart PFM - Web Console. However, because PFM - Web Console restarts on the standby node when a failover occurs, you do not need to restart PFM - Web Console on the standby node after step 2.

### (c) Setting up PFM - Manager for the connection destination Standby

On the standby node, set the IP address or host name for the PFM - Manager that serves as the connection destination for PFM - Web Console in the initialization file (`config.xml`).

Specify the IP address or the host name of the PFM - Manager to connect to in `host` in the `<vserver-connection>` tag under the `<vsa>` tag. If the PFM - Manager to connect to is running on a cluster system, specify the logical IP address or the logical host name.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

### (d) Setting up PFM - Web Console (logical host) Standby

Set the logical IP address or logical host name for PFM - Web Console in the initialization file (`config.xml`) on the standby node.

Specify the logical IP address or the logical host name of the PFM - Web Console host in `ownHost` in the `<vserver-connection>` tag under the `<vsa>` tag.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

### (e) Setting up the storage location for bookmark definition information Standby

Set the storage directory for bookmark definition information in the initialization file (`config.xml`) on the standby node.

Specify the folder for storing bookmark definition information in `bookmarkRepository` in the `<bookmark>` tag under the `<vsa>` tag. Specify a folder on the shared disk to ensure that the information is inherited if a failover occurs.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

### (f) Setting the storage location for process monitoring definition templates Standby

Set the storage folder for process monitoring definition templates in the initialization file (`config.xml`) on the standby node.

Specify the folder for storing bookmark definition information in `processMonitoringTemplatesRepository` in the `<process-monitoring>` tag under the `<vsa>` tag. Specify a folder on the shared disk to ensure that the information is inherited if a failover occurs.

For details about the initialization file (`config.xml`), see the chapter that describes definition files in the manual *JP1/Performance Management Reference*.

### (g) Setting `usrconf.cfg` Standby

If the language setting of the system locale differs from that of the `usrconf.cfg` file, change the setting of the `usrconf.cfg` file on the standby node.

If the system locale has been changed since passwords were set, be sure to check and, if necessary, revise the settings in the `usrconf.cfg` file.

For details about the option definition file (`usrconf.cfg`), see the chapter that describes definition files in the manual *JP1/Performance Management Reference*.

### (h) Setting encrypted communication between a web browser and the monitoring console server Standby

If you will be using encrypted communication between a web browser and the monitoring console server, specify the settings in both PFM - Web Console and the web browser. For details, see the section on changing the settings for encrypted communication between a web browser and the monitoring console server in the *JP1/Performance Management Planning and Configuration Guide*.

### (i) Copying the settings file to the executing node Standby Executing

Copy the initialization file (`config.xml`) edited in (b), (c),(d), and (e) to the executing node.

Copy the file to the following location on the executing node:

```
/opt/jp1pcwebcon/conf/
```

If the settings of the `usrconf.cfg` file on the standby node were changed in (f), you need to copy the file to the executing node. Copy the file to the following location on the executing node:

```
Installation folder\CPSB\CC\web\containers\PFMWebConsole\usrconf
```

### (j) Make sure the shared disk is online Executing

Make sure that the shared disk is online on the execution node. If the shared disk is not online, use the cluster software and the volume manager to bring it online.

### (k) Performing an additional setup for PFM - Agent or PFM - RM information Executing

Options

Use the setup file copied in (a) to perform an additional setup of the agent information for PFM - Agent or PFM - RM on the execution node.

1. Stop the PFM - Web Console service on the executing node.

Use the `jpcwstop` command to stop the services if the PFM - Web Console services are not registered with the cluster software. To perform a forced stop, execute the `jpcwstop` command with the `-immediate` option.

When making changes to the Performance Management configuration such as adding PFM - Agent or PFM - RM after the services are registered with the cluster software, use the cluster software to stop the services. For details on changing the configuration of the cluster system, see *10.5 Changing the cluster system configuration (in UNIX)*.

2. Execute the setup command on the executing node.

Execute the command as follows:

```
jpcwagtsetup
```

For details on the `jpcwagtsetup` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

3. Start the PFM - Web Console service on the executing node.  
Start the PFM - Web Console service that you stopped in step 1.

## (4) Configuring the cluster software

Set up PFM - Web Console in the cluster software. Perform this task on both the executing node and the standby node.

### (a) Registering PFM - Web Console with the cluster software Executing Standby

If you intend to use PFM - Web Console in a logical host environment, register PFM - Web Console with the cluster software. Also, set up the environment so that PFM - Web Console is started and stopped based on instructions from the cluster software.

Generally, the following four command items are required when registering an application in the cluster software: *Start*, *Stop*, *Monitor operations*, and *Forced stop*.

The following table lists and describes the settings for PFM - Web Console.

Table 10–9: Control commands for PFM - Web Console registered in the cluster software

Item	Explanation
Start	Execute the following command to start PFM - Web Console: <code>/opt/jp1pcwebcon/tools/jpcwstart</code>
Stop	Execute the following command to stop PFM - Web Console: <code>/opt/jp1pcwebcon/tools/jpcwstop</code>
Forced stop	Execute the following command to perform a forced stop of PFM - Web Console: <code>/opt/jp1pcwebcon/tools/jpcwstop -immediate</code>
Monitor operations	Use the <code>ps</code> command to check if the following process is running. <code>ps -ef   grep "process-name"   grep -v "grep process-monitored"</code> For details on process names, see <i>10.6.1(3) Service names</i> .

#### Note

- Do not configure PFM - Web Console to start automatically when the OS starts. When PFM - Web Console is registered in the cluster system, it is started and stopped by the cluster software.
- When running PFM - Web Console in a Japanese language environment, configure the cluster software to run a script that sets the `LANG` environment variable before it executes the command that starts PFM - Web Console.
- If the cluster software uses command return values to determine execution results, specify settings so that the command return values from PFM - Web Console are converted to the values that can be correctly interpreted by the cluster software. For details on the command return values for PFM - Web Console, check the reference documentation for each command.
- If you execute a `jpcwstop` command while PFM - Web Console is being used, it might delay the stop processing.

To successfully register the `jpcwstop` command in the cluster software, create a script to wait for several minutes if a value of 4 is returned by the command, and then to execute the `jpcwstop` command again to register the command.

- When you use the `ps` command to identify the process name and logical host name, the command sometimes fails to acquire the information, in which case the information might appear in square brackets. Read the manual page for the `ps` command in your operating system and execute the command again.

## (b) Checking starting and stopping from the cluster software

Executing

Standby

Check whether the cluster software is operating correctly by using it to issue start and stop requests to PFM - Manager on each node.

### 10.4.4 Installing an upgrade for PFM - Agent or PFM - RM

To install an upgrade for PFM - Agent or PFM - RM in a physical host environment where PFM - Agent, PFM - RM, or PFM - Manager is running in a logical host environment:

1. Use the cluster software to stop all PFM services on each logical host.
2. Use the `jpcspm stop -key all` command to stop all PFM services on both the executing and standby physical hosts.
3. Place the shared disk online from the executing node.
4. Install PFM - Agent or PFM - RM on each applicable executing host by overwriting the previous installation.
5. Install PFM - Agent or PFM - RM on each applicable standby host by overwriting the previous installation.
6. Set up Performance Management so that it can run.
7. Use the cluster software to start all PFM services on each logical host.
8. Use the cluster software to start all PFM services on both the executing and standby physical hosts.

For details on PFM - Agent-specific or PFM - RM-specific considerations, see the corresponding PFM - Agent or PFM - RM manual and the *Release Notes*.

### 10.4.5 Unsetup and uninstallation of PFM - Manager

#### (1) Before unsetup and uninstallation

Notes regarding the order of unsetup:

PFM - Manager is required to execute PFM - Agent or PFM - RM. Therefore, when performing unsetup on PFM - Manager, it is necessary to consider its relationship with PFM - Agent or PFM - RM in the system and determine the work order for unsetup. The work order when unsetup is required is the same as the order for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

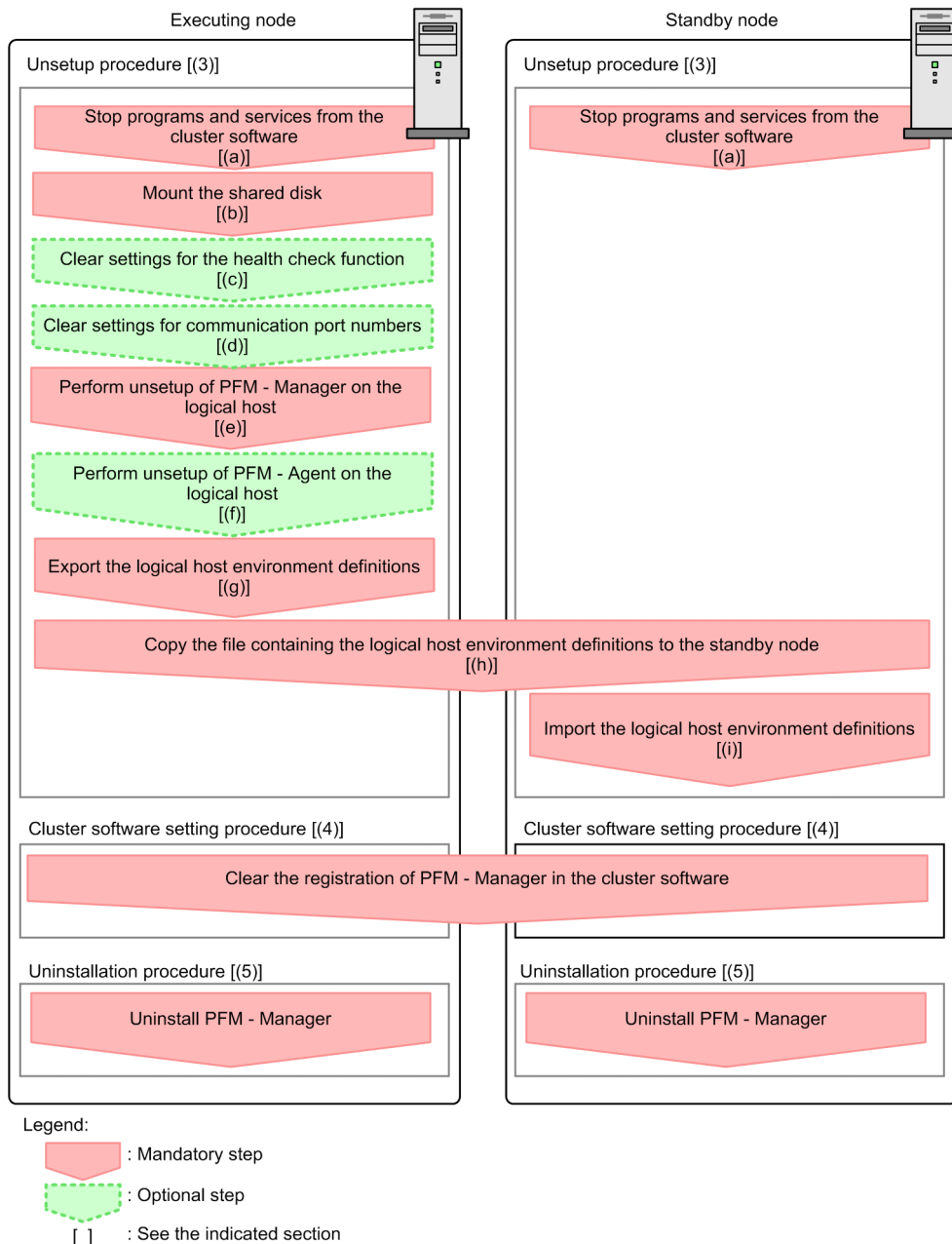


Notes on stopping of services:

Stop all Performance Management programs and services running on the executing nodes and standby nodes on which unsetup is to be performed. Also, stop all PFM - Agent and PFM - RM services across the Performance Management system connected to the instance of PFM - Manager that will be unsetup. For details on how to stop services, see *1. Starting and Stopping Performance Management*.

## (2) Process flow for unsetup and uninstallation

Figure 10–24: Process flow for unsetup and uninstallation of PFM - Manager used on a logical host (in UNIX)



In the procedure explanation, the image indicates the items to be performed on the executing node, and the image indicates the items to be performed on the standby node. In addition, the image indicates the setup items required depending on the environment, and the optional setup items for when changing the default settings.



### (3) Unsetup procedure

First, perform unsetup on the executing node. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the unsetup content from the executing node to the standby node.

#### (a) Stopping from the cluster software Executing Standby

Use operations from the cluster software to stop all Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

#### (b) Making sure the shared disk is mounted Executing

Make sure that the shared disk is mounted. If the shared disk is not mounted, execute the `mount` command to mount it on the file system.

Note:

Even if the shared disk is unmounted, if there is a `jp1pc` directory and associated files in the environment directory of the logical host that is to be unsetup, setup is performed without mounting the shared disk. If that is the case, use the following procedure:

1. Use the `tar` command to archive the `jp1pc` directories in the environment directory of the logical host that is to be unsetup on the local disk.
2. Mount the shared disk.
3. If there is no environment directory of the logical host that is to be unsetup on the shared disk, create an environment directory.
4. Expand the `tar` file in the environment directory of the logical host that is to be unsetup on the shared disk.
5. Unmount the shared disk.
6. Delete the `jp1pc` directory and its associated files in the environment directory of the logical host that is to be unsetup on the local disk.

#### (c) Clearing settings for the health check function Executing Options

Execute the following command on the PFM - Manager host on the executing node to clear the settings for the health check function.

```
jpccconf hc disable
```

For details on the `jpccconf hc disable` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

#### (d) Clearing settings for communication port numbers Executing Options

This procedure is required only when port numbers have been set using the `jpccconf port define` command during the setup in an environment with a firewall.

1. Clear the settings for communication port numbers.

Execute the `jpccconf port define` command to clear the settings for communication port numbers.

For example, execute the following command to clear all the settings for port numbers for services that exist on the host with the logical host name `jp1-hal`.

```
jpccconf port define -key all -lhost jp1-ha1
```

In this example, the `jpccconf port define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode.

The `jpccconf port define` command is used to set the port numbers that are used for communications by PFM - Manager on the logical host or by other Performance Management programs. When entering a port number, a value of 0 will clear the setting. In addition, when this command is executed, the port numbers and service names (service names starting with `jp1pc` by default) for Performance Management defined in the services file are deleted.

For details on the `jpccconf port define` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (e) Performing unsetup of a logical host for PFM - Manager Executing

### 1. Check the logical host settings.

Check the current settings before performing unsetup on the logical host environment. Check the logical host name and shared disk path.

Execute the command as follows:

```
jpccconf ha list -key all
```

An example of executing this command is as follows:

```
# jpccconf ha list -key all

Logical Host Name  Key      Environment Directory      [Instance Name]
-----
jp1-ha1           mgr      "/usr/jp1/jp1pc"

KAVE05136-I The logical host startup information listing ended normally.
```

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

### 2. Delete the logical host environment for PFM - Manager.

When the `jpccconf ha unsetup` command is executed, the settings for starting PFM - Manager on the logical host are deleted. In addition, the files for the logical host on shared disks are also deleted. Execute the command as follows:

```
jpccconf ha unsetup -key Manager -lhost jp1-ha1
```

For details on the `jpccconf ha unsetup` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

Note:

If the shared disk is offline, only the logical host settings will be deleted. The directories and files on the shared disk will not be deleted.

### 3. Check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all
```

Make sure that PFM - Manager has been deleted from the logical host environment.

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (f) Performing unsetup for a logical host of PFM - Agent or PFM - RM Executing

Options

This procedure is required only when there is PFM - Agent or PFM - RM on the same logical host from which unsetup will also be performed for PFM - Manager.

Perform unsetup of PFM - Agent or PFM - RM. For details on the unsetup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

## (g) Exporting the logical host environment definitions Executing

When a logical host environment to perform unsetup of PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file.

Note:

To perform unsetup of a different instance of Performance Management from the same logical host, perform the export after all unsetup procedures are completed

1. Export the logical host environment definitions.

For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file. The export file allows an arbitrary file name.

```
jpccconf ha export -f lhostexp.conf
```

In this example, the `jpccconf ha export` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha export` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## (h) Copying the file containing the logical host environment definitions to the standby node Executing   Standby

Copy the file that has been exported in step (f) from the executing node to the standby node, so that it will be applied on the standby node.

Next, unmount the file system to complete the work. If this shared disk will continue to be used, it is not necessary to unmount the file system.

## (i) Importing the file containing the logical host environment definitions Standby

Import the export file copied from the executing node to the standby node, so that it will be applied to the standby node

Use the `jpccconf ha import` command to apply the Performance Management settings for the logical host created on the executing node to the standby node. If multiple instances of Performance Management have been set up on a single logical host, import all of the instances as one group.

1. Import the logical host environment definitions.

Use the `jpccconf ha import` command to import the exported file of the logical host environment definitions copied from the executing node to the standby node.

For example, execute the following command if the export file name is `lhostexp.conf`.

```
jpccconf ha import -f lhostexp.conf
```

When the command is executed, the environment settings for the standby node are changed to the same environment settings specified for the executing node that has been exported. Therefore, the settings for running PFM - Manager on a logical host are deleted. If you perform unsetup of Performance Management on another logical host, the relevant settings are also deleted.

In this example, the `jpccconf ha import` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf ha import` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

## 2. Check the settings for the logical host environment.

Execute the `jpccconf ha list` command in the same manner as for the executing node, to check the settings of the logical host.

Execute the command as follows:

```
jpccconf ha list -key all
```

For details on the `jpccconf ha list` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

## (4) Clearing the registration of PFM - Manager in the cluster software

Executing

Standby

Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

## (5) Uninstalling PFM - Manager

Executing

Standby

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

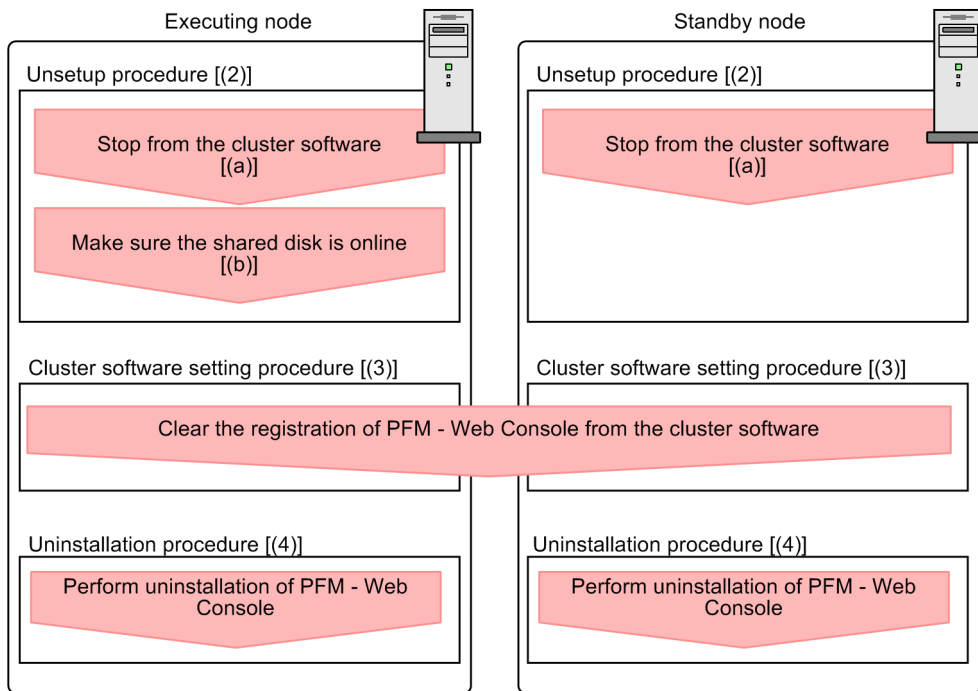
Notes:

- When performing uninstallation of PFM - Manager, stop all Performance Management programs and services on the node where uninstallation is to be performed.
- If uninstallation is performed on Performance Management without deleting the logical host environment, the environment directory might remain. When this happens, delete the environment directory.


## 10.4.6 Unsetup and uninstallation of PFM - Web Console

### (1) Process flow for unsetup and uninstallation

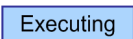
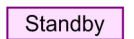
Figure 10–25: Process flow for unsetup and uninstallation of PFM - Web Console used on a logical host (in UNIX)



Legend:

 : Required item

[ ] : See the indicated step.

The image  indicates the steps to be performed on the executing node, and the image  indicates the items to be performed on the standby node.

### (2) Unsetup procedure

#### (a) Stopping from the cluster software

Use operations from the cluster software to stop all Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

#### (b) Making sure the shared disk is online

Make sure that the shared disk is online. If the shared disk is not online, use the cluster software and the volume manager to bring it online.

### (3) Unregister PFM - Web Console with the cluster software Executing

Standby

Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

### (4) Uninstalling PFM - Web Console Executing Standby

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure for PFM - Web Console is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

Note:

If the storage directory for the bookmark definition information has been changed from the default setting, it will not be deleted when you uninstall PFM - Web Console. You need to delete it manually after performing the uninstallation.

## 10.5 Changing the cluster system configuration (in UNIX)

---

After a system is configured and the operation started, as the business expands and processed data volume increases, the system's cluster configuration might need to be changed with the addition of servers or introduction of new applications.

For this reason, the following the Performance Management configuration changes need to be studied in response to changes in the cluster configuration of the monitoring target system:

- Addition of PFM - Agent or PFM - RM due to the addition of a monitored system
- Removal of PFM - Agent or PFM - RM due to the removal of a monitored system
- Changing the logical host name of a machine after operation begins
- Changing the logical host environment after operation begins

This section describes the procedures for making changes to the Performance Management configuration when using a cluster system on a logical host.

### 10.5.1 Adding PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be added in order to monitor the performance of servers or applications that are newly added to a system.

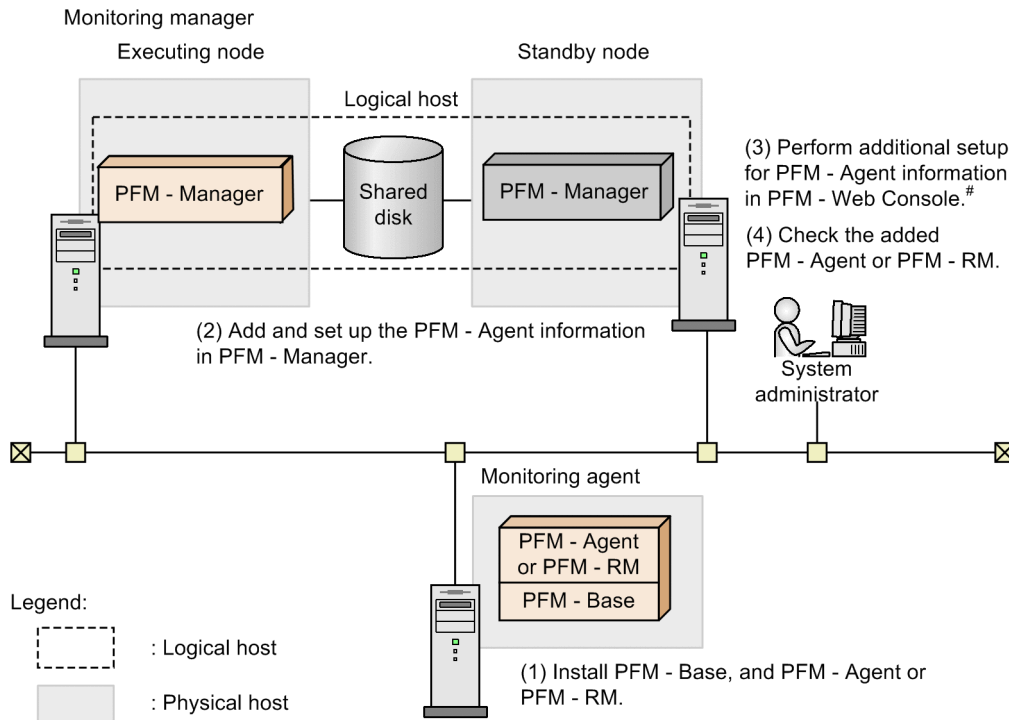
When you add PFM - Agent or PFM - RM with a new product ID that has not previously been used in the Performance Management system, you need to set up the agent information in PFM - Manager and PFM - Web Console.

For details on product IDs, see the appropriate PFM - Agent or PFM - RM manual.

Notes:

- Stop PFM - Manager and all Performance Management programs and services on that node before adding PFM - Agent or PFM - RM. For details on how to stop services, see [1. Starting and Stopping Performance Management](#).
- It is also necessary to stop PFM - Manager used on a logical host while work is being performed. An error might occur if you execute the `jpcconf agent setup` command or the `jpcwagtsetup` command to add PFM - Agent or PFM - RM before the Performance Management programs and services are completely stopped. In such cases, first make sure that all services have completely stopped, and then re-execute the `jpcconf agent setup` command or the `jpcwagtsetup` command.

Figure 10–26: Process flow for adding PFM - Agent or PFM - RM to a Performance Management system in a logical host environment



# Windows is the only OS that supports PFM - Web Console.

## (1) Installing PFM - Base and either PFM - Agent or PFM - RM

For details on how to install, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

## (2) Adding and setting up the PFM - Agent or PFM - RM information in PFM - Manager

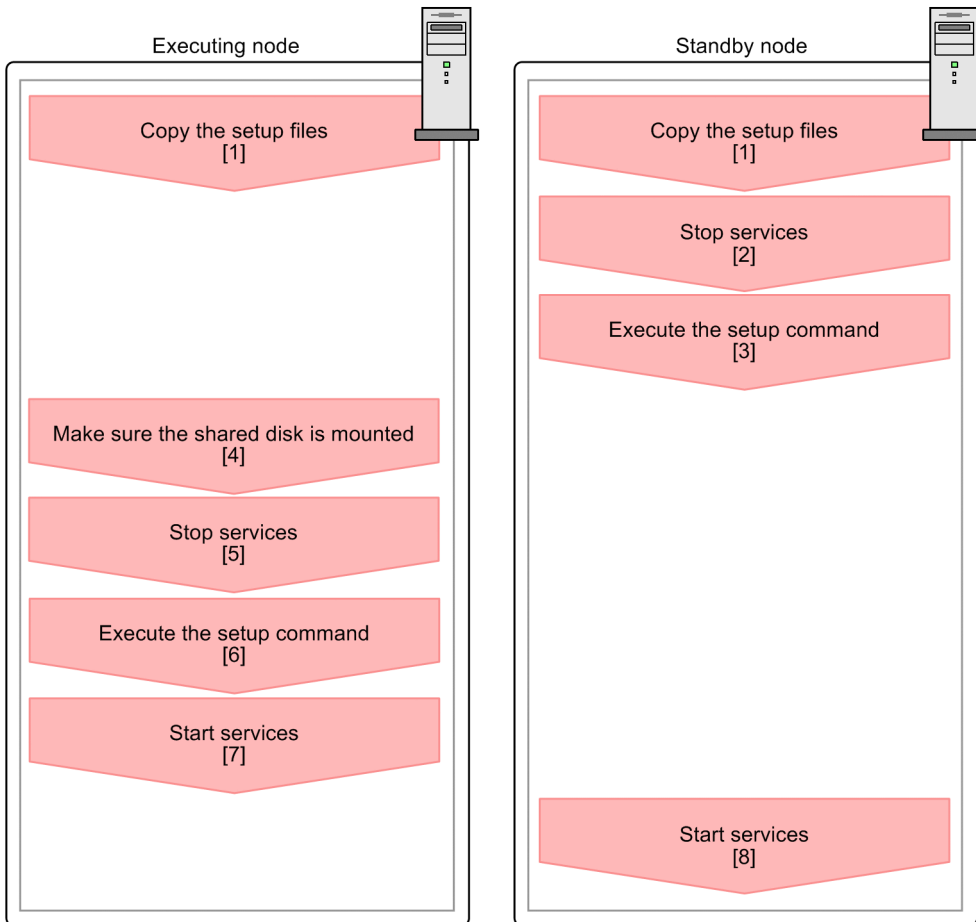
### (a) Process flow of additional PFM - Agent or PFM - RM information setup in PFM - Manager

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.


Perform the addition and setup of the agent information on the standby node first. When the addition and setup are completed on the standby node, next perform setup on the executing node.



Figure 10–27: Additional PFM - Agent or PFM - RM information setup in PFM - Manager



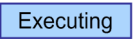

Legend:

-  : Required setup item
- [ ] : See the indicated step.

Notes:

- If you add another PFM - Agent or PFM - RM to the same host as PFM - Manager, an additional setup is not required.
- If you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host, first set up the older version of PFM - Agent or PFM - RM, and then set up the newer version of PFM - Agent or PFM - RM.

## (b) Additional PFM - Agent or PFM - RM information setup procedure in PFM - Manager

The image  indicates a procedure used on the executing node, and the image  indicates a procedure used on the standby node.

### 1. Copying the setup files

Copy the PFM - Agent or PFM - RM setup files to the executing and standby nodes of PFM - Manager.

For details, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

### 2. Stopping services on the standby node

Stop all physical host services on the standby node.

3. Executing the setup command Standby

Execute the `jpccconf agent setup` command on the standby node, and then perform additional setup for the new agent.

Execute the following command:

```
jpccconf agent setup -key xxxx
```

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

For example, execute the following command to set up PFM - Agent for Oracle:

```
jpccconf agent setup -key Oracle
```

In this example, the `jpccconf agent setup` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf agent setup` command, see the chapter that describe commands in the manual *JP1/Performance Management Reference*.

4. Making sure the shared disk is mounted Executing

Make sure that the shared disk has been mounted on the executing node. Write the agent information to the shared disk with the additional setup procedure. Use the cluster software or the volume manager to check that the shared disk has been mounted.

5. Stopping services Executing

Stop all Performance Management programs and services in the physical and logical host environments on the standby node. Use the cluster software to stop the programs and services.

6. Executing setup commands Executing

Execute the `jpccconf agent setup` command on the executing node in the same manner as for the standby mode in order to add and set up the new agent.

```
jpccconf agent setup -key xxxx
```

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

For example, execute the following command to set up PFM - Agent for Oracle:

```
jpccconf agent setup -key Oracle
```

In this example, the `jpccconf agent setup` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf agent setup` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

7. Starting services Executing

Start the Performance Management programs and services that were stopped on the executing node.

8. Starting services on the standby node Standby

On the standby node, start the Performance Management programs and services that you stopped earlier.

### (3) Adding and setting up PFM - Agent or PFM - RM in PFM - Web Console

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

For details on the additional setup procedure, see [10.4.3\(3\)\(b\) Registering agent information in PFM - Web Console](#).

### (4) Checking PFM - Agent or PFM - RM added and set up

1. Start the services in the nodes of PFM - Agent or PFM - RM.

Start the Performance Management programs and services in the nodes of the newly added PFM - Agent or PFM - RM.

2. Check if PFM - Agent or PFM - RM has been added correctly.

Execute the `jpctool service list` command to check if PFM - Manager has been connected correctly.

Execute the command as follows:

```
jpctool service list -id "*" 
```

For details on the `jpctool service list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

## 10.5.2 Deleting PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be deleted when a monitored system is removed from the entire system due to changes in the system configuration.

Note:

Stop all programs and services associated with the instance of PFM - Agent or PFM - RM you are deleting.

### (1) Deleting PFM - Agent or PFM - RM from PFM - Manager

1. Unbind the alarm tables.

If any alarm tables are bound to the instance of PFM - Agent or PFM - RM you are deleting, unbind the alarm tables in PFM - Web Console or by using the `jpctool alarm unbind` command. For details on how to unbind alarm tables in PFM - Web Console, see [6.6.1\(2\)\(b\) Unbinding an alarm table bound to a monitoring agent](#). For details on how to unbind alarm tables using the `jpctool alarm unbind` command, see [6.8.2 Unbinding an alarm table bound to a monitoring agent](#).

2. Delete the agent information.

Delete the agent information managed by PFM - Manager.

Execute the command as follows:

```
jpctool service delete -id xxxx -host host-name -lhost logical-host-name
```

`xxxx` indicates the service ID for each PFM - Agent or PFM - RM.

For example, execute the following command to delete the agent information for PFM - Agent for Oracle in the logical host environment with the host name `jp1` and the logical host name `jp1-ha1`.

```
jpctool service delete -id "O*" -host jp1 -lhost jp1-ha1
```

For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

### 3. Perform unsetup and uninstall PFM - Agent or PFM - RM.

For details on how to perform unsetup and how to uninstall PFM - Agents or PFM - RM, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

### 4. Apply the agent information to PFM - Manager.

Synchronize the agent information between PFM - Manager and PFM - Web Console so that the deletion takes effect in PFM - Web Console. To synchronize the agent information, use the `jpctool service sync` command.

The time when the agent information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console. For details about the `jpctool service sync` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

Note: When performing unsetup of the PFM - RM remote agent

Because the service information is deleted automatically when you unset up the PFM - RM remote agent (by using the `jpccconf target unsetup` command), you do not need to execute the `jpctool service delete` command.

However, you do need to execute the `jpctool service sync` command to apply the changes to PFM - Web Console after the unsetup process.

The following describes when the service information is deleted.

- If PFM - Manager and the PFM - RM service you are deleting are running  
When you execute the `jpccconf target unsetup` command, PFM - RM issues a request to PFM - Manager to delete the service information. PFM - Manager then deletes the service information.
- If PFM - Manager or the PFM - RM service you are deleting is stopped  
PFM - Manager deletes the service information when the PFM - RM service starts and connects to PFM - Manager after the `jpccconf target unsetup` command is executed.

## (2) Deleting PFM - Agent or PFM - RM from PFM - Web Console

### 1. Close and re-open PFM - Web Console on the executing node.

Apply the changes made by the deleted PFM - Agent or PFM - RM information to PFM - Web Console.

After executing the `jpctool service sync` command, close and re-open PFM - Web Console on the executing node.

### 2. Delete agents from the Agents tree.

Delete agents that are no longer required from the **User Agents** node in the Agents tree, as needed.

For details on how to delete agents from the Agents tree, see [3.2 Creating and editing an Agents tree in a Web browser](#) or [3.3 Using commands to create and edit an Agents tree](#).

### 3. Delete the alarm definition information and report definition information.

Delete the unnecessary alarm definition information and report definition information as necessary.

For details on deleting alarm definition information, see [6.4.9\(2\) Deleting an alarm](#) or [6.7.6 Deleting an alarm](#). For details on deleting report definition information, see [5.3.12\(2\) Deleting a report](#) or [5.5.2 Deleting an unnecessary report](#).

## 10.5.3 Changing logical host names after starting operation

This subsection describes the procedures (performed on the Performance Management system) necessary for changing the logical host names of the PFM - Manager host, PFM - Agent host, or PFM - RM host after the Performance Management system is configured.

To change a logical host name, you must first use the `jpccconf host hostname` command to change the monitoring host name.

If you execute the `jpccconf host hostname` command, all existing information, including definition and performance information, is inherited. For details on the `jpccconf host hostname` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

### (1) Changing the PFM - Manager logical host name

#### (a) Overview of changing the PFM - Manager logical host name

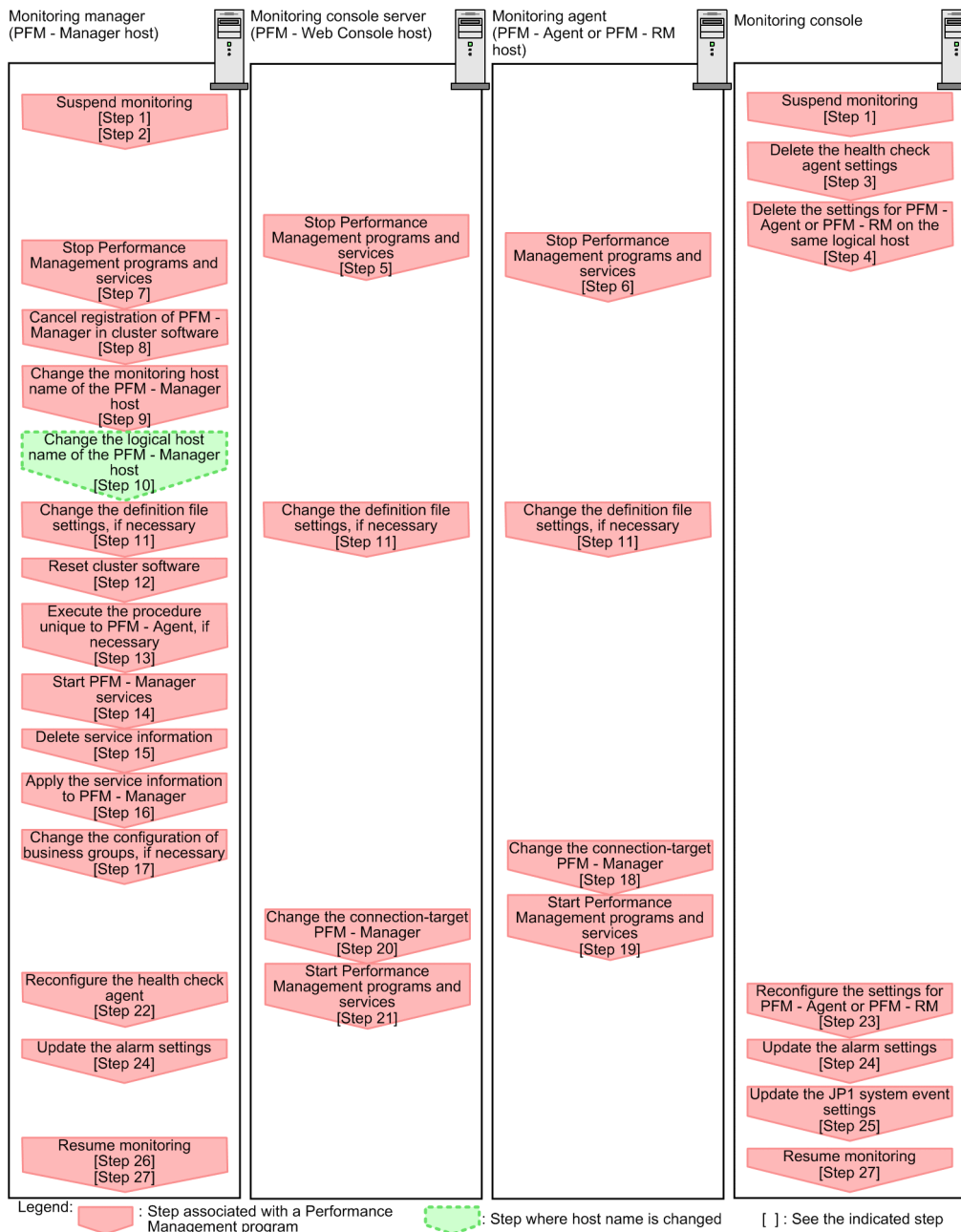
You must work on the following hosts when changing the PFM - Manager logical host name:

- PFM - Manager host
- PFM - Web Console host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Before performing this task in a system that links with JP1/SLM, refer to [13.4.1 Changing host names after linking with JP1/SLM](#).

Figure 10–28: Process flow for changing the PFM - Manager host name



## (b) Procedure for changing the PFM - Manager logical host name

Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Suspend monitoring for the PFM - Manager host whose host name is to be changed.
 

If you do not want health check events to occur while changing the host name, suspend monitoring for the host whose name is to be changed. You can do so by using the `jpctool monitor suspend` command of the PFM - Manager host or from the monitoring console.

For details on suspending monitoring, see [8. Suspending and Resuming Monitoring](#).
2. Suspend monitoring with the new host name specified.
 

If you suspend monitoring in step 1, you also need to suspend monitoring with the new host name specified.

In this case, use the `-force` option of the `jpctool monitor suspend` command of the PFM - Manager host.

3. Clear the setting for the health check agent.

If you are using the health check function, you can delete the agent definitions for the health check agent using your PFM - Web Console (by deleting the definitions from the management folder in the Agents tree and removing the association between the alarm tables and the definitions). For details on how to change the agent definition, see [6. Monitoring Operations with Alarms](#).

4. Delete the settings for PFM - Agent or PFM - RM.

You can use the PFM - Web Console to delete the agent definitions for the logical PFM - Agent host or logical PFM - RM host installed on the same host as the PFM - Manager whose logical host name is to be changed. This involves deleting the definitions from the management folder in the Agents tree. For details about how to change agent definitions, see [3. Monitoring Agents](#).

5. Stop services on the PFM - Web Console host.

On the PFM - Web Console host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcwstop` command.

6. Stop services on the PFM - Agent or PFM - RM host.

On the PFM - Agent or PFM - RM host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcspm stop` command.

7. Stop services on the PFM - Manager host.

Use operations from the cluster software to stop Performance Management programs and services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

8. Cancel the registration of PFM - Manager from the cluster software.

Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

9. Change the monitoring host name of PFM - Manager host.

Execute the `jpcconf host hostname` command to change the monitoring host name.

In the following example, the logical host name is changed from `lhostA` to `lhostB`.

```
jpcconf host hostname -lhost lhostA -newhost lhostB -d /tmp/backup -  
dbconvert convert
```

For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

 **Note**

As a general rule, the directory specified in the `-d` option of the `jpcconf host hostname` command requires disk space equivalent to the total size of the PFM - Agent and PFM - RM Store databases and the import directory on the specified host. If you have made changes to the storage directory or import directory of the Store database, calculate the disk space requirements with reference to the size of the database in the new location.

For example, if PFM - Agent for HiRDB and PFM - Agent for Oracle are located in the environment directory, the directory must have free disk space equivalent to the size of the Store databases in the environment directory plus the size of the database in the import directory. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

10. Change the PFM - Manager logical host name.



Change the PFM - Manager logical host name.

11. Edit the settings in the `hosts` and `jpchosts` files so that the new host name can be resolved to an IP address in the Performance Management system, if necessary.

12. Reconfigure the cluster software.

For details, see [10.4.2\(4\) Cluster software setting procedure](#).

13. Perform any PFM - Agent-specific steps, if necessary.

If PFM - Agent has been installed on the PFM - Manager host, the PFM - Agent-specific procedure might be necessary. The following table describes whether the PFM - Agent-specific procedure is necessary.

**Table 10–10: PFM - Agent-specific procedure is necessary or not**

Configuration		Necessity and reference
The version of PFM - Agent installed on the PFM - Manager host is 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The version of PFM - Agent installed on the PFM - Manager host is earlier than 09-00.	The following PFM - Agents: <ul style="list-style-type: none"> <li>• PFM - Agent for Cosminexus</li> <li>• PFM - Agent for Domino</li> <li>• PFM - Agent for Enterprise Applications</li> </ul>	The PFM - Agent-specific procedure is necessary. For details about the procedure, see <a href="#">10.5.3(4) Optional PFM - Agent-specific steps for host name changes</a> .
	Other than the above	The PFM - Agent-specific procedure is not necessary.

If a PFM - Agent-specific step is to be performed, complete the reference step shown in this table before proceeding to the next step.

14. Start services on the PFM - Manager host.

Use the cluster software to start all PFM - Manager services.

15. Delete service information on the PFM - Manager host.

Even though the PFM - Manager host name is changed, the service information of the Performance Management programs with the old host name remains the same. Therefore, you need to delete unnecessary information.

The types of service information that you need to delete and the method of checking the service information are described as follows:

*Service information on the host with the old host name*

All the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id "*" -host old-host-name -lhost new-host-name
```

*Service information whose service ID contains the old host name*

Items whose Service ID column contains the old host name of the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id "*" -lhost new-host-name
```

Service information can be deleted by using the `jpctool service delete` command.

Delete service information on the host with the old host name by using the following command:

```
jpctool service delete -id "*" -host old-host-name -lhost new-host-name
```



Additionally, delete service information whose service ID contains the old host name by using the following command:

```
jpctool service delete -id "???old-host-name" -host new-host-name -lhost
new-host-name
```

If the message KAVE05233-W is issued during command execution because of a service information deletion error, re-execute the command as follows:

```
jpctool service delete -id "*" -host old-host-name -lhost new-host-name -
force
jpctool service delete -id "???old-host-name" -host new-host-name -lhost
new-host-name -force
```

#### Note

Even though you execute the `jpctool service list` command, old service information that contains the old host name might not be displayed. Because such service information also needs to be deleted from the database, you must execute the `jpctool service delete` command shown above.

For details on the commands, see the chapter that describes the commands in the manual *JPI/Performance Management Reference*.

#### 16. Apply the service information to PFM - Manager.

Synchronize the service information between PFM - Manager and PFM - Web Console so that the deletion takes effect in PFM - Web Console. To synchronize the service information, use the `jpctool service sync` command.

The time when the service information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console. For details about the `jpctool service sync` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

#### 17. Change the business group configuration if needed.

If the PFM - Manager host whose logical host name you changed is assigned to a business group, you need to change the configuration of the business group. For details on how to do so, see [2. Managing User Accounts and Business Groups](#).

#### 18. Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host.

Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the logical host name. Use the `jpccconf mgrhost define` command to change the settings for PFM - Manager for the connection destination.

(Specify the same settings on the physical host of both the executing and standby nodes of the PFM - Manager environment.)

For example, if the host name of PFM - Manager for the connection destination will be changed to *lhostB*, specify and execute the command as follows:

```
jpccconf mgrhost define -host lhostB
```

In this example, the `jpccconf mgrhost define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode. For details on the `jpccconf mgrhost define` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

#### 19. Start services on the PFM - Agent or PFM - RM host.

Start the Performance Management programs and services on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the logical host name. To start services, use `jpccspm start` command.

20. Change PFM - Manager for the connection destination on the PFM - Web Console host.

Change the settings for PFM - Manager for the connection destination on the PFM - Web Console host connected to PFM - Manager for which you have changed the logical host name. Change the information in the Windows initialization file (`config.xml`) to change the settings for PFM - Manager for the connection destination. For details, see the chapter describing installation and setup (in UNIX) in the *JP1/Performance Management Planning and Configuration Guide*.

21. Start services on the PFM - Web Console host.

Start the Performance Management programs and services on the PFM - Web Console host connected to PFM - Manager for which you have changed the logical host name. To start services, use the `jpcteststart` command.

22. Reconfigure the definition for the health check agent.

If you have been using the health check function, reconfigure the definition (that has been cleared at step 3) of the health check agent after changing the host name.

23. Reconfigure the definition of PFM - Agent or PFM - RM.

Reconfigure the definitions (that were deleted in step 4) of the logical PFM - Agent or logical PFM - RM installed on the same host as PFM - Manager for which the logical host name was changed.

24. Update the alarm settings.

In the following cases, you must update the alarm settings by using the `jpctesttool alarm` command of the PFM - Manager host or the monitoring console.

- The action handler of the PFM - Manager host is specified for the action handler that executes actions.  
Edit the alarm to set `PH1<new-pfm-manager-host-name>` for the action handler that executes actions.
- JP1 events are issued by actions.  
Set the JP1 event settings in the action again.

For details on how to edit alarms, see [6. Monitoring Operations with Alarms](#).

25. Update the JP1 system event settings.

If either of the following conditions is met, use the PFM - Web Console to update the JP1 system event settings:

- The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
- The old host name is specified as the name of the monitoring console host for JP1 system events.

For details on the JP1 system events, see [12.2 JP1 events issued from Performance Management to JP1/IM](#).

26. Resume monitoring with the old host name specified.

If you suspend monitoring in step 1, you need to resume monitoring with the old host name specified to delete the settings information of monitoring suspension for the old host name.

In this case, use the `-force` option of the `jpctesttool monitor resume` command of the PFM - Manager host.

27. Resume monitoring for the PFM - Manager host whose host name was changed.

If you suspend monitoring in step 2, use the `jpctesttool monitor resume` command of the PFM - Manager host or use the monitoring console to resume monitoring for the PFM - Manager host.

28. Check whether the JP1 system event settings are properly updated.

Check the following items after changing the logical host name:

- Collection of performance data  
Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).

- Execution of the `jpccrpt` command  
Make sure that there is no problem in outputting the collected performance data.
- The report definitions and alarm definitions  
Make sure that there are no problems with the report definitions and alarm definitions created from the Web browser.
- The actions  
Make sure that there is no problem in executing the created actions.

## **(2) Changing the PFM - Agent or PFM - RM logical host name**

### **(a) Overview of changing the PFM - Agent or PFM - RM logical host name**

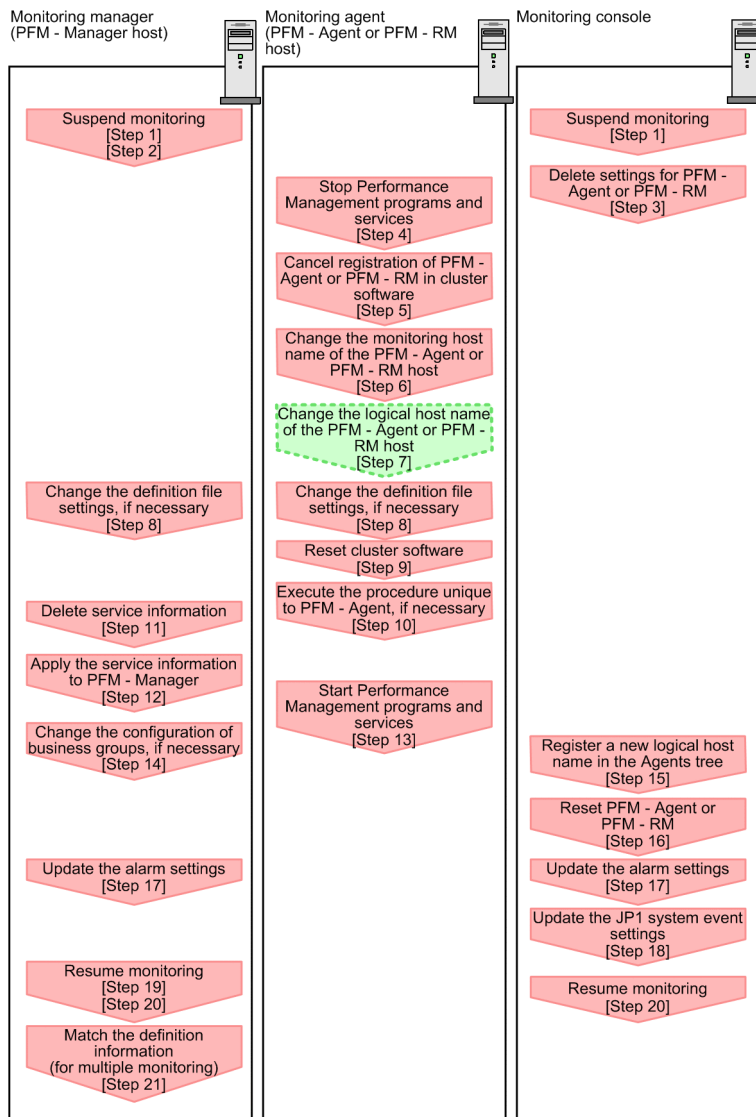
You must work on the following hosts when changing the PFM - Agent or PFM - RM logical host name:

- PFM - Manager host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Before performing this task in a system that links with JP1/SLM, refer to *13.4.1 Changing host names after linking with JP1/SLM*.

Figure 10–29: Changing the logical host name of PFM - Agent or PFM - RM



## (b) Procedure for changing the PFM - Agent or PFM - RM logical host name

Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Suspend monitoring for the PFM - Agent or PFM - RM host whose host name is to be changed.
 

If you do not want health check events to occur while changing the host name, suspend monitoring for the host whose name is to be changed. You can do so by using the `jpctool monitor suspend` command of the PFM - Manager host or from the monitoring console.

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on suspending monitoring, see [8. Suspending and Resuming Monitoring](#).
2. Suspend monitoring with the new host name specified.
 

If you suspend monitoring in step 1, you also need to suspend monitoring with the new host name specified.

In this case, use the `-force` option of the `jpctool monitor suspend` command of the PFM - Manager host.

In a multiple-monitoring configuration, perform this step on the primary manager.

3. Delete the PFM - Agent or PFM - RM information.

Use your PFM - Web Console to delete the agent definitions from the PFM - Agent or PFM - RM host whose logical host name is to be changed (by deleting the definitions from the management folder in the Agents tree and disassociating any alarm tables from them).

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on how to change the agent definition, see [3. Monitoring Agents](#) or [6. Monitoring Operations with Alarms](#).

4. Stop the services on the PFM - Agent or PFM - RM host.

Stop all Performance Management programs and services on the PFM - Agent or PFM - RM host for which you intend to change the logical host name. Use operations from the cluster software to stop Performance Management programs and services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

5. Unregister PFM - Agent or PFM - RM from the cluster software.

Delete the settings related to PFM - Agent or PFM - RM on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

6. Change the monitoring host name for the PFM - Agent or PFM - RM host.

Execute the `jpccconf host hostname` command to change the monitoring host name.

In the following example, the logical host name is changed from `lhostA` to `lhostB`.

```
jpccconf host hostname -lhost lhostA -newhost lhostB -d /tmp/backup -
dbconvert convert
```

Note:

After executing the above command, do not execute any other Performance Management commands until after you change the host name in the next step.

For details on the `jpccconf host hostname` command, see the chapters that describe commands in the manual *JP1/Performance Management Reference*.

 **Note**

As a general rule, the directory specified in the `-d` option of the `jpccconf host hostname` command requires disk space equivalent to the total size of the PFM - Agent and PFM - RM Store databases and the import directory on the specified host. If you have made changes to the storage directory or import directory of the Store database, calculate the disk space requirements with reference to the size of the database in the new location.

For example, if PFM - Agent for HiRDB and PFM - Agent for Oracle are located in the environment directory, the directory must have free disk space equivalent to the size of the Store databases in the environment directory plus the size of the database in the import directory. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

7. Change the PFM - Agent or PFM - RM logical host name.

Change the PFM - Agent or PFM - RM logical host name.

8. Edit the settings in the `hosts` and `jpchosts` files so that the new host name can be resolved to an IP address in the Performance Management system, if necessary.

9. Configure the cluster software.

For details, see [10.4.2\(4\) Cluster software setting procedure](#).

10. Perform any PFM - Agent-specific steps, if necessary.

The following table describes whether the PFM - Agent-specific procedure is necessary.

**Table 10–11: Whether the PFM - Agent-specific procedure is necessary**

Configuration		Necessity and reference
The monitoring host name to be changed is PFM - Agent version 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The monitoring host name to be changed is PFM - Agent for versions earlier than 09-00.	The following PFM - Agents: <ul style="list-style-type: none"> <li>• PFM - Agent for Cosminexus</li> <li>• PFM - Agent for Domino</li> <li>• PFM - Agent for Enterprise Applications</li> </ul>	The PFM - Agent-specific procedure is necessary. For details about the procedure, see <a href="#">10.5.3(4) Optional PFM - Agent-specific steps for host name changes</a> .
	Other than the above	The PFM - Agent-specific procedure is not necessary.

If a PFM - Agent-specific step is to be performed, complete the reference step shown in this table before proceeding to the next step.

11. Delete service information on the PFM - Manager host.

Even though the PFM - Agent or PFM - RM host name is changed, the service information of the Performance Management programs with the old host name remains the same. Therefore, you need to delete unnecessary information from the PFM - Manager host. In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

The types of service information that you need to delete and the method of checking the service information are described as follows:

*Service information on the host with the old host name*

All the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id "*" -host old-host-name
```

*Service information whose service ID contains the old host name*

Items whose Service ID column contains the old host name of the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id "*" -host old-host-name
```

Service information can be deleted by using the `jpctool service delete` command.

Delete service information on the host with the old host name by using the following command:

```
jpctool service delete -id "*" -host old-host-name
```

Additionally, delete service information whose service ID contains the old host name by using the following command:

```
jpctool service delete -id "???old-host-name" -host new-host-name
```

If the message KAVE05233-W is issued during command execution because of a service information deletion error, re-execute the command as follows:

```
jpctool service delete -id "*" -host old-host-name -force
jpctool service delete -id "???old-host-name" -host new-host-name -force
```

#### Note

Even though you execute the `jpctool service list` command, old service information that contains the old host name might not be displayed. Because such service information also needs to be deleted from the database, you must execute the `jpctool service delete` command shown above.

For details on the commands, see the chapter that describes the commands in the manual *JPI/Performance Management Reference*.

#### 12. Apply the service information to PFM - Manager.

Synchronize the service information between PFM - Manager and PFM - Web Console so that the deletion takes effect in PFM - Web Console. To synchronize the service information, use the `jpctool service sync` command.

In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

The time when the service information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console. For details about the `jpctool service sync` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

#### 13. Start services on the PFM - Agent or PFM - RM host.

Start Performance Management programs and services from the cluster software on the PFM - Agent or PFM - RM host for which you have changed the logical host name.

#### 14. Change the business group configuration if needed.

If the PFM - Agent host or PFM - RM host whose logical host name you changed is assigned to a business group, you need to change the configuration of the business group.

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on how to do so, see [2. Managing User Accounts and Business Groups](#).

#### 15. Register the new logical host name in the management folder in the Agents tree as needed.

Register the PFM - Agent or PFM - RM host whose logical host name you changed in the management folder in the Agents tree of PFM - Web Console. For details on how to register a host in the management folder, see [3. Monitoring Agents](#).

#### 16. Reconfigure the definition of step 3 as needed.

Reconfigure the definitions (that were deleted in step 3) of the PFM - Agent or PFM - RM for which the logical host name was changed.

In a multiple-monitoring configuration, perform this step on the primary manager.

#### 17. Update the alarm settings.

In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

In a multiple-monitoring configuration, perform this step on the primary manager.

- When the action handler of the PFM - Agent or PFM - RM host is specified for the action handler that executes actions.

Edit the alarm to set `PH1<new-pfm-agent-or-pfm-rm-host-name>` for the action handler that executes actions.

For details on how to edit alarms, see [6. Monitoring Operations with Alarms](#).

#### 18. Update the JP1 system event settings.

If either of the following conditions is met, use your PFM - Web Console to update the JP1 system event settings:



In a multiple-monitoring configuration, perform this step on the primary manager.

- The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
- The old host name is specified as the name of the monitoring console host for JP1 system events.

For details on the JP1 system events, see *12.2 JP1 events issued from Performance Management to JP1/IM*.

19. Resume monitoring with the old host name specified.

If you suspend monitoring in step 1, you need to resume monitoring with the old host name specified to delete the settings information of monitoring suspension for the old host name.

In this case, use the `-force` option of the `jpctool monitor resume` command of the PFM - Manager host.

In a multiple-monitoring configuration, perform this step on the primary manager.

20. Resume monitoring for the PFM - Agent or PFM - RM host whose host name was changed.

If you suspend monitoring in step 2, use the `jpctool monitor resume` command of the PFM - Manager host or use the monitoring console to resume monitoring for the PFM - Agent or PFM - RM host.

In a multiple-monitoring configuration, perform this step on the primary manager.

21. Match the definitions on the primary manager and the secondary manager (in a multiple-monitoring configuration).

Export the definitions for the multiple-monitoring configuration from the primary manager and import them to the secondary manager so that the primary manager and the secondary manager have the same definitions.

For details about how to match the definition information, see *11.5 Duplicating definition information*.

22. Check whether the JP1 system event settings are properly updated.

Check the following items after changed the settings:

- Collection of the performance data  
Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).
- Execution of the `jpcrept` command  
Make sure that there is no problem in outputting the collected performance data.
- The report definitions and alarm definitions  
Make sure that there are no problem with the report definitions and alarm definitions created by the Web browser.
- The actions  
Make sure that there is no problem in executing the created actions.

### (3) Changing the PFM - Web Console logical host name

Before performing this task in a system that links with JP1/SLM, refer to *13.4.1 Changing host names after linking with JP1/SLM*.

1. Stop services on the PFM - Web Console host.

Use operations from the cluster software to stop Performance Management programs and services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

2. Cancel the registration of PFM - Web Console from the cluster software.

Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.



3. Edit the PFM - Web Console host information in the initialization file (`config.xml`) to refer to the new logical host name.

This step is necessary when the logical host name has been set for the `ownHost` parameter in the `<vsa>` - `<vserver-connection>` tag of the Windows initialization file (`config.xml`).

For details on the procedure, see [10.4.3\(3\)\(d\) Setting up PFM - Web Console \(logical host\)](#) and [10.4.3\(3\)\(i\) Copying the settings file to the executing node](#).

4. If the integrated management product (JP1/IM) is linked for operation monitoring, change the host name specified in each applicable definition file or in the property value for each service.

The location of the host name setting depends on the type of JP1 event that is used.

- If a JP1 user event is used:

Change the host name in the definition files for the tool launcher and for opening monitor windows. For details, see [12.3.2\(4\) Editing and copying the definition files for linkage](#).

- If a JP1 system event is used:

Change the host name in the Monitoring Console Host property value for each service. For details, see [12.3.2\(1\) Configuring so that JP1 events are issued](#).

For details on an integrated management product (JP1/IM), see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

5. Change the PFM - Web Console logical host name.

6. If encrypted communication between a web browser and the monitoring console server is enabled, re-obtain certificates.

You must re-obtain certificates under the new host name.

For details, see the section on changing the settings for encrypted communication between a web browser and the monitoring console server in the *JP1/Performance Management Planning and Configuration Guide*.

7. Reconfigure the cluster software.

For details on the setting procedure, see [10.4.3\(4\) Configuring the cluster software](#).

8. Start services on the PFM - Web Console host.

Use operations from the cluster software to start the PFM - Web Console services.

9. If the integrated management product (JP1/IM) is linked, restart the product (JP1/IM).

## (4) Optional PFM - Agent-specific steps for host name changes

This subsection describes the PFM - Agent-specific steps necessary to perform the following operations for each product:

- Changing the PFM - Manager logical host name
- Changing the PFM - Agent or PFM - RM logical host name

For details on when it is necessary to perform these steps, see [10.5.3\(1\) Changing the PFM - Manager logical host name](#) and [10.5.3\(2\) Changing the PFM - Agent or PFM - RM logical host name](#).

### (a) PFM - Agent for Cosminexus

Edit the definition files in all of the existing instance environments.

- Definition file

`environment-directory/opt/jp1pc/agtc/agent/instance-name/jpcagt.ini`

- What to edit  
Specify a new host name as the value of the `COSMI_HOST` entry in the `[Agent]` section.

## (b) PFM - Agent for Domino

Note:

Perform the following procedure only if you use the health check function provided by PFM - Agent for Domino.

Edit the definition files in all of the existing instance environments.

- Definition file  
`environment-directory/opt/jp1pc/agt1/agent/instance-name/jpcagt.ini`
- What to edit  
Specify a new host name as the value of the following entries in the `[Health Check Options]` section:
  - Host entry in the `[[HTTP Port Check]]` subsection
  - Host entry in the `[[SMTP Port Check]]` subsection
  - Host entry in the `[[POP3 Port Check]]` subsection
  - Host entry in the `[[LDAP Port Check]]` subsection
  - Host entry in the `[[NNTP Port Check]]` subsection

## (c) In PFM - Agent for Enterprise Applications

Execute the `jpccconf inst setup` command for all created instance environments. For example, if an instance environment `o246bcisd500` exists in PFM - Agent for Enterprise Applications, execute the following command:

```
jpccconf inst setup -key agtm -inst o246bcisd500 -lhost jp1-halr3
```

In this example, the `jpccconf inst setup` command is executed in interactive mode. However, the command can also be executed in non-interactive mode.

When you execute the `jpccconf inst setup` command, specify the new host name at the `ASHOST` prompt. The other items are optional. Items for which you do not specify a value retain the existing setting.

## 10.5.4 Changing the logical host environment after starting operation

This subsection describes how to perform operations such as modifying the `jpchosts` file and changing port numbers or the environment directory path when Performance Management is running in a logical host environment.

These settings are required if you want to start PFM - Manager in a logical host environment.

### (1) Modifying the `jpchosts` file

1. Edit the `jpchosts` file on the executing node.
2. Copy the `jpchosts` file from the executing node to the standby node.

## (2) Changing or adding port numbers

1. Set the port numbers by executing the `jpccconf port define` command on the executing node.

Place the shared disk online before you execute the command.

For example, execute the following command to set all of the port numbers for the services on the logical host `jp1-ha1` to the default values:

```
jpccconf port define -key all -lhost jp1-ha1
```

When you execute the `jpccconf port define` command, the port numbers and service names of Performance Management (by default, TCP services whose names start with `jp1pc`) are defined in the `services` file.

For details on how to set port numbers, see the chapter describing installation and setup (in UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

For details on the `jpccconf port define` command, see the chapter on commands in the manual *JPI/Performance Management Reference*.

2. Execute the `jpccconf ha export` command on the executing node.

The settings for Performance Management in the logical host environment are exported to a file you specify.

For example, execute the command as follows to export the settings for the logical host environment to the file `lhostexp.conf`:

```
jpccconf ha export -f lhostexp.conf
```

3. Copy the file you exported using the `jpccconf ha export` command from the executing node to the standby node.

4. Execute the `jpccconf ha import` command to import the exported file into the standby node.

The shared disk does not need to be online on the standby node during this step.

The environment definition file exported from the executing node is imported into the standby node.

For example, execute the command as follows to import the file `lhostexp.conf`:

```
jpccconf ha import -f lhostexp.conf
```

When you execute the `jpccconf ha import` command, the environment of the standby node becomes the same environment as the executing node.

## (3) Changing the environment directory path

To change the environment directory path when you are already using Performance Management in a logical host environment:

- For PFM - Manager, PFM - Base, PFM - Agent, and PFM - RM

The logical host must be set up again. Use the following procedure to perform migration. For details about how to unset up and set up PFM - Agent or PFM - RM as described in steps 2 and 3, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

1. Back up the definition information or operation monitoring data.
2. Unset up the logical host environment.
3. Set up the logical host with a new environment directory path specified.
4. Restore the definition information or operation monitoring data.

- For PFM - Web Console

1. Stop PFM - Web Console.

2. Change the environment directory path.

For details, see *10.4.3(3)(e) Setting up the storage location for bookmark definition information* and *10.4.3(3)(f) Setting the storage location for process monitoring definition templates*.

When you want to inherit the bookmark definition information and process monitoring definition templates, copy the appropriate folder beforehand.

3. Start PFM - Web Console.

## 10.6 Operation in a cluster system

---

### 10.6.1 Starting and stopping Performance Management in a cluster system

This section describes starting up and stopping Performance Management on a logical host in a cluster system.

The order to start up and stop Performance Management is the same as for non-cluster systems. For details, see *1. Starting and Stopping Performance Management*.

#### (1) Starting up Performance Management

##### (a) Starting services manually

To start up Performance Management used on a logical host, use the cluster software to start up the logical host on which Performance Management has been registered.

#### Important

If you start up Performance Management using a method other than the cluster software, there might be a difference between the actual Performance Management status and the status controlled by the cluster software, causing an error to be assessed.

##### (b) Starting services automatically

If you wish to automatically start up Performance Management used on a logical host when starting up the cluster system, set the system so that the cluster software automatically starts up the logical host on which Performance Management has been registered.

#### (2) Stopping Performance Management

##### (a) Stopping services manually

Use the cluster software to stop the logical host on which Performance Management has been registered to stop Performance Management used on a logical host.

#### Important

- If you stop Performance Management using a method other than the cluster software, such as by using the `jpcspm stop` command, there might be a difference between the actual Performance Management status and the status controlled by the cluster software, causing an error to be assessed.
- Use the cluster software to stop Performance Management if, when changing Performance Management settings, you want to only stop Performance Management without stopping resources such as the shared disk and logical IP address. If the cluster software does not have the ability to stop Performance Management only, temporarily suppress monitoring of Performance Management actions, and then use the `jpcspm stop` command to manually stop Performance Management. In such cases, you need to prepare a mechanism to suppress monitoring of actions when you register Performance Management in the cluster,

## (b) Stopping services automatically

If you wish to automatically stop Performance Management used on a logical host when stopping the cluster system, set the system so that the cluster software automatically stops the logical host on which Performance Management has been registered.

### Tip

Methods to stop Performance Management include stopping the logical host and then stopping the node, or performing failovers for the logical host to another node and then stopping the node.

## (3) Service names

Performance Management on a logical host has the following service names (in Windows) or process names (in UNIX or Linux), and they are different from cases in which Performance Management is run in a non-cluster system.

Notes about the current directory when a logical host is used:

When PFM - Manager is used on a logical host, the current directory of the services is the directory on the shared disk on which you configured the environment.

For that reason, the services directory name displayed in the window of PFM - Web Console is not the installation directory but is instead the directory on the shared disk.

The following table lists Windows service names or process names on the physical host and logical host. INST means the instance name and LHOST means the logical host name.

Table 10–12: Service names on physical and logical hosts (in Windows)

Performance Management service name	Windows service name on physical host	Windows service name on logical host
Action Handler	PFM - Action Handler	PFM - Action Handler [LHOST]
Agent Collector and Remote Monitor Collector (for a single instance)	PFM - Agent Collector for xxxx <sup>#</sup>	PFM - Agent Collector for xxxx <sup>#</sup> [LHOST]
Agent Collector and Remote Monitor Collector (for multi-instances)	PFM - Agent Collector for xxxx <sup>#</sup> INST	PFM - Agent Collector for xxxx <sup>#</sup> INST [LHOST]
Agent Collector (for health check agent)	PFM - Agent for HealthCheck	PFM - Agent for HealthCheck [LHOST]
Agent Store and Remote Monitor Store (for a single instance)	PFM - Agent Store for xxxx <sup>#</sup>	PFM - Agent Store for xxxx <sup>#</sup> [LHOST]
Agent Store and Remote Monitor Store (for multi-instances)	PFM - Agent Store for xxxx <sup>#</sup> INST	PFM - Agent Store for xxxx <sup>#</sup> INST [LHOST]
Agent Store (for health check agent)	PFM - Agent Store for HealthCheck	PFM - Agent Store for HealthCheck [LHOST]
Correlator	PFM - Correlator	PFM - Correlator [LHOST]
Master Manager	PFM - Master Manager	PFM - Master Manager [LHOST]
Master Store	PFM - Master Store	PFM - Master Store [LHOST]
Name Server	PFM - Name Server	PFM - Name Server [LHOST]
Trap Generator	PFM - Trap Generator	PFM - Trap Generator [LHOST]
Web Console	PFM - Web Console	PFM - Web Console
Web Service	PFM - Web Service	PFM - Web Service

Performance Management service name	Windows service name on physical host	Windows service name on logical host
View Server	PFM - View Server	PFM - View Server [ <i>LHOST</i> ]

#

xxxx indicates the name of the monitored program for each PFM - Agent or PFM - RM.

**Table 10–13: Process names on physical and logical hosts (in UNIX)**

Performance Management service name	Process name on physical host	Process name on logical host
Action Handler	jpcah	jpcah <i>LHOST</i>
Agent Collector and Remote Monitor Collector (for a single instance)	jpcagtX <sup>#</sup>	jpcagtX <sup>#</sup> <i>LHOST</i>
Agent Collector and Remote Monitor Collector (for multi-instances)	jpcagtX <sup>#</sup> _INST	jpcagtX <sup>#</sup> _INST <i>LHOST</i>
Agent Collector (for health check agent)	jpcagt0	jpcagt0 <i>LHOST</i>
Agent Store and Remote Monitor Store (for a single instance)	agtX <sup>#</sup> /jpcsto	agtX <sup>#</sup> /jpcsto <i>LHOST</i>
Agent Store and Remote Monitor Store (for multi-instances)	agtX <sup>#</sup> /jpcsto_INST	agtX <sup>#</sup> /jpcsto_INST <i>LHOST</i>
Agent Store (for health check agent)	agt0/jpcsto	agt0/jpcsto <i>LHOST</i>
Correlator	jpcep	jpcep <i>LHOST</i>
Master Manager	jpcomm	jpcomm <i>LHOST</i>
Master Store	mgr/jpcsto	mgr/jpcsto <i>LHOST</i>
Name Server	jpensvr	jpensvr <i>LHOST</i>
Trap Generator	jpctrap	jpctrap <i>LHOST</i>
View Server	jpcevsvr	jpcevsvr <i>LHOST</i>

#

X indicates the product ID of each PFM - Agent or PFM - RM.

**Table 10–14: Process names on physical and logical hosts**

Performance Management service name	Process name on physical host	Process name on logical host
Web Console	cjstartweb <sup>#</sup> PFMWebConsole	Same as on physical host
Web Service	httpsd <sup>#</sup> -R /opt/jp1pcwebcon/CPSB/httpsd/libexec	Same as on physical host
	cprfd <sup>#</sup> -PRFID PFMWebCon -CTMID PFMWebCon	Same as on physical host

#

When you display process information using the `ps` command, process names might appear with their absolute paths in the command column, or might appear with different options from those shown above. Check how the process name appears in your environment before using it.

## 10.6.2 Managing user accounts in a cluster system

The system administrator logs on to the system from the window of PFM - Web Console and manages user accounts.

### (1) Logging on to PFM - Web Console

The procedure for logging on to PFM - Web Console is the same as that for a non-cluster system. However, enter the following URL in the Web browser to display the PFM Web Console login window:

```
http://name-of-host-on-which-PFM-Web-Console-is-installed:20358/  
PFMWebConsole/login.do
```

Specify the logical IP address or the logical host name for *name-of-host-on-which-PFM-Web-Console-is-installed*.

In addition, change the URL to log on to according to the environment as follows:

- If encrypted communication is enabled  
Change `http` to `https`.  
If a host name in FQDN format is specified as a common name in the certificate signing request file, change *name-of-host-on-which-PFM-Web-Console-is-installed* to *name-of-host-on-which-PFM-Web-Console-is-installed + domain-name*.
- If the port number has been changed  
Specify the new port number, not 20358.

For details on the logon procedure, see [1.5.1 Logging on to PFM - Web Console](#).

PFM - Web Console is connected using the logical IP address of the node that runs PFM - Manager when used on a logical host.

### (2) Managing user accounts

The managing of Performance Management user accounts is the same as with a non-cluster system. For details, see [2. Managing User Accounts and Business Groups](#).

## 10.6.3 Managing agents in an integrated cluster system

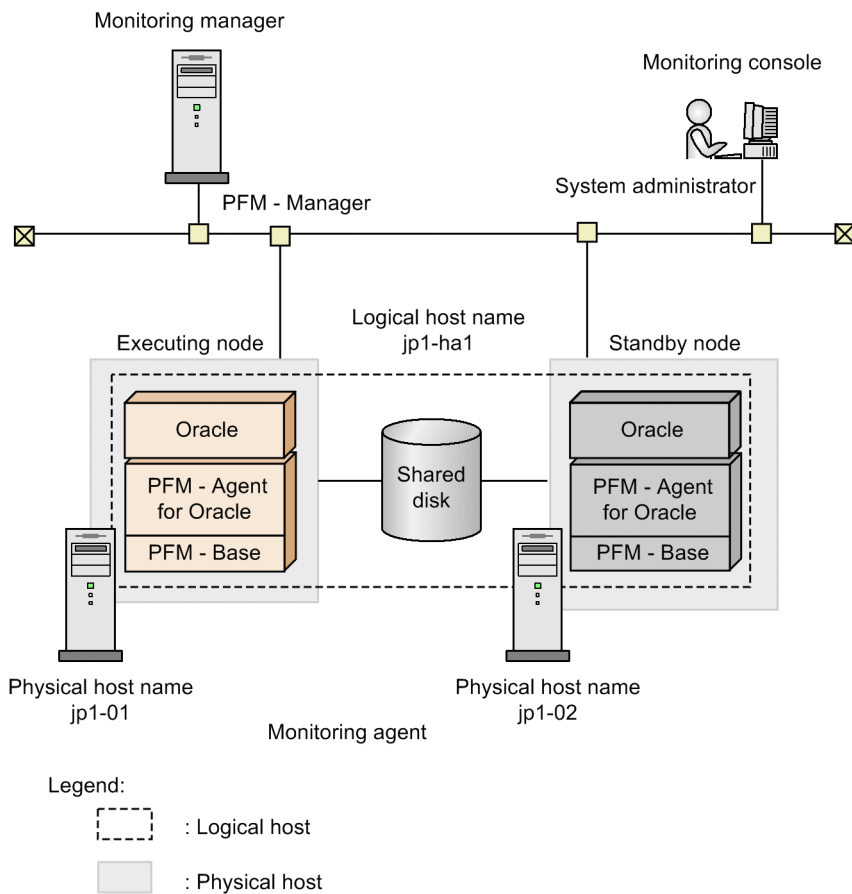
Only one agent with the logical host name is displayed in the window of PFM - Web Console when PFM - Agent or PFM - RM runs on a logical host in a cluster system. An agent using an executing node or standby node name is not displayed.

The agent that runs on the executing node is operated when you operate the agent displayed as the logical host name.

For example, when Oracle with a cluster configuration that runs in an environment having the same logical host name `jp1-ha1` is monitored by PFM - Agent for Oracle that runs in the environment having the same logical host name `jp1-ha1`, the operations are as shown in the following figure. An agent that runs on the logical host environment is displayed using the logical host name. You are automatically connected to PFM - Agent for Oracle that runs on the executing node when you operate this agent.



Figure 10–30: Example of monitoring Oracle by PFM - Agent for Oracle in a cluster configuration



**Tip**

The agent with the physical host name is displayed in the window of PFM - Web Console when PFM - Agent or PFM - RM runs on a non-cluster system.

### 10.6.4 Collecting and managing operation monitoring data in a cluster system

The collection and management of operation monitoring data is the same as with a non-cluster system. For details, see the chapter describing Performance Management functionality in the *JPI/Performance Management Planning and Configuration Guide*.

### 10.6.5 Creating reports in a cluster system

Reports are created in a cluster system in the same manner as with a non-cluster system. For details, see [5. Creation of Reports for Operation Analysis](#).

## 10.6.6 Performing realtime operation monitoring by alarms in a cluster system

Alarms need to be set in order to notify users when an error occurs in a monitoring target system. Note that the method of setting alarms is different from that for a non-cluster system when a logical host is used in a cluster system.

Notes about the nodes that executes actions:

- If `LOCAL` is set for **Command Execution Action Handler**, actions are executed on the node on which PFM - Agent or PFM - RM that performs alarm monitoring operates. For example, when an alarm occurs with PFM - Agent or PFM - RM used on a logical host, actions are executed on the executing node on which PFM - Agent or PFM - RM runs.
- When Performance Management runs on a logical host, if you specify the logical host name or `LOCAL` for **Command Execution Action Handler**, commands are executed on the node on which Performance Management operates. For that reason, you need to configure the environment in such a way that commands can be executed in the same way on both the executing and standby nodes.
- Also, if the Action Handler service runs on a logical host, the current directory is as described below. The environment directory means the environment directory name specified with the `jpccconf ha setup` command.

```
environment-directory\jplpc\bin\action\
```

- When Performance Management is running on a cluster system and a JP1 event is issued as an alarm action, the JP1 event is registered in the event server of JP1/Base on a physical host as standard behavior. When Performance Management and JP1/Base are operated on the same logical host, use the `-r logical-host-name` option to additionally specify the logical host name as the event server name in the message text (JP1 event attribute to be passed to the `jpccimevt` command) field where the JP1 event is registered.

You cannot specify the event server name of JP1/Base that runs on a different logical host.

For details on how to set alarms, see [6.4 Setting alarms using the Web browser \(Alarms tree\)](#).

## 10.6.7 Performing backup and restore in a cluster system

You need to back up the data periodically in case of problems when Performance Management runs on a logical host in a cluster system.

The following information needs to be backed up:

- Definition information required to operate Performance Management
  - Report definition information
  - Alarm table definition information
  - Service definition information
- Operation monitoring data collected by Performance Management
  - Performance data
  - Event data

In addition to the above, the bookmark definition information that is set in PFM - Web Console also needs to be backed up. Note that the information that needs to be backed up is the same as with a non-cluster system.

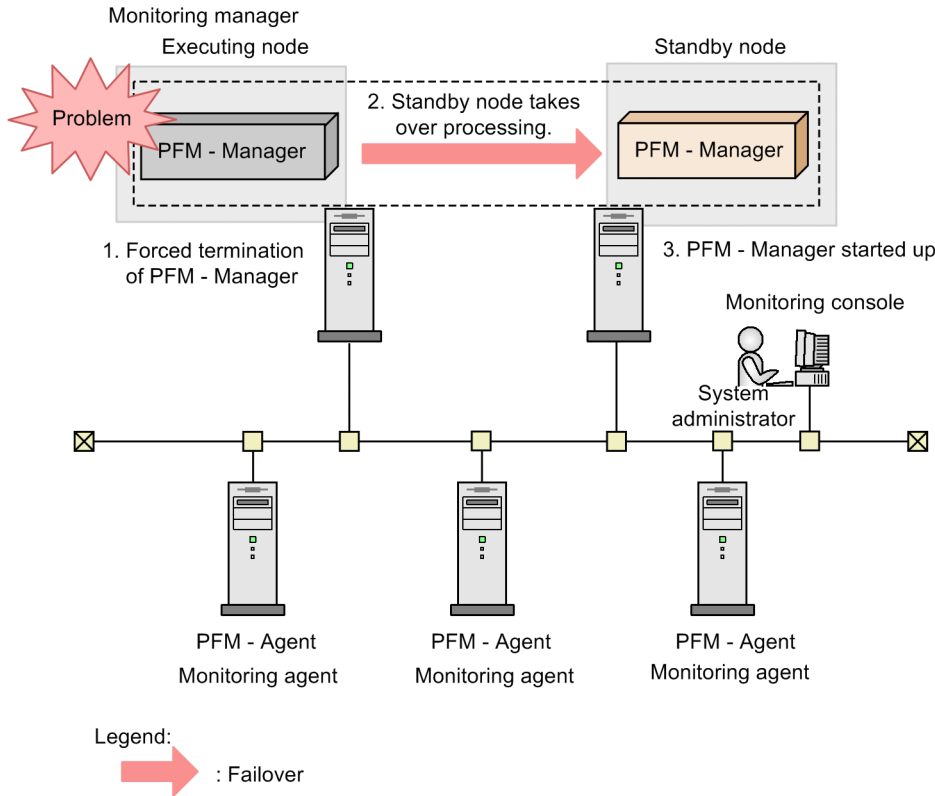
For details on how to perform backup and restore, see [9. Backing Up and Restoring Data](#).

## 10.6.8 Performing the required operation when a failover occurs in a cluster system

When a failure occurs on the executing node, the cluster software executes a failover and the standby node takes over the processing.

### (1) Flow of processing for a failover when a failure occurs in PFM - Manager

Figure 10–31: Flow of processing when a failover occurs on the PFM - Manager host



1. The cluster software forces PFM - Manager to terminate when a failover occurs.
2. The cluster software directs the standby node to take over the PFM - Manager processing from the executing node.
3. The cluster software starts up PFM - Manager on the standby node.

#### (a) Operation on PFM - Web Console

The KAVJS0012-E message is displayed if you are performing operations from a PFM - Web Console window when a failover occurs in PFM - Manager.

To connect to the failover destination PFM - Manager:

1. Log out from the window of PFM - Web Console.  
Click the **Logout** menu in the Main window.
2. Log on in the window of PFM - Web Console.  
Log on from the window of PFM - Web Console again after the failover destination PFM - Manager starts up.

## Important

If a failover occurs while you are working with the bookmarks, the information that was not correctly written in the bookmarks definition information is lost. Correct the bookmark definition if the bookmarks cannot be operated properly.

### (b) Operations using PFM - Agent or PFM - RM

You do not need to perform special operations in PFM - Agent or PFM - RM when a failover occurs in PFM - Manager during operation. The performance data continues to be collected in PFM - Agent or PFM - RM during a failover of PFM - Manager.

### (2) Effects when PFM - Manager stops

Stopping PFM - Manager affects the entire Performance Management system.

PFM - Manager performs integrated management of the agent information for each node where PFM - Agent or PFM - RM runs. Also, PFM - Agent or PFM - RM controls alarm event reports sent when a performance value exceeds a threshold value during monitoring and execution of actions triggered by an alarm event. For that reason, stopping PFM - Manager affects the Performance Management system in the areas listed in the following table.

Table 10–15: Effects on PFM - Web Console when PFM - Manager stops

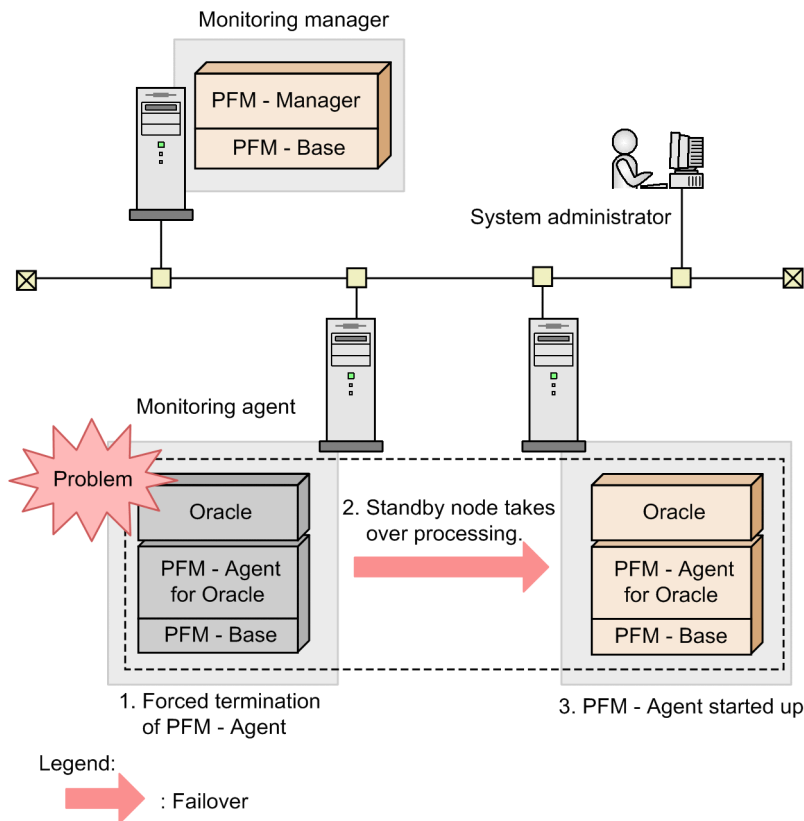
Effect	Solution
<ul style="list-style-type: none"><li>An alarm flashing in red in the window of PFM - Web Console returns to green immediately after PFM - Manager restarts or when a failover occurs, and then starts flashing in red again.</li></ul> <p>When PFM - Manager stops, the KAVJS0012-E message occurs and no further operations can be performed.</p>	Start up PFM - Manager, and then log on again.
<ul style="list-style-type: none"><li>You cannot log on to Performance Management when you attempt to log on from the window of PFM - Web Console if PFM - Manager has stopped.</li></ul>	Start up PFM - Manager, and then log on again.

Table 10–16: Effects on PFM - Agent or PFM - RM when PFM - Manager stops

Effect	Solution
<ul style="list-style-type: none"><li>The Performance data continues to be collected.</li><li>Since the alarm event that occurred cannot be reported to PFM - Manager, the alarm event is retained for each alarm definition and the report is retried until PFM - Manager starts up. The oldest alarm event is overwritten when more than three alarm events are retained. If PFM - Agent or PFM - RM is stopped, all retained alarm events are deleted.</li><li>When PFM - Manager restarts, the alarm status that has already been reported to PFM - Manager is reset at once. Then PFM - Manager checks the status of PFM - Agent or PFM - RM and updates the alarm status.</li><li>When you attempt to stop PFM - Agent or PFM - RM, it takes time because the attempt to stop the program is not sent to PFM - Manager.</li></ul>	<p>Start up PFM - Manager.</p> <p>You can continue using the PFM - Agent or PFM - RM that is running without any changes. However, since an alarm might not be reported as expected, check the KAVE00024-I message output to the common message log of PFM - Agent or PFM - RM after PFM - Manager recovers.</p>

### (3) Overview of failover when a failure occurs in PFM - Agent or PFM - RM

Figure 10–32: Flow of processing when a failover occurs in PFM - Agent or PFM - RM



1. The cluster software forces PFM - Agent or PFM - RM to terminate when a failover occurs.
2. The cluster software directs the standby node to take over the PFM - Agent or PFM - RM processing from the executing node.
3. The cluster software starts up PFM - Agent or PFM - RM on the standby node.

#### (a) Operations in the window of PFM - Web Console

A message appears, according to the status, if you operate in the window of PFM - Web Console during a PFM - Agent or PFM - RM failover. In such cases, wait until the failover completes and the operation starts.

If you operate in the window of PFM - Web Console after the PFM - Agent or PFM - RM failover, you will be connected to and operate PFM - Agent or PFM - RM that is started up on the failover destination node.

## 10.7 Failure recovery in a cluster system

---

When a failure occurs on the executing node, the cluster software executes a failover and the standby node takes over the processing. When a failover takes place, processing that was being executed by the executing node stops.

The system administrator identifies the cause of the failure that occurred on the executing node. After removing the cause of the failure, you need to switch the processing to the executing node to recover from the failure.

Collect and analyze the following log information to identify the cause of the failure:

- Performance Management log information

This information is the same as that collected in a non-cluster system. Collected information includes:

- System log
- Common message log
- Operation status log
- Trace log
- Cluster software and OS log information

We recommend that you also collect the log information for the cluster system, and the log information output by the operating system itself.

For details on the log information output by Performance Management, see [17.4 Log information to be output when Performance Management is used](#).

### 10.7.1 Collecting the log information in a cluster system

Pay attention to the following items when you collect the Performance Management log information in a cluster system:

- The common message log and trace log are output to the shared disk when Performance Management is used on a logical host.  
Log information before and after the failover is recorded in the same log file since the log file on the shared disk is inherited together with the system when a failover takes place.
- If Performance Management is used on a logical host, it is necessary to refer to the information from around the time when a failure occurs. For this reason, you need to extract the log information on both the executing node that stopped the processing due to the failover and the failover destination standby node.

For details on how to collect the log information output by Performance Management, see [17.6 Procedures for collecting data in the event of trouble](#).

## 10.8 Notes on cluster systems

---

### 10.8.1 Detecting failovers

It is difficult for Performance Management to detect failovers on PFM - Manager, PFM - Agent, or PFM - RM nodes. To detect the occurrence of a failover, you need to utilize methods such as using cluster software management tools, SNMP traps issued by the cluster software, or message monitoring of log files. For details on message monitoring of log files, see *16.5 Detecting problems by linking with the integrated system monitoring product*.

### 10.8.2 Starting and stopping Performance Management

Use the cluster software to start and stop Performance Management that is used on a logical host registered in the cluster software. If you start or stop Performance Management by executing the `jpcspm start` or `jpcspm stop` command outside the operating cluster software, issues like the following might occur:

- There is a difference between the actual Performance Management status and the status controlled by the cluster software, which is incorrectly reported as an error
- There is a conflict between attempts to start and stop Performance Management from the cluster software and by direct execution of commands, preventing you from starting or stopping Performance Management as intended.

### 10.8.3 Setting Status Server services

One host can run only one Status Server service. For that reason, the Status Server service on a physical host manages the status of the physical host and logical host services. You need to set the Status Server service not to perform a failover or run constantly.

### 10.8.4 Executing commands

Only the executing node can execute the following PFM - Web Console commands when Performance Management is used on a logical host:

- `jpcaspsv` command
- `jpcasrec` command
- `jpcmkkey` command
- `jpcprocdef` command
- `jpcrdef` command
- `jpcrpt` command

Both the executing node and standby node can execute the `jpcwras` and `jpcwagtsetup` commands. These two commands act for the physical host that executes the commands.

## 10.8.5 Networks

Performance Management on a physical host cannot operate if it cannot communicate using the physical IP address that corresponds to the physical host name (in the Windows system, the host name displayed when the `hostname` command is executed, and in the UNIX system, the host name displayed when the `uname -n` command is executed).

## 10.8.6 When using JP1 authentication mode

To use JP1 authentication mode in an environment using PFM - Manager on a cluster system, JP1/Base must also be used on the cluster system. The JP1/Base version must be 10-00 or later.



# 11

## Configuring and Employing Performance Management for Multiple Monitoring

This chapter describes how to set up Performance Management for multiple monitoring and how to duplicate the definition information. It also explains the processing flow when Performance Management is running in a multiple-monitoring configuration.

## 11.1 Overview of multiple monitoring

---

### 11.1.1 About multiple monitoring

The multiple-monitoring functionality lets two managers (PFM - Manager and PFM - Web Console) monitor the same agents (PFM - Agent and PFM - RM). The monitoring agents (PFM - Agent and PFM - RM) send data to and receive data from each of the managers.

One of two managers for multiple monitoring is designated as the *primary Manager* and the other as the *secondary Manager*. The primary Manager has priority when communicating with the monitoring agents.

### 11.1.2 Features of multiple monitoring

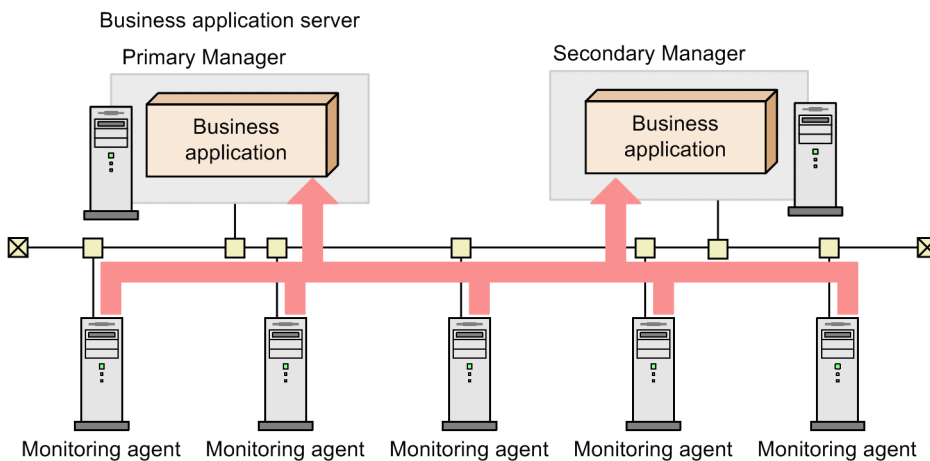
In a multiple-monitoring configuration, even if an error occurs on the primary Manager, the secondary Manager can continue monitoring. This reduces monitoring downtime and improves the availability.

In addition, as a crisis management measure, you can place the two managers on separate sites so that information assets are saved in separate locations.

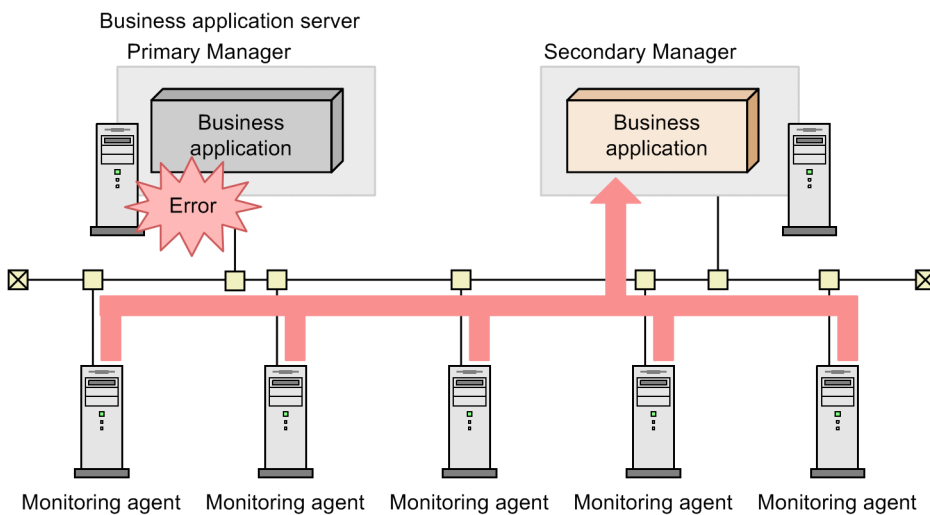
The following figure shows how performance data flows when an error occurs on the primary Manager.

Figure 11–1: Flow of performance data when an error occurs on the primary Manager in a multiple-monitoring configuration

Flow of performance data when the primary Manager operates normally



Flow of performance data when there is a failure on the primary Manager



Legend:

- : Flow of performance data
- : Running application
- : Waiting application

When you employ multiple monitoring, the definition information of the managers must be duplicated. Definition information set on one manager (PFM - Manager and PFM - Web Console) can only migrate to the other manager by an export and import.

When you set remote actions, you can select which manager executes remote actions for events that are sent from the monitoring agent. For details, see [11.3.5 Controlling remote actions](#).

In a multiple-monitoring configuration, the secondary Manager cannot perform some operations because consistency must be maintained between the primary Manager and the secondary Manager. The following describes operations which the secondary Manager cannot perform.

PFM - Manager commands:

- `jpccconf agttree import command`

- `jpccconf bgdef delete` command
- `jpccconf bgdef import` command
- `jpctool alarm active` command
- `jpctool alarm bind` command
- `jpctool alarm copy` command
- `jpctool alarm delete` command
- `jpctool alarm import` command
- `jpctool alarm inactive` command
- `jpctool alarm unapplied` command
- `jpctool alarm unbind` command
- `jpctool config alarmsync` command
- `jpctool monitor resume` command
- `jpctool monitor suspend` command

PFM - Web Console commands:

- `jpcrdef create` command
- `jpcrdef delete` command

Operations in PFM - Web Console:

- Updating the PFM - Manager definition (except for properties operation)
- Setting binding of alarm tables
- Starting and stopping monitoring
- Suspending and resuming monitoring
- Checking alarm application status and applying alarm information
- Updating the bookmark of PFM - Web Console
- Updating the process monitoring template of PFM - Web Console

When an error occurs on the primary Manager, you can switch from the primary Manager to the secondary Manager to perform the above operations, thus giving the previously secondary Manager the primary functions. For details, see [11.7 Switching the primary Manager and the secondary Manager](#).

### 11.1.3 Definition information for multiple monitoring

This subsection describes definition information that needs to be matched between the primary Manager and the secondary Manager.

#### (1) Definition information on the primary Manager that needs to be duplicated on the secondary Manager

Set the definition information shown in the following table on the primary Manager and duplicate it onto the secondary Manager.

If you configure a multiple-monitoring environment and then change the definition information, you must duplicate the definition information on the primary Manager onto the secondary Manager. For details about how to duplicate the definition information, see *11.5 Duplicating definition information*.

**Table 11–1: Definition information to be duplicated from the primary Manager onto the secondary Manager**

No.	Definition information	How to check	How to match
1	Alarm information (alarm definition / Action definition)	See <i>11.6.1(1) Checking alarm information of alarm definition and action definition</i> .	See <i>11.5 Duplicating definition information</i> .
2	Binding information	See <i>11.6.1(2) Checking binding information</i> .	
3	Report definition	See <i>11.6.1(3) Checking report definitions</i> .	
4	Business group information	See <i>11.6.1(4) Checking business group information</i> .	
5	Performance Management user account information	See <i>11.6.1(5) Checking Performance Management user account information and Agents tree (User Agents) information</i> .	
6	Agents tree (User Agents) information		
7	Auto alarm bind setting	See <i>11.6.1(8) Checking the settings of auto alarm bind</i> .	
8	Bookmark definition information	See <i>11.6.2(1) Checking bookmark definition information</i> .	
9	Process monitoring template information	See <i>11.6.2(2) Checking process monitoring template information</i> .	

## (2) Definition information for which the same setting must be specified on the primary Manager and the secondary Manager

The definition information shown in the following table must be set on both the primary Manager and the secondary Manager. You must make the settings consistent between the primary Manager and the secondary Manager. You can check whether the settings are consistent by using the method shown in the *How to check* column.

If you configure a multiple-monitoring environment and then change the definition information, you must match the information of the primary Manager and the secondary Manager. See the *How to match* column and take appropriate action.

**Table 11–2: Definition information for which the same setting must be specified on the primary Manager and the secondary Manager**

No.	Definition information	How to check	How to match
1	Managed agent information	See <i>11.6.1(6) Checking managed agent information</i> .	See the chapter that describes how to delete service information in the <i>JP1/Performance Management Planning and Configuration Guide</i> (This definition

No.	Definition information	How to check	How to match
1	Managed agent information	See <a href="#">11.6.1(6) Checking managed agent information.</a>	information becomes inconsistent only when the number of PFM - Agent or PFM - RM services managed by PFM - Manager is reduced).
2	Settings of PFM - Manager for the connection destination	See <a href="#">11.6.1(7) Checking the settings of PFM - Manager for the connection destination.</a>	See <a href="#">11.3.4 Setting PFM - Manager for the connection destination for multiple monitoring.</a>
3	Settings of the health check agent	Check whether editable properties values for the host name <Health Check> on the Services tree and the host name <Health Check> (store) match. <sup>#1</sup>	See <a href="#">3.4.8 Distributing agent properties as a batch</a> and distribute properties from the health check agent on the primary Manager to that on the secondary Manager.
4	JP1/SLM linkage definition information <ul style="list-style-type: none"> <li>Linked JP1/SLM host name</li> </ul>	Check whether the properties values of the <b>ITSLM Coordination Configuration/ITSLM Coordination</b> node in the Service Properties window for the Master Manager service on the Services tree match. <sup>#1</sup>	Match the editable properties values of <b>ASSIGN ITSLM COORDINATION</b> of the <b>ITSLM Coordination Configuration/MANAGE ITSLM COORDINATION</b> node in the Service Properties window for the Master Manager service on the Services tree. <sup>#1</sup>
5	Settings related to JP1 events	In the Service Properties window for the Master Manager service on the Services tree, check whether the editable properties values of the <b>JP1 Event Configurations</b> node, the <b>JP1 Event Configurations/Alarm</b> node, and the <b>JP1 Event Configurations/System</b> node match. <sup>#1</sup>	In the Service Properties window for the Master Manager service on the Services tree, match the editable properties values of the <b>JP1 Event Configurations</b> node, the <b>JP1 Event Configurations/Alarm</b> node, and the <b>JP1 Event Configurations/System</b> node. <sup>#1</sup>
6	JP1/SLM linkage definition information <ul style="list-style-type: none"> <li>Custom monitoring items</li> </ul>	Check whether the contents of the <code>monitoringitems.cfg</code> files match. <sup>#2</sup>	See the chapter that describes definition files in the manual <i>JP1/Performance Management Reference</i> and match the <code>monitoringitems.cfg</code> setting values.
7	Host information configuration file ( <code>jpchosts</code> )	Check whether the contents of the <code>jpchosts</code> files match. <sup>#2</sup>	See the chapter that describes how to set IP addresses in the <i>JP1/Performance Management Planning and Configuration Guide</i> and match the <code>jpchosts</code> settings.
8	Setting of Authentication mode	Check whether the <code>UserServer.authenticationMode</code> label values in the <code>jpccsvr.ini</code> files match. <sup>#2</sup>	See <a href="#">2.4 Setting the user account authentication mode</a> and match the <code>UserServer.authenticationMode</code> label value.
9	Startup information (definition in <code>jpccomm.ini</code> )	Necessity for matching differs depending on the setting items. See <a href="#">Table 11-3 Definition information that must be matched in jpccomm.ini.</a>	
10	Health check function	Check whether the execution result of the <code>jpccconf hc display</code> command matches.	Execute the <code>jpccconf hc enable</code> command or the <code>jpccconf hc disable</code> command to match the setting. <sup>#3</sup>
11	Status management function	Check whether the execution result of the <code>jpccconf stat display</code> command matches.	Execute the <code>jpccconf stat enable</code> command to match the setting. <sup>#3</sup>
12	Product name display function	Check whether the execution result of the <code>jpccconf prodname display</code> command matches.	Execute the <code>jpccconf prodname enable</code> command or the <code>jpccconf prodname disable</code> command to match the setting. <sup>#3</sup>

No.	Definition information	How to check	How to match
13	IPv6 communication	Check whether the execution result of the <code>jpccconf ipv6 display</code> command matches.	Execute the <code>jpccconf ipv6 enable</code> command or the <code>jpccconf ipv6 disable</code> command to match the setting. <sup>#3</sup>
14	Port number settings	Check whether the execution result of the <code>jpccconf port list -key stat</code> command matches. <sup>#4</sup>	Execute the <code>jpccconf port define -key stat</code> command to match the setting. <sup>#3</sup>
15	Encrypted communication	Check whether the execution result of the <code>jpccwconf https display</code> command matches.	Execute the <code>jpccwconf https enable</code> command or the <code>jpccwconf https disable</code> command to match the setting. <sup>#3</sup>

#1

For details, see the appendix that describes verification of definition information in the manual *JP1/Performance Management Reference*.

#2

For details, see the appendix that lists files and directories in the manual *JP1/Performance Management Reference*.

#3

For details, see the chapter that describes commands in the manual *JP1/Performance Management Reference*.

#4

The port number of Name Server and Status Server must match.

The following table shows definition information that must be matched in the startup information file (`jpccomm.ini`).

**Table 11–3: Definition information that must be matched in `jpccomm.ini`**

No.	Section name	Label name
1	Common Section	Multiple Alarm Table Bind
2		Alarm Message Mode
3		JP1 Event Double Quote
4		Correlator Startup Mode
5		Retry Getting Alarm Status
6		Business Group Monitor Mode
7		Agent Remote Protection
8		Service List Protection
9		Prioritize Manager Startup Communication
10		Remote Action Control
11		Alarm Command Wait Mode
12		Alarm Command Timeout
13		Historical Data Collection Priority Mode
14		Random Retry Mode
15		Monitoring Suspend Mode
16		Auto Sync for Suspend Setting
17		Auto Alarm Bind Mode
18	All sections other than the following sections: <ul style="list-style-type: none"> <li>Common Section</li> </ul>	NS Keepalive Mode

No.	Section name	Label name
18	• Action Log Section	NS Keepalive Mode
19	All the following sections: • Name Server Section • Master Manager Section • Correlator Section	NS Connection Timeout <sup>#</sup>
		NS Maximum Connections
20	Tools Section	StartService Retry Interval
21		StartService Retry Count
22	Agent Collector 0 Section	Historical Data Collection Priority Mode
23	Action Handler Section	Action Execution Count Limitation
24		Action Concurrent Execution Count
25		Action Execution Queue Count
26		Action Execution Time Limit

#

With version 11-50 or later, if the value differs between the primary and secondary managers, set the value to 70.

If an item in the startup information file (`jpccomm.ini`) is inconsistent, take action as follows:

1. Stop the Performance Management programs and services.
2. Open `jpccomm.ini` with a text editor.
3. Match the section names and label names of PFM - Manager in [Table 11-3](#) between the primary Manager and the secondary Manager.
4. Save and close `jpccomm.ini`.
5. Start the Performance Management programs and services.

For details, see the chapter that describes definition files in the manual *JPI/Performance Management Reference*.

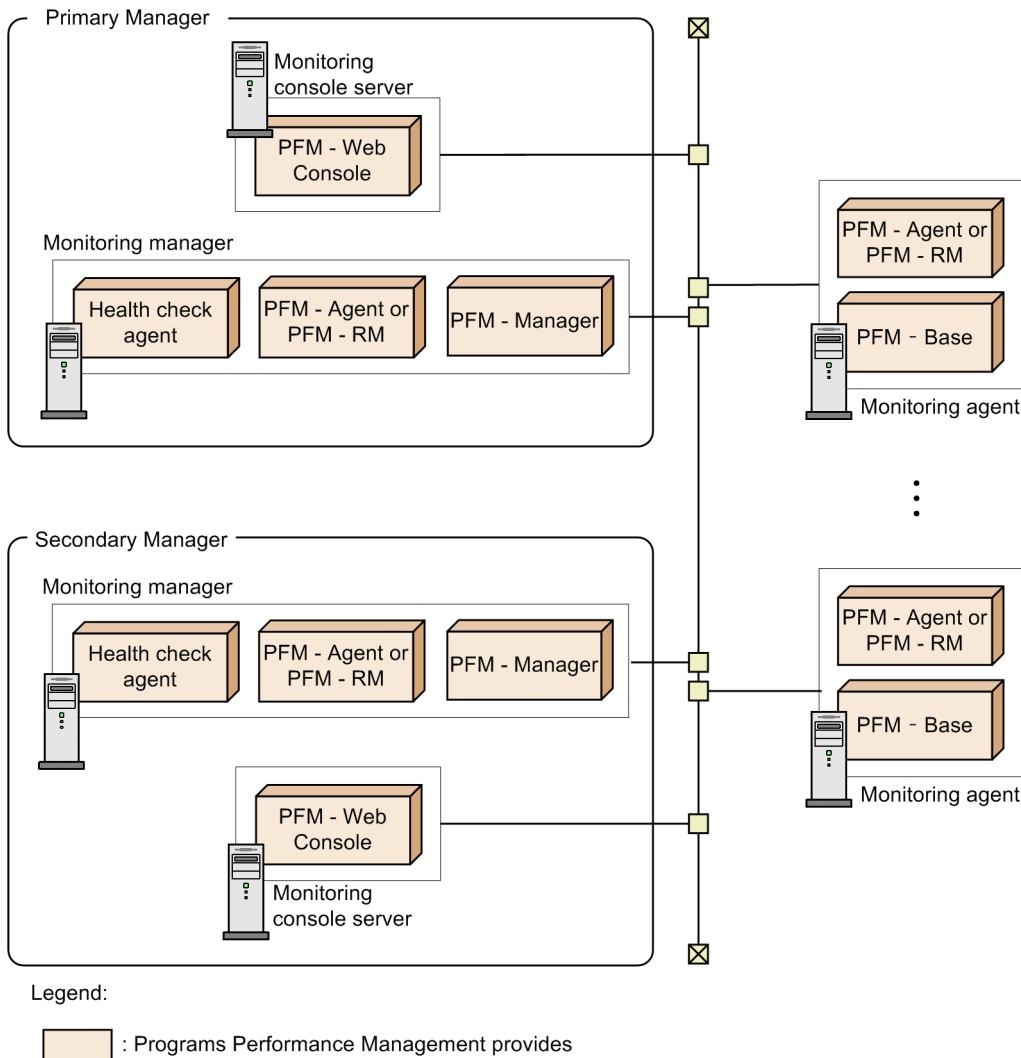


## 11.2 Before configuring a multiple-monitoring environment

### 11.2.1 System configuration for multiple monitoring

The following figure shows a system configuration for multiple monitoring.

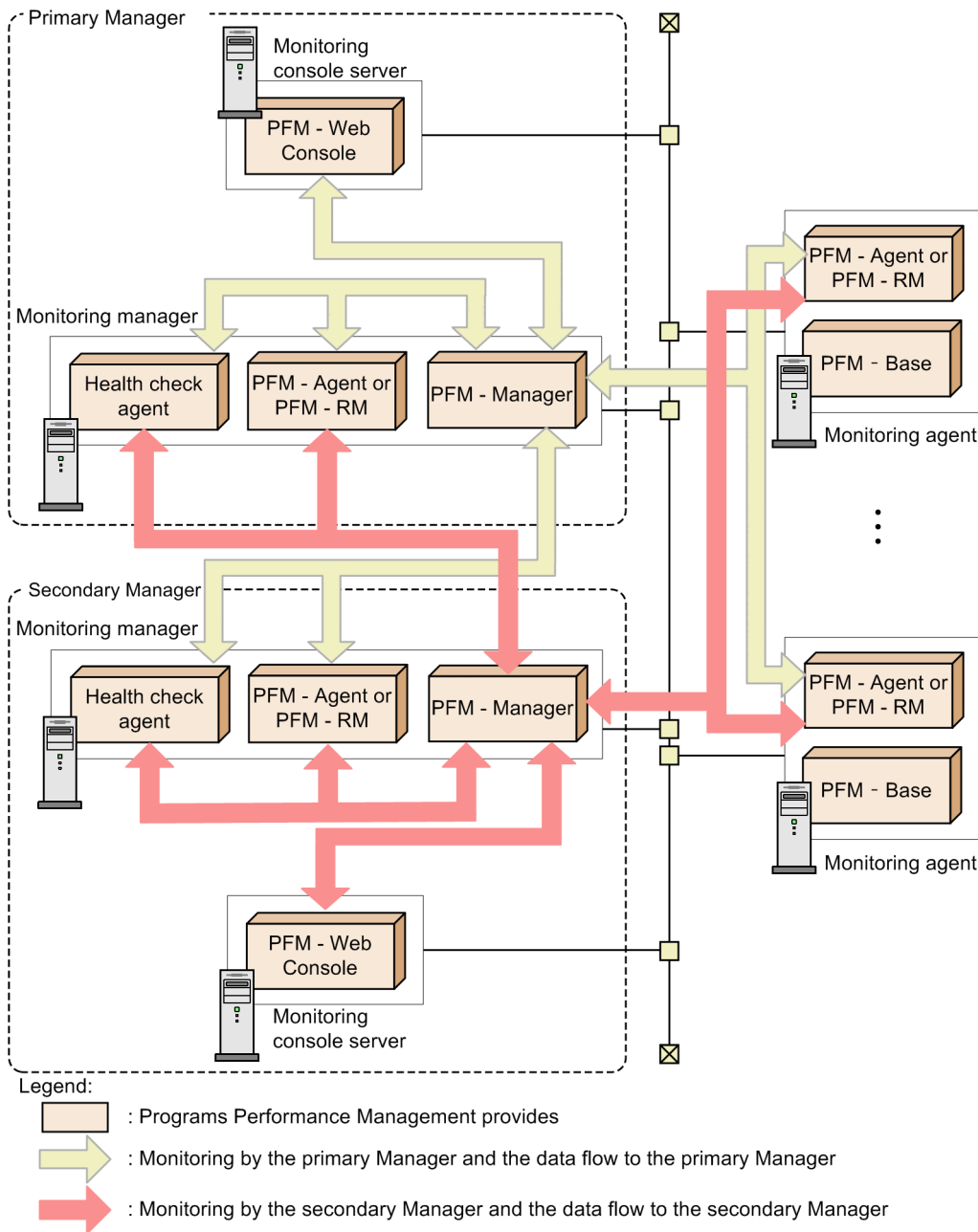
Figure 11–2: System configuration for multiple monitoring



Multiple monitoring needs two server sets consisting of a monitoring manager and a monitoring console server. These sets are referred to as the *primary Manager* and the *secondary Manager*.

The following figure shows the relationships of the programs used for multiple monitoring.

Figure 11–3: Relationships of programs for multiple monitoring



PFM - Web Console cannot be connected to two PFM - Manager services. Connect PFM - Manager with PFM - Web Console on a one-to-one basis.

The primary Manager and the secondary Manager must manage the same monitoring agent.

The following are prerequisites that are common to PFM - Manager on the primary Manager, PFM - Manager, PFM - Agent, and PFM - RM on the secondary Manager:

- The status management function is enabled.
- The settings of PFM - Manager for the connection destinations match.
- The operation mode for remote actions matches.

## 11.2.2 Prerequisite product version

The following table shows prerequisite program version for multiple monitoring.

Table 11–4: Prerequisite program version

Host	Product name	Supporting version
PFM - Manager host	PFM - Manager	10-10 or later
	PFM - Agent	10-00 or later
	PFM - RM	10-00 or later
PFM - Web Console host	PFM - Web Console	10-10 or later
PFM - Agent host or PFM - RM host	PFM - Base	10-10 or later
	PFM - Agent	10-00 or later
	PFM - RM	10-00 or later

## 11.2.3 Prerequisites related to PFM - Manager

Make sure the following conditions are met.

### (1) Version

VV-RR-SS of the version of PFM - Manager must match between the primary Manager and the secondary Manager.

For details about how to check the version information, see the appendix that describes how to check the version information in the *JP1/Performance Management Planning and Configuration Guide*.

### (2) OS

The version of the OS that PFM - Manager runs on must be the same for the primary Manager and the secondary Manager. However, the service packs do not have to be the same.

### (3) System configuration

PFM - Manager on the primary Manager and the secondary Manager must not be set up in a logical host environment.

## 11.2.4 Prerequisites related to PFM - Web Console

Make sure the following conditions are met.

### (1) Version

VV-RR-SS of the version of PFM - Web Console must match between the primary Manager and the secondary Manager.

For details about how to check the version information, see the appendix that describes how to check the version information in the *JP1/Performance Management Planning and Configuration Guide*.

## **(2) OS**

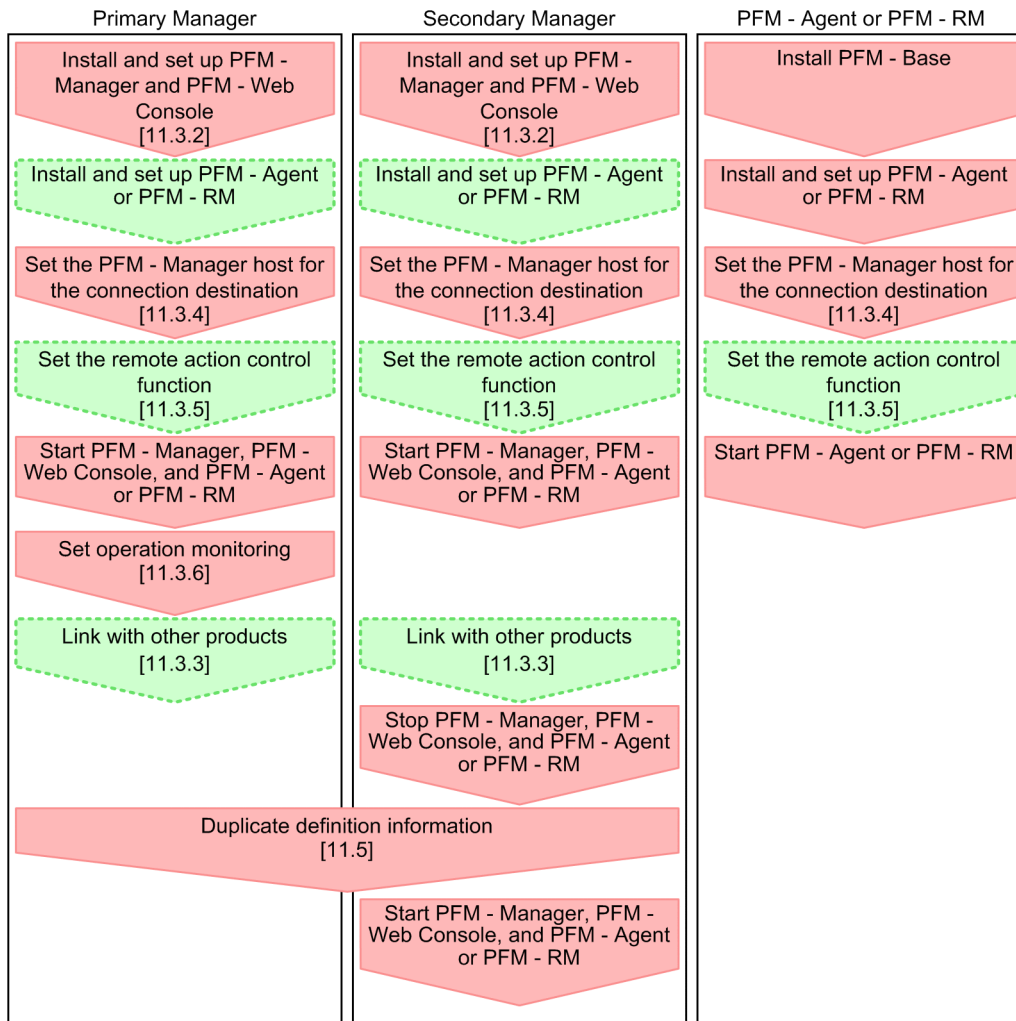
The version of the OS that PFM - Web Console runs on must be the same for the primary Manager and the secondary Manager. However, the service packs do not have to be the same.

## 11.3 Setting up multiple monitoring

### 11.3.1 Procedure for setting up multiple monitoring

The following figures show the procedures for setting up multiple monitoring in two cases with different installation environments.

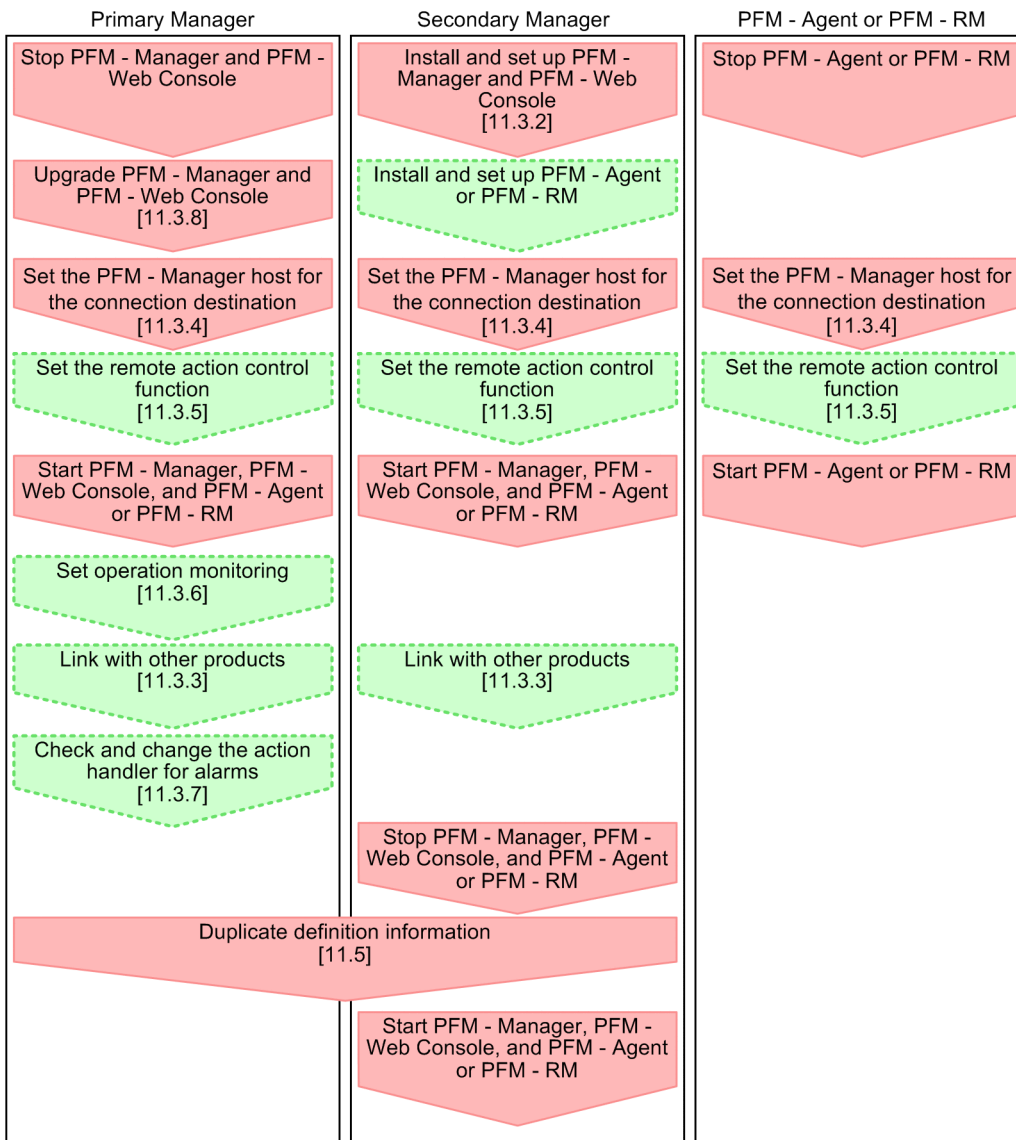
Figure 11–4: Setup procedure when the primary Manager and the secondary Manager are newly installed




Legend:

- ▾ : Required setup items
- ▾ : Optional setup items
- [ ] : Reference

Figure 11–5: Setup procedure when an existing environment is set as the primary Manager, and the secondary Manager is newly installed



Legend:

 : Required setup items

 : Optional setup items

[ ] : Reference

## 11.3.2 Installing and setting up programs

### (1) Installation and setup

Install and set up PFM - Manager and PFM - Web Console. Install and set up the programs in the same way as you would when not configuring multiple monitoring. For details, see the chapter that describes installation and setup (for Windows) or installation and setup (for UNIX) in the *JPI/Performance Management Planning and Configuration Guide*.

## (2) Settings that must be done before duplicating definition information

You must set the following items before you can duplicate definition information. Set the following information on both the primary Manager host and the secondary Manager host.

- The following information in [Table 11-2 Definition information for which the same setting must be specified on the primary Manager and the secondary Manager](#)
  - Host information configuration file (`jpchosts`)
  - Setting of Authentication mode
  - Health check function
  - Status management function
  - Product name display function
  - IPv6 communication
  - Encrypted communication
- The information in [Table 11-3 Definition information that must be matched in `jpccomm.ini`](#)

### Important

Match the settings between the primary Manager and the secondary Manager.

## 11.3.3 Link with other systems in a multiple-monitoring environment

When linking with other JP1 products in a multiple-monitoring environment, you must specify the same settings on the primary Manager and the secondary Manager.

The following describes settings for each linkage product.

### (1) When linking with JP1/IM

The settings when linking with JP1/IM are the same as those when multiple monitoring is not configured. For details, see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

### Important

- When two PFM - Manager services are linked to one JP1/IM service, reports might not be displayable from JP1/IM. For details, see [17.3.7 A connection from the time the JP1/IM's Event Console starts monitoring to PFM - Web Console cannot be established](#).
- When a Performance Management report for the host (on which the problem occurred) is displayed from an event in the integrated console, a connection with PFM - Web Console specified in the performance report definition file (`performance.conf`) is established. This connection is required irrespective of whether the monitoring manager is primary or secondary. The report is not displayed if a connection with the specified PFM - Web Console cannot be established. In this case, edit the PFM - Web Console settings in the performance report definition file so that a connection can be established correctly. For details about how to specify settings in the performance report definition file, see [12.3.3 Setup for linking with JP1/IM \(settings for displaying reports from events in the integrated console\)](#).

## (2) When linking with JP1/SLM

The settings when linking with JP1/SLM are the same as those when multiple monitoring is not configured. For details, see [13. Performance Monitoring Linked with JP1/Service Level Management \(JP1/SLM\)](#).

### ! Important

Only one PFM - Manager service can be linked per JP1/SLM service. Even if the primary Manager goes down, service monitoring in JP1/SLM can continue because performance information continues to be sent from PFM - Agent and PFM - RM. However, you cannot perform operations for Performance Management such as starting or stopping of monitoring from JP1/SLM. Therefore, when the primary Manager goes down, you must change the connection target to the secondary Manager.

## (3) When linking with JP1/AJS3

The settings when linking with JP1/AJS3 are the same as those when multiple monitoring is not configured. For details, see [14. Monitoring Linked with JP1/AJS3](#).

### ! Important

When Performance Management reports are directly displayed from JP1/AJS3, a connection with PFM - Web Console specified in the JP1/AJS3 - Web Console environment-settings file (`ajs3web.conf`) is established irrespective of whether the monitoring manager is primary or secondary. The reports are not displayed if a connection with the specified PFM - Web Console cannot be established.

To avoid such problems in a multiple-monitoring environment, set up individual instances of JP1/AJS3 - Web Console on both the primary PFM - Web Console and the secondary PFM - Web Console.

## 11.3.4 Setting PFM - Manager for the connection destination for multiple monitoring

To configure multiple monitoring, you must set PFM - Manager for the connection destination. Set PFM - Manager for the connection destination of the PFM - Manager host of the primary Manager, and the PFM - Manager, PFM - Agent, and PFM - RM hosts of the secondary Manager.

Also, if you change the monitoring host name or physical host name of PFM - Manager on one Manager, you must reconfigure PFM - Manager for the connection destination on PFM - Manager, PFM - Agent, and PFM - RM on the other Manager.

PFM - Manager for the connection destination can be set by using the `jpccconf mgrhost define` command as follows. The host names to be specified for the `-host` argument differ depending on the program that executes the command.

```
jpccconf mgrhost define -host host-name-A, host-name-B [-lhost logical-host-name] [-noquery]
```

The following table shows the specifications for *host-name-A* and *host-name-B*.



Table 11–5: Specifications for host-name-A and host-name-B

Program executing the command	Host name to be specified for host-name-A	Host name to be specified for host-name-B
PFM - Manager on the primary Manager	localhost	PFM - Manager host name on the secondary Manager
PFM - Manager on the secondary Manager	PFM - Manager host name on the primary Manager	localhost
PFM - Agent and PFM - RM	PFM - Manager host name on the primary Manager	PFM - Manager host name on the secondary Manager

For details about setting up PFM - Agent and PFM - RM, see the chapter that describes the procedure for changing PFM - Manager for the connection destination in the *JP1/Performance Management Planning and Configuration Guide*.

For details about the `jpccconfmgrhost define` command, see the chapter that describes commands in the manual *JP1/Performance Management Reference*.

### 11.3.5 Controlling remote actions

In a multiple-monitoring configuration, an agent sends events to PFM - Manager on both the primary Manager and the secondary Manager. Events are sent to PFM - Manager on the primary Manager first, and on the secondary Manager next. However, in a case such as when a remote action does not need to be executed twice for a single event, you can set the execution mode to control the execution of remote actions. For details about remote actions, see [6.3.2 Configuring the host to automatically execute commands](#).

To set the execution mode for remote actions, specify the value of the Remote Action Control label by directly editing the `jpccomm.ini` file on the PFM - Agent or PFM - RM host on which alarms are issued. Set the same value for the execution mode on all the hosts.

The following table describes the execution mode for remote actions and shows the specification value.

Table 11–6: Execution mode for remote actions

Execution mode	Value to be specified for the Remote Action Control label	Description
All execution modes	all	Executes both remote actions for events that are sent to the primary and secondary systems.
One-side execution mode	one	Executes only the remote action for the event for which sending succeeds first of events that are sent to the primary and secondary systems.
Primary execution mode	primary	Executes only the remote action for an event that is sent to the primary system.

The `jpccomm.ini` file is stored in the following location.

In Windows:

*installation-folder*\

In UNIX:

`/opt/jp1pc/`

To set the execution mode for remote actions:

1. Stop the Performance Management programs and services.  
Use the `jpcspm stop` command to stop any of the Performance Management programs and services that are running.
2. Open `jpccomm.ini` with a text editor.
3. Set the execution mode for controlling remote actions.  
Change the following label value in the `Common Section` section in the `jpccomm.ini` file.  

```
Remote Action Control=xxx#
```

  
#  
Specify `all`, `one`, or `primary` for `xxx`.
4. Save and close `jpccomm.ini`.
5. Use the `jpcspm start` command to start the Performance Management programs and services.
6. Restart PFM - Web Console.

### 11.3.6 Setting operation monitoring

You must set the following items before you can duplicate definition information. Set the following information on both the primary Manager host and the secondary Manager host.

- The following information in [Table 11-2 Definition information for which the same setting must be specified on the primary Manager and the secondary Manager](#)
  - Settings of the health check agent
  - Settings related to JP1 events



#### Important

Match the settings between the primary Manager and the secondary Manager.

Set anything required for operation monitoring at the same time.

### (1) Additional settings to be specified when you are using the auto alarm bind function

When you are using the auto alarm bind function, specify the following settings:

#### (a) Enabling the products

On the PFM - Manager host, execute the following command to confirm if the pre-registration of alarms or reports is enabled for the agents to which you want to apply the auto alarm bind function:

```
jpccconf agent list
```

If the pre-registration of alarms or reports is not enabled for the agents, enable it by executing the following command:

```
jpccconf agent setup -key service-key -register
```

### Note

If you execute the command with the service key of agents specified by mistake, you can use the following command to restore the setting back to its previous state:

```
jpccconf agent setup -key service-key -unregister
```

## (b) Specifying the auto alarm bind setting

You can specify the auto alarm bind setting as follows:

When using PFM - Web Console

Specify the auto alarm bind setting from the Automatic Bind Settings window. For details, see the section describing the Auto Alarm Bind Setting window in the manual *JP1/Performance Management Reference*.

When using PFM - Manager

Directly edit the auto alarm bind setting file. For details, see the section describing the auto alarm bind setting file (`jpcautobind.cfg`) in the manual *JP1/Performance Management Reference*.

### Important

- With PFM -Web Console, you only need to specify the auto alarm bind setting on the primary manager (no need to specify the same setting on the secondary manager).
- If you change the auto alarm bind setting after configuring a multiple monitoring environment, you have to duplicate definition information again to ensure synchronization. For details, see [11.5 Duplicating definition information](#). For details about how to confirm synchronization, see [11.6.1\(8\) Checking the settings of auto alarm bind](#).

## 11.3.7 Checking and changing the action handler for alarms

If Action Handler on the PFM - Manager host is specified as the action handler in the alarm definition, we recommend that you change it to *Manager*. Changing to *Manager* allows the Action Handler service in PFM - Manager which receives events to execute remote actions even if the definition information is duplicated.

In addition, when you specify the action handler of the agent to which the alarm table is bound, we recommend that you set the action handler to *LOCAL*.

You can check the action handler in the alarm properties. For details, see [6.6.6 Displaying alarm properties \(definitions\)](#).

The action handler settings can be edited by using the `jpctool alarm` command in the monitoring console or PFM - Manager on the primary Manager. For details about how to edit the alarm definition from the monitoring console, see [6.4 Setting alarms using the Web browser \(Alarms tree\)](#). Also, for details about how to edit the alarm definition by using commands, see [6.7 Setting alarms by using commands](#).

### 11.3.8 Upgrading PFM - Manager and PFM - Web Console

Upgrade PFM - Manager and PFM - Web Console. The upgrade procedure is the same as that when multiple monitoring is not configured. For details, see the chapter that describes the procedure for upgrading the Performance Management programs in the *JP1/Performance Management Planning and Configuration Guide*.

 **Important**

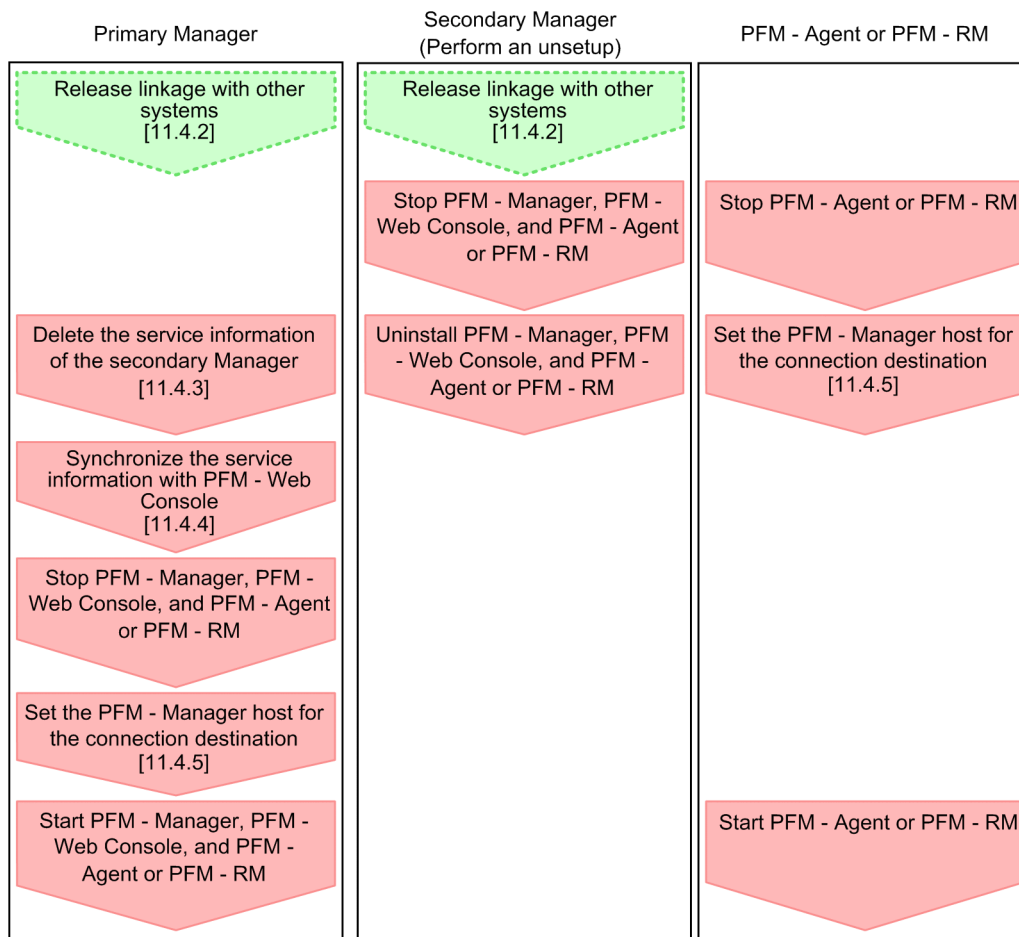
The primary Manager and the secondary Manager must use the same version of PFM - Manager and PFM - Web Console. When you upgrade these programs, make sure that the version is the same for the primary Manager and the secondary Manager.

## 11.4 Unsetting up multiple monitoring

### 11.4.1 Procedure of unsetting up multiple monitoring

The following figures show procedures for terminating multiple-monitoring functionality in two different cases.

Figure 11–6: Procedure for terminating multiple monitoring when uninstalling the secondary Manager



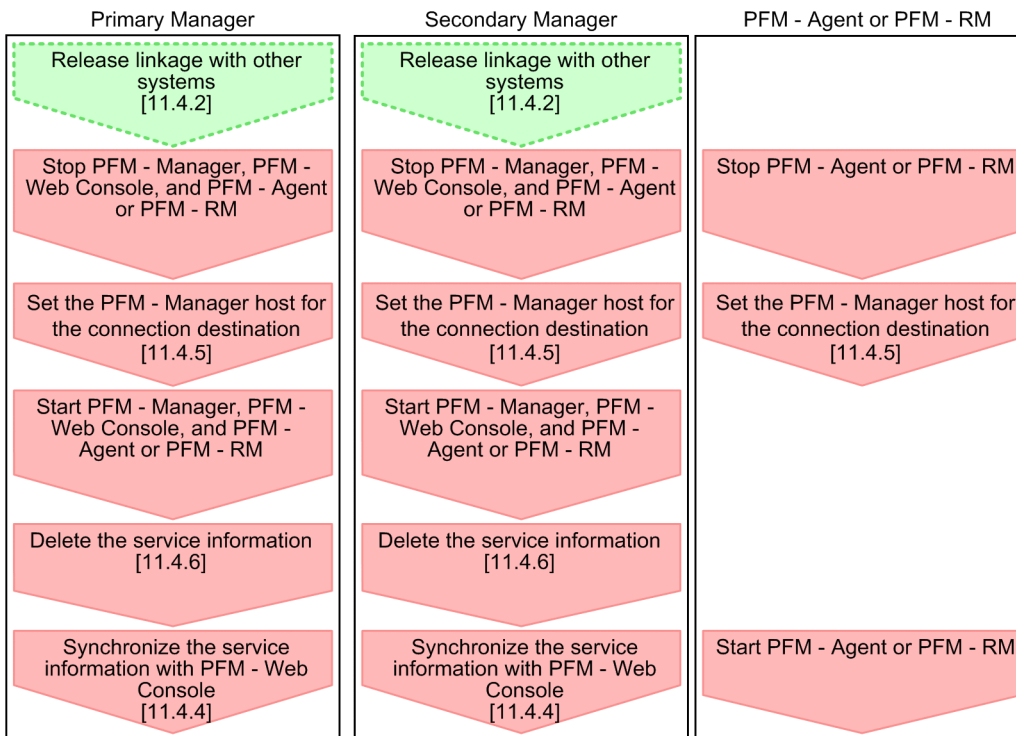
Legend:



  : Required setup items

  : Optional setup items

[ ] : Reference

Figure 11–7: Procedure for terminating multiple monitoring when the primary Manager and the secondary Manager will be used separately



Legend:  
 : Required setup items  
 : Optional setup items  
 [ ] : Reference

## 11.4.2 Releasing links with other systems in a multiple-monitoring environment

When releasing links with other JP1 products in a multiple-monitoring environment, you must release the links on both the primary Manager and the secondary Manager.

The following describes settings for each linkage product.

### (1) Releasing links with JP1/IM

The settings to change when releasing links to JP1/IM are the same as those when multiple monitoring is not configured. For details, see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

### (2) Releasing links with JP1/SLM

The settings to change when releasing links to JP1/SLM are the same as those when multiple monitoring is not configured. For details, see [13. Performance Monitoring Linked with JP1/Service Level Management \(JP1/SLM\)](#).

### 11.4.3 Deleting the services of the secondary Manager

Delete the service information of the secondary Manager from PFM - Manager on the primary Manager.

The following is an example of executing the command:

```
jpctool service delete -id * -host PFM - Manager-host on-the-secondary-Manager
```

### 11.4.4 Synchronizing service information with PFM - Web Console

To apply deletion of the service information to PFM - Web Console, synchronize the service information of PFM - Manager with that of PFM - Web Console. To synchronize the service information, use the `jpctool service sync` command.

### 11.4.5 Reconfiguring PFM - Manager for connection destination to release multiple monitoring

To terminate multiple monitoring, you must reconfigure PFM - Manager for the connection destination. Reconfigure PFM - Manager for the connection destination of the PFM - Manager host of the primary Manager, and the PFM - Manager, PFM - Agent, and PFM - RM hosts of the secondary Manager.

#### (1) Setting of PFM - Manager

Set `localhost` as the only PFM - Manager for the connection destination in PFM - Manager on the primary Manager and the secondary manager.

The following is an example of executing the command:

```
jpccconf mgrhost define -localhost
```

#### (2) Setting of PFM - Agent and PFM - RM

Set only one host as PFM - Manager for the connection destination in PFM - Agent and PFM - RM.

The following is an example of executing the command:

```
jpccconf mgrhost define -host host-name
```

### 11.4.6 Deleting service information

Because the configuration changes when you terminate multiple monitoring, delete the service information registered in PFM - Manager.

The following is an example of executing the command:

```
jpctool service delete -id * -host agent-host-name
```

For details, see the description of how to delete Performance Management service information in the *JPI/Performance Management Planning and Configuration Guide*.

## 11.5 Duplicating definition information

---

To duplicate definition information, export the definition information to be duplicated from the primary Manager and import it into the secondary Manager.

The following describes the prerequisites for exporting and importing definition information. If an error message is output to the standard error output and common message log, see the message contents and correct the error.

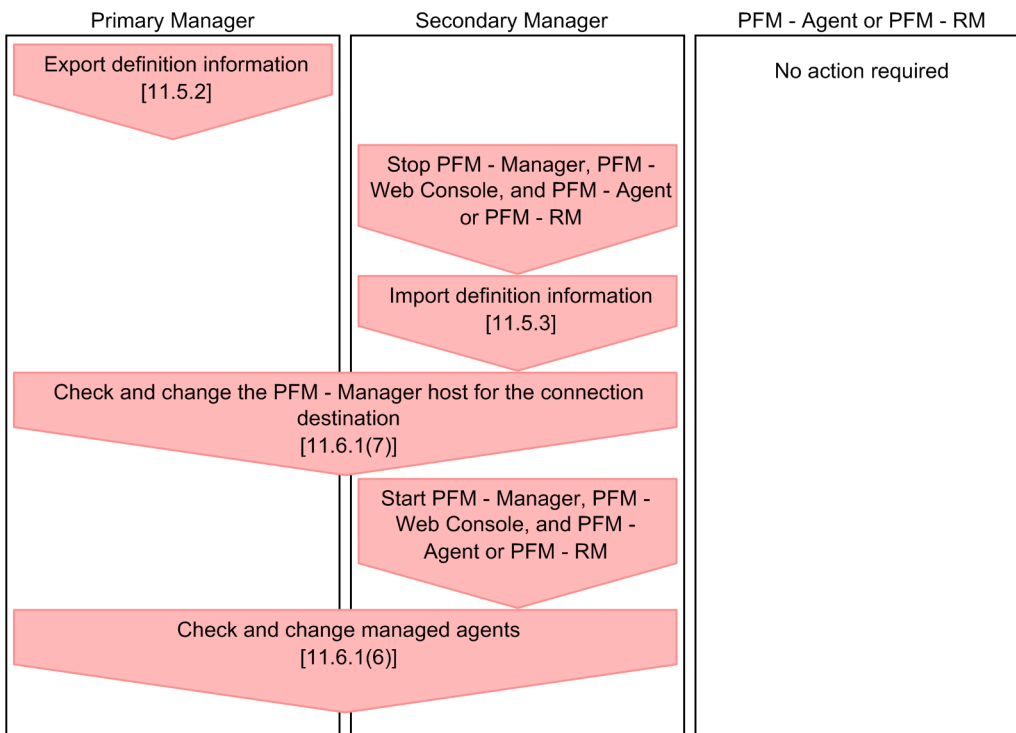
- Prerequisites common to exporting and importing  
Two host names are set for PFM - Manager for the connection destination.
- Prerequisites for importing
  - The system configuration at the time of import is completely the same as that at the time of export.
  - The version of PFM - Manager of the host from which the definition information is exported must match that of the host to which the definition information is imported.
  - The version of PFM - Web Console of the host from which the definition information is exported must match that of the host to which the definition information is imported.
  - All the PFM services in the host to which the definition information is imported must be stopped.
  - The definition information shown in [Table 11-2 Definition information for which the same setting must be specified on the primary Manager and the secondary Manager](#) of the host from which the definition information is exported must match that of the host to which the definition information is imported.
  - The setting values (the values specified in the `Monitoring Level` property in the `Health Check Configurations` folder of health check agents) for the monitoring level of the health check function on the host from which the definition information is exported, must match that on the host to which the definition information is imported.

### 11.5.1 Procedure for duplicating definition information


The following figure shows the procedure for duplicating definition information.



Figure 11–8: Procedure for duplicating definition information



Legend:

 : Required setup items

[ ] : Reference

## 11.5.2 Exporting definition information

This subsection describes the procedure for exporting definition information of PFM - Manager and PFM - Web Console.

### (1) Exporting the definition information of PFM - Manager

To execute the `jpctool config mgrexpport` command to export the definition information of PFM - Manager:

1. Log on to the host on which PFM - Manager has been installed.
2. Use the `jpctool alarm unapplied` command or the Alarm Application Status window to check the alarm application status.  
Verify that the alarm application status is `Successful` or `Inactive`. If the status is neither `Successful` nor `Inactive`, take the appropriate corrective action according to the application status until the status becomes `Successful`. For details about how to check the application status and take the appropriate corrective action, see the descriptions about the `jpctool alarm unapplied` and `jpctool config alarmsync` commands in the manual *JP1/Performance Management Reference* or see [6.6.5 Checking alarm application status](#).
3. Execute the `jpctool config mgrexpport` command to export the definition information of PFM - Manager.

For example, to export the definition information of PFM - Manager to the `/tmp/pfmexport` directory, execute the command as follows:

```
jpctool config mgrexpport -d /tmp/pfmexport
```

For details about the `jpctool config mgrexpport` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

## (2) Exporting the definition information of PFM - Web Console

Execute the `jpgcwebbackup` command to create a backup file for the definition information of PFM - Web Console. Use a part of the created backup file as the export data.

The following are the definition information files of PFM - Web Console that need to be exported.

- Bookmark definition information

The bookmark definition information is stored in the following location on the PFM - Web Console host by default.

- In Windows  
`installation-folder\bookmarks\`
- In UNIX  
`/opt/jp1pcwebcon/bookmarks/`

- Definition information of the process monitoring definition template

The definition information of the process monitoring definition template is stored in the following location on the PFM - Web Console host by default.

- In Windows  
`installation-folder\processMonitoringTemplates\`
- In UNIX  
`/opt/jp1pcwebcon/processMonitoringTemplates/`

To export the definition information of PFM - Web Console:

1. Log on to the host on which PFM - Web Console has been installed.
2. Move to the command execution path.

- In Windows  
`installation-folder\tools`
- In UNIX  
`/opt/jp1pcwebcon/tools`

3. Execute the `jpgcwebbackup` command to back up the definition information.

The following are notes on executing the command:

- Do not specify a network drive for the backup destination.
- Do not change the definition information and system configuration while backup is in process.
- Do not perform any change operations that can be performed only by administrator users.

For example, when you back up the definition information to the `c:\backup` directory, execute the command as follows:

```
jpgcwebbackup -d c:\backup
```

For details about the `jpgcwebbackup` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

## 11.5.3 Importing definition information

This subsection describes the procedure for importing definition information of PFM - Manager and PFM - Web Console.

### (1) Importing the definition information of PFM - Manager

Import the definition information file of PFM - Manager exported by using the `jpctool config mgrexport` command.

To execute the `jpctool config mgrimport` command to import the definition information file of PFM - Manager:

1. Copy the definition information file.

Copy the definition information file of PFM - Manager exported by using the `jpctool config mgrexport` command.

2. Log on to the host on which the import-destination PFM - Manager has been installed.

3. Execute the `jpctool config mgrimport` command to import the definition information of PFM - Manager.

For example, when you import the definition information of PFM - Manager copied in step 1 that is stored in the `/tmp/pfmimport` directory, execute the command as follows:

```
jpctool config mgrimport -d /tmp/pfmimport
```

For details about the `jpctool config mgrimport` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

### (2) Importing the definition information of PFM - Web Console

You must manually import (copy) the definition information of PFM - Web Console. Host names are needed for copying the data. So, you will need to confirm the names of the source and destination hosts beforehand. The following describes how to check the host names.

The following is the procedure for copying the definition information of PFM - Web Console. In this procedure, the storage location of the copied data is assumed to be `C:\backup`.

- Name of the host which the data is to be copied from

Check the `host` value in the initialization file (`C:\backup\jplpcwcbbackup\jplpcWebCon\conf\config.xml`).

- Name of the host which the data is to be copied to

Check the `host` value in the initialization file (`config.xml`) on the import destination.

1. Log on to the PFM - Web Console host to which you want to copy the data.

2. Execute the `jpcwstop` command to stop the PFM - Web Console services on the host.

For details about the `jpcwstop` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

3. Delete or save data on the host to which you want to copy the data.

When you copy the bookmark definition information and process monitoring definition template definition information, you need to empty the following copy-destination directory. Delete or move any existing data.

- Bookmark definition information

Directory specified for `bookmarkRepository` in the initialization file (`config.xml`) on the copy-destination host.

- Process monitoring definition template definition information

Directory specified for `processMonitoringTemplatesRepository` in the initialization file (`config.xml`).

### Important

- If you have never started up PFM - Web Console on the copy-destination host, you need to create the directories.
- If the above setting values are commented out or blank, the default storage directories will be used as the copy-destinations.

For details about the default storage directories, see [11.5.2\(2\) Exporting the definition information of PFM - Web Console](#).

#### 4. Copy the bookmark definition information.

Check the `bookmarkRepository` value in the initialization file (`config.xml`) on the copy-destination host and perform the following operation according to the setting value.

- When the setting value is commented out or blank

Copy the file as follows: `C:\backup\jplpcwcbbackup\bookmarks\host-name-(copy-source)` to `installation-folder\bookmarks\host-name-(copy-destination)`.

- When the setting value exists

Copy the file as follows: `C:\backup\jplpcwcbbackup\bookmarks\host-name-(copy-source)` to `directory-specified-for-bookmarkRepository\host-name-(copy-destination)`.

#### 5. Copy the process monitoring definition template definition information.

Check the `processMonitoringTemplatesRepository` value in the initialization file (`config.xml`) on the copy-destination host and perform the following operation according to the setting value.

- When the setting value is commented out or blank

Copy the file as follows: `C:\backup\jplpcwcbbackup\processMonitoringTemplates` to `installation-folder\processMonitoringTemplates`.

- When the setting value exists

Copy the file as follows: `C:\backup\jplpcwcbbackup\processMonitoringTemplates` to `directory-specified-for-processMonitoringTemplatesRepository`.

#### 6. Execute the `jpcwstart` command to start the PFM - Web Console services on the host.

## 11.6 Checking duplication of definition information and operation monitoring data

---

If definition information is inconsistent between the primary Manager and the secondary Manager, the system cannot be operated in a multiple-monitoring configuration. For details about definition information that must be consistent and the procedure for matching definition information, see [11.1.3 Definition information for multiple monitoring](#).

### 11.6.1 Checking duplication of the PFM - Manager definition information

Use the following procedure to check whether the PFM - Manager definition information is duplicated and consistent between the primary Manager and the secondary Manager.

#### (1) Checking alarm information of alarm definition and action definition

1. Start the PFM - Manager service on the primary Manager if it has stopped.
2. Execute the following command in PFM - Manager on the primary Manager.

```
jpctool alarm export -f output-file-name -key service-key
```

3. Start the PFM - Manager service on the secondary Manager if it has stopped.
4. Execute the following command in PFM - Manager on the secondary Manager.

```
jpctool alarm export -f output-file-name -key service-key
```

5. Compare the output files of the primary Manager and the secondary Manager.  
If the output files match, the alarm information matches.

#### (2) Checking binding information

1. Start the PFM - Manager service on the primary Manager if it has stopped
2. Execute the following command in PFM - Manager on the primary Manager.

```
jpctool alarm list -key service-key -table alarm-table-name
```

3. Start the PFM - Manager service on the secondary Manager if it has stopped.
4. Execute the following command in PFM - Manager on the secondary Manager.

```
jpctool alarm list -key service-key -table alarm-table-name
```

5. Compare the display results of the primary Manager and the secondary Manager.  
If the display results match, the binding information matches.

#### (3) Checking report definitions

1. Start the PFM - Manager service and the PFM - Web Console service on the primary Manager if they have stopped.

2. Execute the following command in PFM - Web Console on the primary Manager.

Specify the input file so that all reports are output.

```
jpcrdef output -o output-file-name input-file-name
```

3. Execute the following command in PFM - Web Console on the secondary Manager.

Specify the input file so that all reports are output.

```
jpcrdef output -o output-file-name input-file-name
```

4. Compare the output files of the primary Manager and the secondary Manager.

If the output files match, the report definitions match.

## (4) Checking business group information

1. Start the PFM - Manager service on the primary Manager if it has stopped.

2. Execute the following command in PFM - Manager on the primary Manager to display the list of business group names.

```
jpccconf bgdef list
```

3. Check the result of step 2 and execute the following command in PFM - Manager on the primary Manager.

```
jpccconf bgdef export -f output-file-name -group business-group-name
```

4. Start the PFM - Manager service on the secondary Manager if it has stopped.

5. Execute the following command in PFM - Manager on the secondary Manager to display the list of business group names.

```
jpccconf bgdef list
```

6. Check the result of step 5 and execute the following command in PFM - Manager on the secondary Manager.

```
jpccconf bgdef export -f output-file-name -group business-group-name
```

7. Compare the output files of the primary Manager and the secondary Manager.

If the output files match, the business group information matches.

## (5) Checking Performance Management user account information and Agents tree (User Agents) information

1. Compare files that are collected from the primary Manager and the secondary Manager.

The collected files are in binary format. Compare these files. If they match, the Performance Management user account information and the User Agents information are consistent. Use a command, such as FC (Windows) or diff (UNIX), to compare the binary files.

The Performance Management user account information and the User Agents information are managed in the same file. The following table shows the file path.

Table 11–7: Path of files to be compared

Data	Authentication mode	Path
Performance Management user account information, Agents tree (User Agents) information	PFM authentication	In Windows: <i>installation-folder</i> \mgr\viewsvr\data\UserList.lmk In UNIX: /opt/jplpc/mgr\viewsvr/data/UserList.lmk
	JP1 authentication	In Windows: <i>installation-folder</i> \mgr\viewsvr\data\UserListforJP1.lmk In UNIX: /opt/jplpc/mgr\viewsvr/data/UserListforJP1.lmk

## (6) Checking managed agent information

1. Start the PFM - Manager service on the primary Manager if it has stopped.
2. Execute the following command in PFM - Manager on the primary Manager.

```
jpctool service list -id * -host *
```

3. Start the PFM - Manager service on the secondary Manager if it has stopped.
4. Execute the following command in PFM - Manager on the secondary Manager.

```
jpctool service list -id * -host *
```

5. Compare the display results of the primary Manager and the secondary Manager.  
If the service IDs other than Status Server, Trap Generator, and View Server match, the managed agent information matches.

## (7) Checking the settings of PFM - Manager for the connection destination

1. Execute the following command in PFM - Manager on the primary Manager.

```
jpccconf mgrhost display
```

2. Execute the following command in PFM - Manager on the secondary Manager.

```
jpccconf mgrhost display
```

3. Compare the display results of the primary Manager and the secondary Manager.  
If the display results match, the settings of PFM - Manager for the connection destination match between the primary Manager and the secondary Manager.

## (8) Checking the settings of auto alarm bind

1. Compare files as binary that are collected from the primary Manager and the secondary Manager.  
The following files are collected:

In Windows:  
*installation-directory*\jpcautobind.cfg

In UNIX:

```
/opt/jp1pc/jpcautobind.cfg
```

Compare these files. If they match, the settings of auto alarm bind are consistent. Use a command, such as `FC` (Windows) or `diff` (UNIX), to compare the binary files.

## 11.6.2 Checking duplication of the PFM - Web Console definition information

Use the following procedure to check whether the PFM - Web Console definition information is duplicated and consistent between the primary Manager and the secondary Manager.

### (1) Checking bookmark definition information

1. Check the `bookmarkRepository` value in the initialization file (`config.xml`) on the PFM - Web Console host on the primary Manager.

Perform step 2 according to the `bookmarkRepository` value.

2. Copy the following bookmark definition information to the proper folder as follows:

- When the `bookmarkRepository` value is commented out or blank  
*installation-folder\bookmarks\PFM-manager-host-name-on-the-primary-Manager*
- When the `bookmarkRepository` value exists  
*bookmarkRepository-value\host-name-of-the-connection-target-PFM-Manager*

3. Check the `bookmarkRepository` value in the initialization file (`config.xml`) on the PFM - Web Console host on the secondary Manager.

Perform step 4 according to the `bookmarkRepository` value.

4. Copy the following bookmark definition information to the proper folder as follows:

- When the `bookmarkRepository` value is commented out or blank  
*installation-folder\bookmarks\PFM-manager-host-name-on-the-secondary-Manager*
- When the `bookmarkRepository` value exists  
*bookmarkRepository-value\host-name-of-the-connection-target-PFM-Manager*

5. Compare the bookmark definition information files that were collected from the primary Manager and the secondary Manager on a folder-by-folder basis.

Collected files are in binary format. If you compare these files on a folder-by-folder basis and make sure that all the files match, the bookmark definition information is consistent.

### (2) Checking process monitoring template information

1. Check the `processMonitoringTemplatesRepository` value in the initialization file (`config.xml`) on the PFM - Web Console host on the primary Manager.

Perform step 2 according to the `processMonitoringTemplatesRepository` value.

2. Copy the following process monitoring template information to the proper folder as follows:

- When the `processMonitoringTemplatesRepository` value is commented out or blank



*installation-folder\processMonitoringTemplates*

- When the `processMonitoringTemplatesRepository` value exists  
*processMonitoringTemplatesRepository-value*

3. Check the `processMonitoringTemplatesRepository` value in the initialization file (`config.xml`) on the PFM - Web Console host on the secondary Manager.

Perform step 4 according to the `processMonitoringTemplatesRepository` value.

4. Copy the following process monitoring template information to the proper folder as follows:

- When the `processMonitoringTemplatesRepository` value is commented out or blank  
*installation-folder\processMonitoringTemplates*
- When the `processMonitoringTemplatesRepository` value exists  
*processMonitoringTemplatesRepository-value*

5. Compare the process monitoring template information files that were collected from the primary Manager and the secondary Manager on a folder-by-folder basis.

Collected files are in binary format. If you compare these files on a folder-by-folder basis and make sure that all the files match, the process monitoring template information is consistent.

### 11.6.3 Checking the settings of PFM - Manager to which the monitoring agent connects

You can separately check the host names of the primary Manager and the secondary Manager that are set on a host on which PFM - Agent or PFM - RM is running.

#### (1) Checking from PFM -Web Console

You can display the properties of the `Multiple Manager Configuration` node in the Service Properties window of PFM - Web Console. Use the displayed properties to check PFM - Manager for the connection destination host name of the primary Manager and the secondary Manager.

Display the properties of the following services from PFM - Web Console:

- The Collector service and Store service of PFM - Agent or PFM - RM
- The Collector service and Store service of the health check agent
- The Action Handler service

For details, see the description of the Service Properties window in the manual *JPI/Performance Management Reference*.

#### (2) Checking by using a command

You can check the host name of the primary Manager and the secondary Manager that is set for each agent by using a command. For details, see the description of the `jpccnf mgrhost display` command in the manual *JPI/Performance Management Reference*.

## 11.6.4 Checking whether operation monitoring data matches

### (1) Checking performance data (health check agent)

1. Start the PFM - Manager service and the PFM - Web Console service on the primary Manager if they have stopped.
2. Access PFM - Web Console on the primary Manager from a browser.
3. Open the Agents window and display the historical report of a record which you want to check for consistency.
4. Click **Export** in the **View report** page, and then save the CSV file.
5. Access PFM - Web Console on the secondary Manager from a browser.
6. Perform steps 3 and 4.
7. Compare the CSV files collected from the primary Manager and the secondary Manager.  
If the files match, performance data matches.

### (2) Checking event data

1. Start the PFM - Manager service and the PFM - Web Console service on the primary Manager if they have stopped.
2. Access PFM - Web Console on the primary Manager from a browser.
3. Open the Agents window and change **Display format** to **Products**.
4. Click **Event History** while the root directory is being selected.  
**Settings for the report display period** opens.
5. Set period for which you want to compare event data and the condition expression, and click the **OK** button.
6. Click **Export** in the **View report** page, and then save the CSV file.
7. Access PFM - Web Console on the secondary Manager from a browser.
8. Perform steps 3 and 6.
9. Compare the CSV files collected from the primary Manager and the secondary Manager.  
If the files match, event data matches.

## 11.7 Switching the primary Manager and the secondary Manager

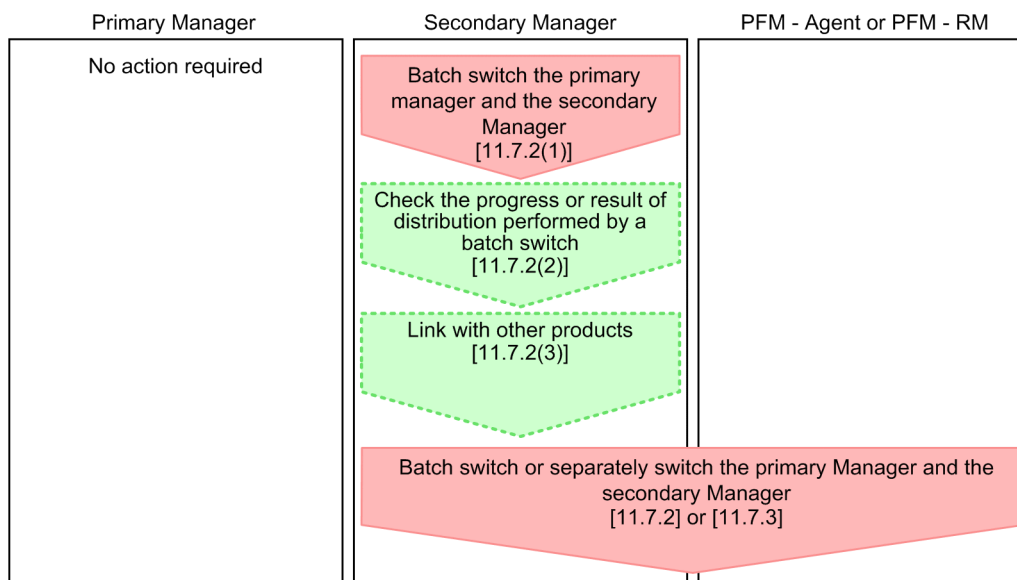
This section describes the procedure for switching the primary Manager and the secondary Manager. You need to switch the primary Manager and the secondary Manager in various cases such as when you need to maintain or replace a machine, you need to stop the primary Manager, or an error occurs on the primary Manager and it goes down. For details about the procedure for switching when an error occurs, see [17.3.2 The host name is not distributed to agents when the `jpccconf primmgr notify` command is executed](#) and [17.3.3 The host name is not distributed to the primary Manager when the `jpccconf primmgr notify` command is executed](#).

When an error occurs, operation monitoring data might be inconsistent between the primary Manager and the secondary Manager. For details about how to check whether the data is consistent, see [11.6.4 Checking whether operation monitoring data matches](#).


### 11.7.1 Procedure for switching the primary Manager and the secondary Manager


The following figure shows the procedure for switching the primary Manager and the secondary Manager.

Figure 11–9: Procedure for switching the primary Manager and the secondary Manager



Legend:

 : Required setup items

 : Optional setup items

[ ] : Reference

Confirm that the primary Manager and the secondary Manager were switched by checking the progress of distribution or the distribution result of the primary Manager. For details about actions when a switch fails, see [17.3.2 The host name is not distributed to agents when the `jpccconf primmgr notify` command is executed](#) and [17.3.3 The host name is not distributed to the primary Manager when the `jpccconf primmgr notify` command is executed](#).

## 11.7.2 Batch switching the primary Manager and the secondary Manager

To switch the primary Manager and the secondary Manager, execute the `jpccconf primmgr notify` command in PFM - Manager on the secondary Manager.

### (1) Procedure for batch switching the primary Manager and the secondary Manager

1. In PFM - Manager on the secondary Manager, execute the `jpccconf primmgr notify` command.

The PFM - Manager that executed the command is set as the primary Manager. The host name that is newly set as the primary Manager is distributed as a batch to all the hosts in the PFM system on which the Status Server service is running.

The host name is not distributed to hosts on which the Status Server service is stopped. When the PFM - Manager service on the primary Manager stops for some reasons such as that the host going down, distribution to PFM - Manager on the primary Manager will fail. For details about actions when a distribution fails, see [17.3.2 The host name is not distributed to agents when the `jpccconf primmgr notify` command is executed](#) and [17.3.3 The host name is not distributed to the primary Manager when the `jpccconf primmgr notify` command is executed](#).

For details, see the description of the `jpccconf primmgr notify` command in the manual *JPI/Performance Management Reference*.

2. Output the setting result of the primary Manager to a file.

After execution of the `jpccconf primmgr notify` command and distribution to all hosts have completed, the result is output to a file in CSV format. For details, see the description of the `jpccconf primmgr notify` command in the manual *JPI/Performance Management Reference*.

### (2) Checking the progress or result of distribution performed by a batch switch

Check whether the host switch and batch distribution of the host name have succeeded. Perform the switch operation again as necessary.

#### (a) Checking the progress of distribution

You can check the progress of distribution by using the `jpccconf primmgr notify` command. For details, see the description of the `jpccconf primmgr notify` command in the manual *JPI/Performance Management Reference*.

#### (b) Checking the result of distribution

You can check the result of distribution by checking the CSV file output by the `jpccconf primmgr notify` command. If a distribution fails, you will need to perform a batch switch or separate switch again. For details, see [17.3.2 The host name is not distributed to agents when the `jpccconf primmgr notify` command is executed](#) and [17.3.3 The host name is not distributed to the primary Manager when the `jpccconf primmgr notify` command is executed](#).

### (3) Setting linkage with other products

When the system is linked to other JP1 products in a multiple-monitoring environment before the manager is switched, you will need to reset linkage with those products after the switch has completed. For details about the settings of linkage products required for multiple monitoring, see [11.3.3 Link with other systems in a multiple-monitoring environment](#).

### 11.7.3 Switching the primary Manager and the secondary Manager separately

Separately switch the primary Manager and the secondary Manager on hosts on which PFM - Agent or PFM - RM is running.

#### (1) Procedure for switching the primary Manager and the secondary Manager separately

You can execute the `jpccconf mgrhost define` command on a host on which PFM - Agent or PFM - RM is running to switch the primary Manager that is set as PFM - Manager for the connection destination with the secondary Manager

Use the message displayed after the `jpccconf mgrhost define` command is executed to check the result of executing the command. For details about the `jpccconf mgrhost define` command, see the description of the `jpccconf mgrhost define` command in the manual *JP1/Performance Management Reference*.

# 12

## Linking with the Integrated Management Product JP1/IM for Operation Monitoring

This chapter describes operation monitoring by linking Performance Management with the integrated management product JP1/IM. The chapter covers the setup procedure for linking Performance Management with JP1/IM, and how to perform operation monitoring of the target system by using Performance Management from JP1/IM.

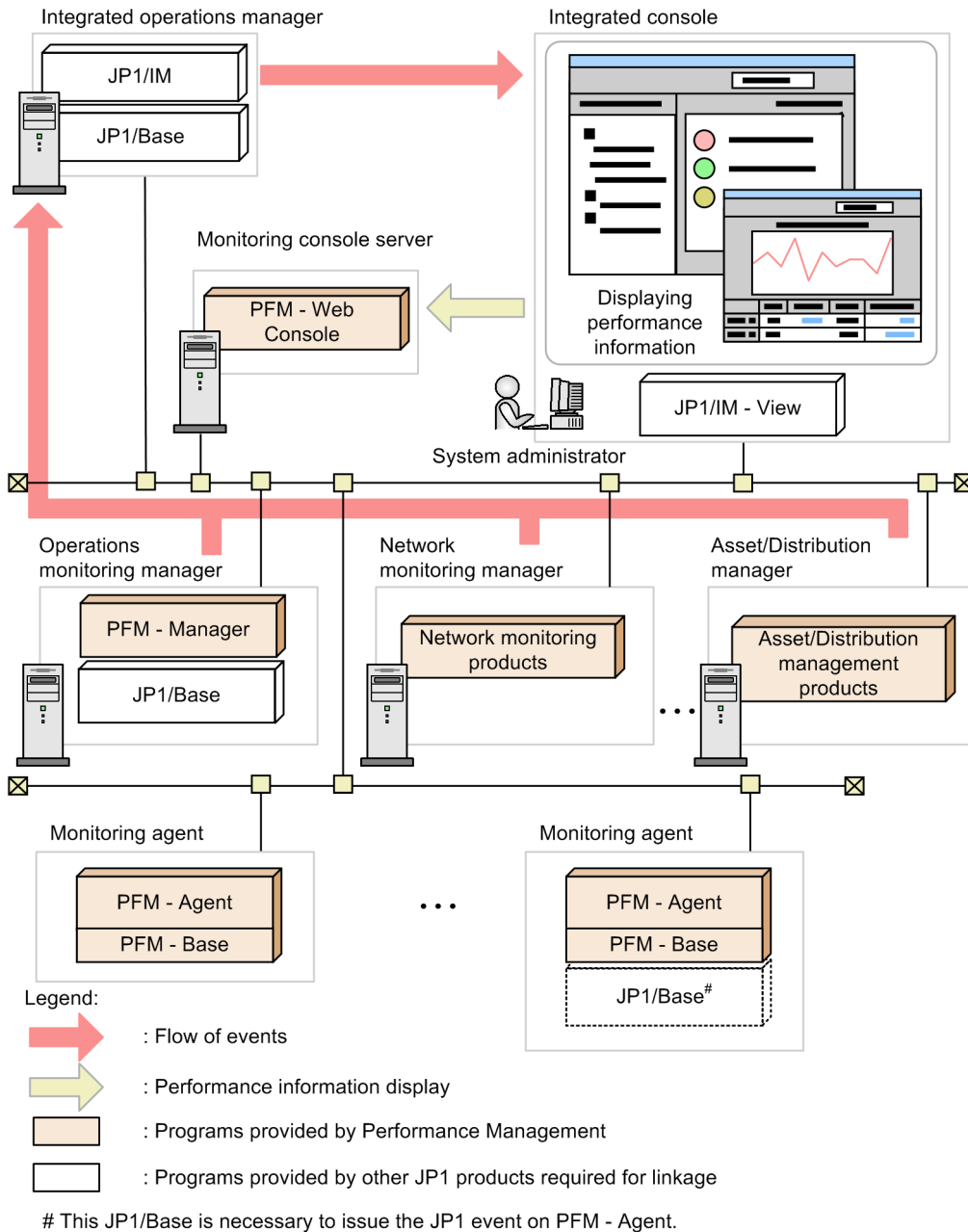
# 12.1 Overview of linking with the integrated management product JP1/IM for operation monitoring

Performance Management enables you to monitor operations by linking with the integrated management product JP1/IM.

By linking with JP1/IM, you can use the same display to monitor Performance Management, other JP1 products, and other programs. If a problem occurs, you can also display a Performance Management report about the host on which the problem occurred, based on the JP1 events issued for the problem. Moreover, you can log on to Performance Management as a JP1 user.

The following figure shows an example of operation monitoring by using Performance Management linked with JP1/IM.

Figure 12–1: Example of operation monitoring by Performance Management linked with JP1/IM



Reference note: What is *JP1/IM*?

JP1/IM is a product that provides integrated operations management of the JP1 series. It provides the functionality to perform integrated management of entire enterprise information systems. With JP1/IM, monitoring is possible with the *integrated console* function and with the *integrated scope* function that allows the entire system to be visualized from a business standpoint. The integrated scope includes a visual monitoring window that allows the entire enterprise system to be visualized from a business standpoint, thereby allowing for the intuitive monitoring of large-scale, complex systems.

JP1/IM provides two methods for monitoring Performance Management. You can select the method that best matches the item being monitored and your goals. Their respective features are as follows:

- Monitoring by using the integrated console  
A console window is used for monitoring JP1 events occurring in the system subject to monitoring (monitoring agent). This method enables JP1 event filtering, and event searches.
- Monitoring by using the integrated scope  
A visual-display window is used for monitoring JP1 events occurring in the monitoring agent. For example, you can effectively visualize the entire system by grouping events by operation or organization, or by grouping by business units across the country or data center layout.

### 12.1.1 Monitoring by using integrated console

The Event Console window in JP1/IM's integrated console can list JP1 events issued from Performance Management.

You can use a displayed JP1 event to display a window of PFM - Web Console (Web browser) from which you can identify the cause of the JP1 event. Moreover, you can use the Web browser to check the contents of alarm definitions, and you can view the report. You can set the console to display only specified JP1 events by changing the display conditions for the event console. When a JP1 event is issued due to an alarm event occurring in Performance Management or a Performance Management service status change, the JP1 event is sent to JP1/IM via JP1/Base, and then is displayed in the Event Console window.

### 12.1.2 Monitoring by using integrated scope

This method enables grouping of systems and monitoring from a tree- or map-type window.

You can display icons on the Monitoring tree window that indicate the operating statuses of the monitoring agents and can check the statuses by checking the color of the icons. In JP1/IM, a monitoring target is called a *monitored object*.



#### Tip

The name of the icon that indicates the operating status of the monitoring agent is *agent-name* Monitoring (PFM) for single-instance agents, and *agent-name\_instance-name* Monitoring (PFM) for multi-instance agents. For example, for a single-instance PFM - Agent for Platform (Windows), Windows Monitoring (PFM) appears as the icon name. For a multi-instance PFM - Agent for Oracle with the instance name `InstA`, Oracle\_InstA Monitoring (PFM) appears as the icon name.

When a JP1 event is issued in Performance Management, the color of the icon for PFM - Agent or PFM - RM changes to a color that indicates the error status. This helps to easily identify agents with problems.



## Note

To use the JP1/IM integrated scope to automatically generate a Monitoring tree, JP1/Base must be running on the PFM - Agent or PFM -RM host that is to be added to the tree.

For details, see the *JP1/Integrated Management - Manager Overview and System Design Guide*, *JP1/Integrated Management - Manager Configuration Guide*, and the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

### 12.1.3 Linkage of Performance Management and JP1/IM

You can set up Performance Management so that a JP1 event detected by JP1/IM triggers display of a report in a window of PFM - Web Console. You can also set it up to enable a window of PFM - Web Console to be displayed from the integrated management menu in JP1/IM.

The following describes linked functions for Performance Management and JP1/IM:

- Displaying a report from JP1/IM

From a JP1 event displayed in the event console window in the JP1/IM integrated console, a report about the host on which the problem occurred can be displayed in the PFM - Web Console window.

Note that the following reports cannot be displayed:

- Reports using target performance data that is collected with the **Do not save** setting enabled
- Reports that exceed the retention period for the target performance data

To display these reports, you need to change the settings for performance data. For details on how to specify settings for performance data, see the section that describes the management functionality for performance data and steps to specify settings in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- Starting the window of PFM - Web Console from the Tool Launcher window of JP1/IM

You can display the window of PFM - Web Console from the Tool Launcher window of JP1/IM to perform performance monitoring.

## 12.2 JP1 events issued from Performance Management to JP1/IM

### 12.2.1 JP1 event types

There are two types of JP1 events: *JP1 system events* and *JP1 user events*. The main differences are as follows:

Table 12–1: Differences between JP1 system events and JP1 user events

Item		JP1 system event	JP1 user event
Event ID		A numerical value from 00004800 to 00004881 is output (fixed number).	Any numerical value can be output. <sup>#1</sup>
Issued event	Occurrence of alarm events	Yes	Yes
	Status change of agents	Yes	No
	Status change of Performance Management services	Yes	No
	Events for operations <sup>#2</sup>	Yes	No
	Change of health check status	Yes	No
	Suspending or resuming monitoring	Yes	No

Legend:

Yes: Events are issued

No: Events are not issued

#1

Any value can be specified when setting up a JP1 user event.

#2

This is an event generated by PFM - Agent or PFM - RM.

Compared to the JP1 user event type, the JP1 system event type covers a larger range of events. Also, when setting up JP1 system events to be issued, you do not need to edit or copy any definition files required by JP1/IM - Manager. We recommend that you use the JP1 system event type if you are using PFM - Manager 09-00 or later.

The JP1 user event type includes events that are equivalent to conventional Performance Management JP1 events (PFM - Manager versions earlier than 08-11).

You should consider these factors when determining which JP1 event type to use.

## 12.3 Installation and setup when linking with JP1/IM

This section describes the installation and setup procedures for setting up an environment for linking with JP1/IM.

When linking with JP1/IM, make sure that PFM - Manager uses the same character set as the instance of JP1/IM with which you are linking. If the character sets are different, double-byte characters and single-byte Katakana characters will not be displayed correctly.

### 12.3.1 Prerequisites for installation when linking with JP1/IM

The following prerequisite conditions for linking with JP1/IM must be satisfied:

- The PFM - Manager host must have JP1/Base installed in order to log on to Performance Management as a JP1 user. Use JP1/Base to manage users.
- JP1/Base on the PFM - Manager host must be configured as an object to be managed by JP1/IM - Manager.
- To start PFM - Web Console from JP1/IM View, the JP1/IM - View host must have a Web browser installed.
- Performance Management 08-00 or later and an earlier version of Performance Management cannot be set up at the same time when establishing linkage with JP1/IM.
- The JP1 authentication mode must be used to display reports from the JP1/IM integrated console.

Note:

If Performance Management earlier than 08-00 is used for setting up the JP1/IM linkage function, you need to perform unsetup of the JP1/IM linkage function of the earlier version (previous to 08-00) and then set up the JP1/IM linkage function using version 08-00 or later again.

- To display a report about the host on which the problem occurred from a JP1 event displayed in the JP1/IM integrated console, the following conditions must be satisfied:
  - If the OS of a monitored host is UNIX, the actual host name is used as the monitoring host name in Performance Management. The result of the `uname -n` command must match the result of the `hostname` command. If it does not, take either of the following actions:  
Change the method for acquiring the host name to `hostname`.  
Configure the environment of the monitored host so that the `hostname` command and the `uname -n` command produce the same output.
  - The name of the event server that issues a JP1 event must match the name of the monitoring host in Performance Management. Names are case sensitive.
  - When a JP1 event is issued, JP1/PFM - Agent or JP1/PFM - RM must be monitoring the host on which the problem occurred.  
To display an OS performance report about a job execution host, PFM - Agent for Platform or PFM - RM for Platform must be monitoring the host.
- The following product versions are required.

No.	Product name	Version
1	JP1/Integrated Management	JP1/IM - Manager 11-10 or later
2		JP1/IM -View 11-10 or later
3	JP1/Base	JP1/Base 11-00 or later <sup>#</sup>

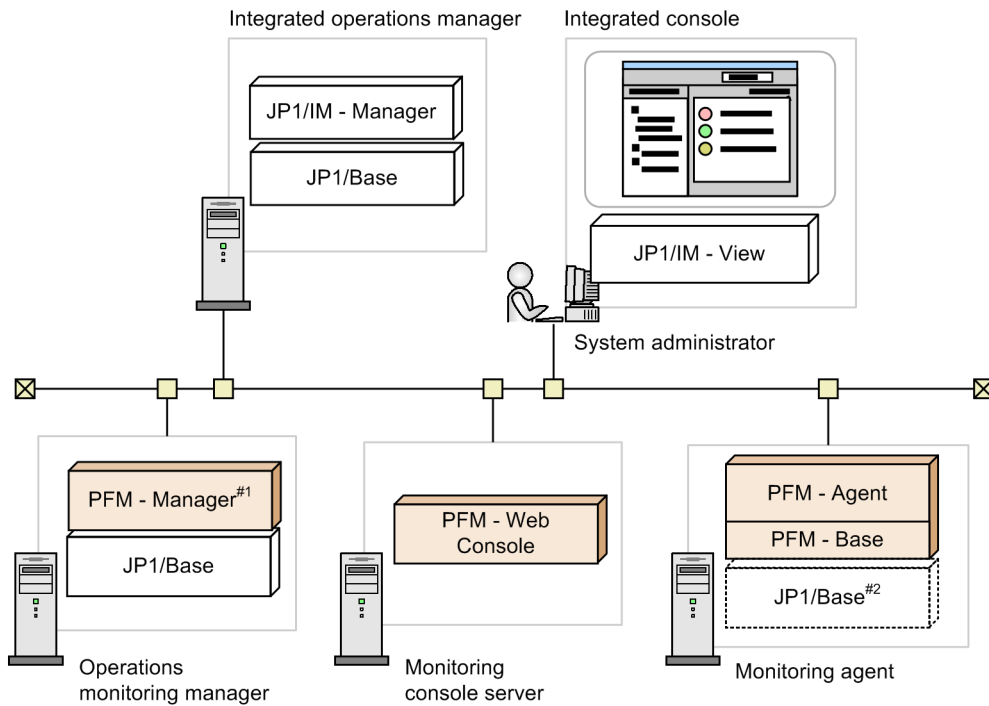
No.	Product name		Version
4	JP1/Performance Management	JP1/PFM - Web Console	11-10 or later <sup>#</sup>

#

If you are running multiple Performance Management systems, the products in all the Performance Management systems must have these versions or later. If an earlier-version product is included, reports might not be displayed because of unsuccessful connection with the PFM - Web Console instance for which reports are to be displayed.

The following figure shows the installation configuration:

Figure 12–2: JP1/IM installation configuration for linkage with JP1/IM



Legend:

- : Programs provided by Performance Management
- : Programs provided by other JP1 products required for linkage
- #1 : When performing IM linkage (including monitoring object linkage) in an environment where PFM - Manager is set on a logical host, JP1/Base must be installed on both the executing and standby hosts.
- #2 : This JP1/Base is necessary to issue the JP1 event on PFM - Agent.

## 12.3.2 Setup for linking with JP1/IM (settings for using JP1/IM to monitor events that occurred in Performance Management)

If the name of the Performance Management monitoring host differs from its actual host name, the monitoring host name must be added to the JP1/IM host information file (`jcs_hosts`). After editing the file, use the following procedure to apply the changes:

1. Import the host information.

```
jcshostsimport -o (host-information-file)
```

2. Reload JP1/IM.

```
jco_spmc_reload
```

For details on the host information file and JP1/IM commands, see the *JP1/Integrated Management - Manager Overview and System Design Guide* or the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The table below shows the procedure for specifying the settings required for using JP1/IM to monitor events that occurred in Performance Management. The required settings depend on the JP1 event type used and the extent of linkage between Performance Management and JP1/IM.

**Table 12–2: Procedure for specifying the settings required for using JP1/IM to monitor events that occurred in Performance Management**

No.	Procedure	Refer to:	Necessity for setting	
			JP1 system event	JP1 user event
1	Configuration for issuing JP1 events In the PFM - Web Console, set up the configuration so that JP1 events are issued when a monitored event occurs in JP1/IM.	<a href="#">12.3.2(1)</a>	Required	Required
		<a href="#">12.3.2(2)</a>	Optional (set if necessary)	Optional (set if necessary)
2	Defining alarm events and reports Define alarm events to be monitored in JP1/IM and operation reports in the PFM - Web Console.	<a href="#">12.3.2(3)</a>	Required	Required
3	Setting for linking with JP1/IM integrated console Edit the definition files required in JP1/IM - Manager, and then store them under a directory for JP1/IM.	<a href="#">12.3.2(4)(a)</a>	None required <sup>#1</sup>	Required
4	Setting for linking with the Tool Launcher window of JP1/IM <sup>#2</sup> Edit the definition files required in JP1/IM - View, and then store them under a directory for JP1/IM.	<a href="#">12.3.2(4)(b)</a>	Required if linking	Required if linking
5	Setting for linking with the integrated scope of JP1/IM <sup>#3</sup> Execute the command for linkage with the monitored object ( <code>jpccconf im</code> command).	<a href="#">12.3.2(5)</a>	Required if linking	Required if linking
6	Specifying whether the messages of JP1 user events are enclosed in quotes In UNIX, specify whether JP1 user event messages are enclosed in quotes.	<a href="#">12.3.2(6)</a>	Unavailable	Optional (Set if not using quotation mark)

#1

For a JP1 system event, you do not need to edit or copy the definition file, even when linking with JP1/IM integrated console.

#2

You must complete no. 3 in the table (setting for linking with JP1/IM integrated console) before you can configure Performance Management to link with the JP1/IM Tool Launcher.

#3

You must complete no. 3 in the table (setting for linking with JP1/IM integrated console) before you can configure Performance Management to link with the JP1/IM integrated scope.

Note:

Linkage with the system-monitored object for Performance Management in JP1/IM is required in order to enable monitoring with the integrated scope. For details on settings and operations of JP1/IM, see the *JP1/Integrated*

This subsection describes the setup procedures for linking with JP1/IM.

## (1) Configuring so that JP1 events are issued

To configure the setting:

1. From the monitoring console Web browser, log on to PFM - Web Console.  
Log on to a user account that has administrator user permissions.  
You must have administrator user permissions to use the Services window.
2. In the navigation frame of the main window, select the **Services** tab.
3. In the navigation frame of the Services window, choose the service to be set.  
The selected service is marked with a checkmark.  
The following table lists the events that trigger JP1 system events and the properties to be set for each target service.
4. Set the property values appropriate for the JP1 event you want to issue.  
The following table lists the JP1 events to be issued and the properties to be set for each target service.

Table 12–3: JP1 events to be issued and properties to be set for each target service

Event to be issued	Services that trigger events	Properties to be set	Setting procedure location
Events related to the operation of, or a change in the status of, PFM services (Event IDs of JP1 system events: 00004800 to 00004830)	PFM - Manager services <ul style="list-style-type: none"> <li>• Name Server</li> <li>• Master Manager</li> <li>• Master Store</li> <li>• Correlator</li> <li>• Trap Generator</li> <li>• View Server</li> </ul>	<b>JP1 Event Configurations</b> node for Master Manager	12.3.2(1)(a)
	PFM - Agent and PFM - RM services <ul style="list-style-type: none"> <li>• Agent Collector and Remote Monitor Collector</li> <li>• Agent Store or Remote Monitor Store</li> </ul> These services are used instance by instance (for multi-instance agents).	<b>JP1 Event Configurations</b> node for Agent Collector or Remote Monitor Collector	
	Status Server service <sup>#2</sup> <ul style="list-style-type: none"> <li>• Status Server</li> </ul>	<b>JP1 Event Configurations</b> node for Master Manager, Agent Collector, Remote Monitor Collector, or Action Handler <sup>#1</sup>	
	Action Handler service <ul style="list-style-type: none"> <li>• Action Handler</li> </ul>		
Event related to a change in agent status (Event ID of JP1 system event: 00004850)	PFM - Agent and PFM - RM services <ul style="list-style-type: none"> <li>• Agent Collector or Remote Monitor Collector</li> <li>• Agent Store or Remote Monitor Store</li> </ul>	<b>JP1 Event Configurations</b> node for Agent Collector or Remote Monitor Collector	

Event to be issued	Services that trigger events	Properties to be set	Setting procedure location
Event related to a change in agent status (Event ID of JP1 system event: 00004850)	These services are used instance by instance (for multi-instance agents).	<b>JP1 Event Configurations</b> node for Agent Collector or Remote Monitor Collector	<i>12.3.2(1)(a)</i>
Alarm event (JP1 system event issued for alarms) (Event ID of JP1 system event: 00004840)	--	<b>Alarm</b> node under <b>JP1 Event Configurations</b> for Master Manager, Agent Collector, Remote Monitor Collector, or Action Handler on the host that has the Action Handler service specified for executing actions in response to alarms	<i>12.3.2(1)(b)</i>
Events related to suspending or resuming monitoring (Event IDs of JP1 system events: 00004870, 00004871, 00004880, 00004881)	--	<b>System</b> node under <b>JP1 Event Configurations</b> for Master Manager	<i>12.3.2(1)(c)</i>
Events related to a change in the health check status (Event ID of JP1 system event: 00004860)	--	<b>Health Check Configurations</b> node of Health check Agent Collector	<i>12.3.2(1)(d)</i>

Legend:

--: Not applicable

#1

Use the same value for the listed services on the same host.

#2

The Status Server service does not appear as a service on a logical host.

## (a) Configuring the issuing of JP1 system events by individual PFM services

1. Select the **JP1 Event Configurations** node.

At the bottom of the information frame, the properties of the **JP1 Event Configurations** node are displayed.

2. Select the service for which you want JP1 system events to be issued, and then set the following property value:  
**Service for which events are issued:** Yes

## (b) Configuring the issuing of JP1 system events by alarms

1. Select the **Alarm** node under the **JP1 Event Configurations** node.

At the bottom of the information frame, the properties of the **Alarm** node are displayed.

2. Set the properties to the following:

Specify a JP1 event type to be associated if an alarm event occurs.

### JP1 Event Mode

To use a JP1 system event: JP1 System Event

To use a JP1 user event: JP1 User Event

## (c) Configuring the issuing of JP1 system events for suspending or resuming monitoring

1. Select the **System** node under the **JP1 Event Configurations** node.  
At the bottom of the information frame, the properties of the **System** node are displayed.
2. Set the properties to the following:

### Monitoring Suspend

Specify whether to issue a JP1 system event when monitoring is suspended or resumed. The default value is **No**.

To issue a JP1 system event: **Yes**

To issue a JP1 system event only in the primary system in a multiple monitoring environment: **Yes (Primary)**

To issue no JP1 system event: **NO**

## (d) Configuring events related to a change in health check status

1. Select the **Health Check Configurations** node.  
The bottom of the information frame displays the properties of the **Health Check Configurations** node.
2. Set the properties to the following:  
**JP1 Event:** **Yes**

## (2) Configuring options for JP1 system events

1. From the Web browser of the monitoring console, log on to PFM - Web Console.  
Log on with a user account that has administrator user permissions.  
You must have administrator user permissions to use the Services window.
2. In the navigation frame of the Main window, select the **Services** tab.
3. For Master Manager, Agent Collector, Remote Monitor Collector, or Action Handler, select the **JP1 Event Configurations** node.  
Master Manager, Agent Collector, Remote Monitor Collector, and Action Handler use the same property value for the services on the same host.

### JP1 Event Send Host

Specify the name of an event server connected to JP1/Base using 255 or less alphanumeric characters. You can only specify an event server running on the same logical or physical host as the Performance Management service that issues the JP1 events. You cannot specify an IP address. Any preceding or trailing spaces in the specified value are ignored.

If you specify an out-of-range value or if no value is specified, a physical host is used as the event-issuing host. The default value is blank.

If a logical host is configured and the event related to the change of health check status (JP1 system event with event ID 00004860) is set, select the **Health Check Configurations** node for the health check Agent Collector service. Then, set the following property:

**JP1 Event - Send Host Mode:** JP1 Event Send Host Value

### Monitoring Console Host

To start the PFM - Web Console, specify the name of the PFM - Web Console host in the JP1/IM - Manager monitor startup function. Specify the name with 255 or less alphanumeric characters. You cannot specify an IP address. Any preceding or trailing spaces in the specified value are ignored.



If an out-of-range value is specified or if no value is specified, the name of the PFM - Manager for the connection destination of PFM - Agent Console is assumed.

The default value is blank.

### Monitoring Console Port

Specify the port number (http request port number) for the PFM - Web Console to be started. If no value is specified, the value 20358 is assumed.

The default value is blank.

### Monitoring Console Https

If JP1/IM - Manager's monitor startup feature is used to start PFM - Web Console, specify whether encrypted communication using `https` is to be used to connect to PFM - Web Console.

The default value is `No`.

## (3) Associating alarms with JP1 events and reports

In the Alarms window of PFM - Web Console, set up the following items:

- Set up the issuing of a JP1 event as an action.  
This item sets up the issuing of a JP1 event as the action to be performed when an alarm is issued.
- Associate alarms with reports.  
This item enables reports to be displayed in the window of PFM - Web Console from the JP1/IM event console.

For details on the definition of alarms, see [6. Monitoring Operations with Alarms](#).

The following procedure mainly describes operations for setting up JP1 events to be issued and for associating alarms with reports.

1. Log on to PFM - Web Console as a user with administrator user permissions.
2. In the navigation frame of the Main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms window, select the alarm definition for which you want to issue JP1 events.  
The selected alarm is marked with a checkmark.
4. Choose the **Edit** method in the method frame.
5. In the Edit > Main Information window in the information frame, click the **Next** button.
6. In the Edit > Action window, enter settings in the **Actions to be executed** area.  
In **Command**, select conditions (**Abnormal**, **Warning**, or **Normal**) of the alarm for which you want to issue JP1 events.
7. In **Report to be displayed**, click the **Browse** button to select the report to be associated with the alarm.  
The selected report is marked with a checkmark.
8. Click the **Finish** button.
9. Click the **Next** button.
10. In the **Command definition** area of the Edit > Action Definitions window, click the **JP1 Event** button.
11. In the New Alarm > Action Definitions > JP1 Event Settings window, set the event ID and other information.  
For example, suppose you want to send the JP1 event under the following conditions:

Conditions:

- Set the event ID to 001.
- Set the message text to the content of the message text (%MTS), which you set in the **Message** of the New Alarm Table > Main Information dialog box.
- Convert the alarm status to a severity-level JP1 event.

Set as follows:

**Event ID:** 001

**Message:** %MTS

**Convert the alarm level to the severity level:** Selected

Note:

Do not modify the attributes of the JP1 event if you want to link with the JP1/IM monitoring objects.

For a JP1 system event, the information set for **Event ID** is output as an event ID (JPC\_USER\_EVENTID) identifying an extended JP1 event attribute. For a JP1 user event, the information is output as an event ID for a basic JP1 event attribute.

For details on JP1 event types, see *12.2 JP1 events issued from Performance Management to JP1/IM*.

12. Click the **OK** button.

The issuing of the JP1 event is defined as an alarm action, and the selected report is associated. For details on the issued JP1 events, see *12.6 List of attributes of JP1 events issued when linking with JP1/IM*.

13. Select the Action Handler service of the host that issues the JP1 event.

When you enter settings in the JP1 Event Settings window, the setting in **Action handler** changes automatically. By default, the Action Handler service on the PFM - Manager host is selected. If you want to issue the JP1 event on a host other than the PFM - Manager host, you must modify the setting in **Action handler**.

Note 1

To issue a JP1 event, JP1/Base must be installed on the same host as the Action Handler that issues the event.

Note 2

To issue a JP1 event during Performance Management monitoring using the JP1/IM integrated scope, you must select an Action Handler service running on the same host as PFM - Manager.

Note 3

You can change which host's Action Handler service is selected by setting the `selectAHModeForJP1Event` parameter in the initialization file (`config.xml`). For details on how to enter settings in the initialization file (`config.xml`), see the section describing the file in the appendixes of the manual *JP1/Performance Management Reference*.

If you want to issue the JP1 event on a host other than the automatically selected host, you must modify the setting in **Action handler** manually.

14. When you want to issue a JP1 event to a logical host in a logical host environment, add the `-r logical-host-name` option to **Command arguments**.

If you do not specify this option, JP1 events are registered in the physical host.

15. Click the **Finish** button.

## (4) Editing and copying the definition files for linkage

In order to enable monitoring of JP1 events by using JP1/IM, you need to edit the JP1/IM definition files that are provided by Performance Management according to the environment and to copy the files to each of the corresponding JP1/IM directories.

### Tip

- You might need to restart JP1/IM to enable the editing of definition files in JP1/IM. For details on restart timings of the definition files and timing when the definition files take effect, see the *JP1/Integrated Management - Manager Overview and System Design Guide*, *JP1/Integrated Management - Manager Configuration Guide*, and the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- If the source and destination hosts for the copied JP1/IM definition files are running different operating systems and one of those operating systems is Linux, change the encoding of the target definition files by using, for example, a text editor or the `nkf` command. The resulting encoding must be as follows:  
If the operating system to which JP1/IM definition files are copied is Linux:  
UTF-8  
If the operating system from which JP1/IM definition files are copied is Linux:  
Shift JIS or EUC

The JP1/IM definition file provided by Performance Management is stored in the following folder:

- In Windows:  
`PFM-Web-Console-installation-folder\sample\imconf`
- In UNIX:  
`/opt/jp1pcwebcon/sample/imconf/`

### (a) Definition files required in JP1/IM - Manager

When you use monitoring with the integrated console to issue a JP1 user event, you must edit and copy the definition file required by JP1/IM - Manager. This is not necessary when you use monitoring with the integrated console to issue a JP1 system event.

- Definition file for the extended event attributes

This file defines the extended event attributes of JP1 events.

File name:

```
hitachi_jp1_pfmwebcon_attr_language-codes.conf
```

Items to edit:

Change the `order id` value to the event ID set by the JP1 event-issuing command. To display reports from JP1/IM, you also need to set the specified event ID in the definition file for opening monitor windows.

For example, specify the following when the event ID is 00001234:

```
@define-block type="event-attr-order-def";  
block platform="BASE",extended="false";  
order id="00001234"  
,attrs="_COMMON|E.JPC_AGENT|E.JPC_MGR|E.JPC_TIME|E.JPC_REPORTID";  
@define-block-end;
```

## Copy destination

Copy the edited definition file for the extended event attributes to the directory on the host that has JP1/IM - Manager installed as listed below:

For physical hosts:

- In Windows:  
*installation-folder-for-jp1/im-manager*\JP1Cons\conf\console\attribute\
- In UNIX:  
/etc/opt/jp1cons/conf/console/attribute/

For logical hosts:

- In Windows:  
*shared-folder*\jp1cons\conf\console\attribute\
- In UNIX:  
*shared-directory*/jp1cons/conf/console/attribute/

For details, see the *JP1/Integrated Management - Manager Overview and System Design Guide*, *JP1/Integrated Management - Manager Configuration Guide*, and the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Definition file for opening monitor windows

This file defines settings for opening monitor windows. The definition file for opening monitor windows is used to open a monitor window, such as one for the event-issuing source, from the event console window of JP1/IM - View. You need to enter settings in this file if you want to display a View Report window in PFM - Web Console when a JP1 event occurs.

File name:

`hitachi_jp1_pfmwebcon_mon_language-codes.conf`

Items to edit:

Change the value of the `EVENT_ID` to the event ID set with the JP1 event-issuing command. Also, change the communication protocol, host name, and port number in `PATH` to those of PFM - Web Console. Note that the specified event ID needs to be set in the definition file for the extended event attributes.

For example, if 00001234, http, PFM-WebCon, and 20358 are assigned to the event ID, communication protocol, host name, and port number, respectively, specify as follow:

```
DEF_KEY PRODUCT_NAME=/PFM/ALARM_EVENT EVENT_ID=00001234 INTERFACE=PC_MONITOR
DEF_MTR_CALL NAME=PC_MONITOR EXEC_ID=default_browserPATH="http://PFM-WebCon:20358/
PFMWebConsole/login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER$UR
LENC%&manager=%IM_EVC_PARAMETER_1$URLENC%&reportId=%IM_EVC_PARAMETER_2$URLENC%&nod
e=%IM_EVC_PARAMETER_3$URLENC%" PARAM=E.JPC_MGR,E.JPC_REPORTID,E.OBJECT_ID
```

## Copy destination

Copy the edited definition file for opening monitor windows to the directory on the host that has JP1/IM - Manager installed as listed below:

For physical hosts:

- In Windows:  
*installation-folder-for-jp1/im-manager*\JP1Cons\conf\console\monitor\
- In UNIX:

```
/etc/opt/jplcons/conf/console/monitor/
```

For logical hosts:

- In Windows:  
`shared-folder\jplcons\conf\console\monitor\`
- In UNIX:  
`shared-directory/jplcons/conf/console/monitor/`

For details, see the *JP1/Integrated Management - Manager Overview and System Design Guide*, *JP1/Integrated Management - Manager Configuration Guide*, and the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Example of displaying View Report windows in PFM - Web Console for several instances of PFM - Manager

Note

A PFM - Web Console instance is required for each PFM - Manager instance. For example, if there are two PFM - Manager instances, there must be two PFM - Web Console instances.

You need to use different event IDs to display View Report windows in PFM - Web Console for multiple PFM - Managers.

For example, if 00000000 and 00001111 are assigned to the event IDs, specify the definition file for the extended event attributes and the definition file for opening monitor windows as follows:

Definition file for the extended event attributes:

```
@file type="extended-attributes-definition", version="0300";
@product name="/PFM/ALARM_EVENT";
@define-block type="event-attr-def";
block platform="BASE", extended="false", lang="English";
attr name="E.JPC_AGENT", title="Agent host name";
attr name="E.JPC_MGR", title="Manager host name";
attr name="E.JPC_TIME", title="Alarm time";
attr name="E.JPC_REPORTID", title="Report ID";
@define-block-end;
@define-block type="event-attr-group-def";
block platform="BASE", extended="false";
group name="_COMMON", attrs="";
group name="_COMMON_START", attrs="";
group name="_COMMON_END", attrs="";
@define-block-end;
@define-block type="event-attr-order-def";
block platform="BASE", extended="false";
order id="00000000", attrs="_COMMON|E.JPC_AGENT|E.JPC_MGR|E.JPC_TIME|E.JPC_REPORTID";
order id="00001111", attrs="_COMMON|E.JPC_AGENT|E.JPC_MGR|E.JPC_TIME|E.JPC_REPORTID";
@define-block-end;
```

Definition file for opening monitor windows:

```
DESC_VERSION=0300

#PFM - View definition file for monitor window transitions

DEF_KEY PRODUCT_NAME=/PFM/ALARM_EVENT EVENT_ID=00000000 NTERFACE=PC_MONITOR1
DEF_KEY PRODUCT_NAME=/PFM/ALARM_EVENT EVENT_ID=00011111 NTERFACE=PC_MONITOR2

DEF_MTR_CALL NAME=PC_MONITOR1 EXEC_ID=default_browser PATH="http://PFM-Webcon1:8080/
PFMWebConsole/login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER
$URLE
NC%&manager=%IM_EVC_PARAMETER_1$URLENC%&reportid=%IM_EVC_PARAMETER_2$URLE
NC%&node=%l
M_EVC_PARAMETER_3$URLENC%" PARAM=E.JPC_MGR,E.JPC_REPORTID,E.OBJECT_ID

DEF_MTR_CALL NAME=PC_MONITOR2 EXEC_ID=default_browser PATH="http://PFM-Webcon2:20358
/PFMWebConsole/login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USE
R$URL
ENC%&manager=%IM_EVC_PARAMETER_1$URLENC%&reportId=%IM_EVC_PARAMETER_2$URLE
NC%&node=
%IM_EVC_PARAMETER_3$URLENC%" PARAM=E.JPC_MGR,E.JPC_REPORTID,E.OBJECT_ID
```

In the example above, the event ID 00000000 corresponds to PFM - Web Console host name PFM-Webcon1 and port number 8080. Similarly, the event ID 00011111 corresponds to PFM - Web Console host name PFM-Webcon2 and port number 20358.

## (b) Definition files required in JP1/IM - View

- Definition file for the tool launcher

The definition file for the tool launcher defines the tree structure and display items to be displayed in the Tool Launcher window in JP1/IM - View. You need to set the definition file for the tool launcher to enable the window of PFM - Web Console to be displayed from the Tool Launcher window.

File name

```
hitachi_jp1_pfmwebcon_tree.conf
```

Items to edit

Also, change the communication protocol, host name, and port number in `arguments` to those of PFM - Web Console.

For example, if `http`, `PFM-WebCon`, and `20358` are assigned to the communication protocol, host name, and port number, respectively, specify as follow:

```
name="Server Availability Management (Administrator)";
execute_id="default_browser";arguments="http://PFM-WebCon:20358/WebConsole/
login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER$URLENC %"
;@define-block-end;
```

Copy destination

Copy the edited definition file for the tool launcher to the folder on the host that has JP1/IM - View installed, as follows:

```
installation-folder-for-JP1/IM - View\conf\function\language-codes\
```

- Example: Windows of PFM - Web Console are started respectively by differing hosts  
You need to define blocks within the definition file for the tool launcher corresponding to respective PFM - Web Console to enable differing hosts to start windows of PFM - Web Console respectively. For details, see the JP1/

*Integrated Management - Manager Overview and System Design Guide, JP1/Integrated Management - Manager Configuration Guide, and the manual JP1/Integrated Management - Manager Command and Definition File Reference.*

The following provides an example of setting the definition file for the tool launcher and an example of the Tool Launcher window display.

Example settings: Definition file for the tool launcher

```

@file type="function-definition", version="0300";
#-----
@define-block type="function-tree-def";
id="jco_JP1_PC_manager1";
parent_id="jco_folder_ServerAvailability";
name="Server Availability Management 1";
execute_id="default_browser";
arguments="http://PFM-
WebCon1:20358/PFMWebConsole/login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&user
Name=%JCO_JP1USER$URLENC%";
@define-block-end;
#-----
@define-block type="function-tree-def";
id="jco_JP1_PC_manager2";
parent_id="jco_folder_ServerAvailability";
name="Server Availability Management 2";
execute_id="default_browser";
arguments="http://PFM-
WebCon2:32222/PFMWebConsole/login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&user
Name=%JCO_JP1USER$URLENC%";
@define-block-end;
#-----
@define-block type="function-tree-def";
id="jco_folder_ServerAvailability";
parent_id="root";
name="Server Availability Management";
@define-block-end;
#-----

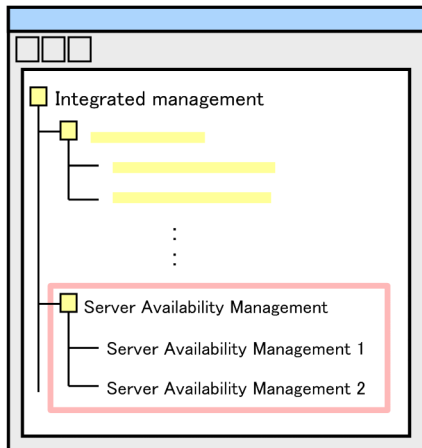
```

Setting of Server 1

Setting of Server 2

Setting of the server availability management folder

Example of the Tool Launcher window



In the examples above, double-clicking **Server Availability Management 1** in the Tool Launcher window connects the program to PFM - Web Console with the host name of *PFM - WebCon1* and port number *20358*, and then starts the corresponding window of PFM - Web Console. Similarly, double-clicking **Server Availability Management 2** in the Tool Launcher window connects the program to PFM - Web Console with the host name of *PFM - WebCon2* and port number *32222*, and then starts the corresponding window of PFM - Web Console.



## (5) Using icons to monitor the system operating status by linking with the JP1/IM monitored object function

If you want to use icons to monitor the operating status of the system in Performance Management by linking with the monitored object function of JP1/IM, you need to execute the `jpccconf im` command on the PFM - Manager host and then automatically generate the monitoring tree. This step is required for JP1/IM to collect definition information from Performance Management. In a cluster environment, the logical host names of PFM - Manager and JP1/Base must be the same.

1. Execute the `jpccconf im` command on the PFM - Manager host.

Execute the `jpccconf im` command on the PFM - Manager host as shown below to start linkage with JP1/IM:

```
jpccconf im enable
```

Execute the command as shown below to stop linkage with JP1/IM:

```
jpccconf im disable
```

If PFM - Manager is in a logical host environment, execute the command one time on both the active and standby nodes.

2. In the JP1/IM integrated scope, automatically generate the monitoring tree.

For details on how to do so, see the *JP1/Integrated Management - Manager Overview and System Design Guide*, the *JP1/Integrated Management - Manager Configuration Guide*, and the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

## (6) Setting quotation marks enclosing a JP1 user event message

For UNIX, a JP1 user event message can be enclosed in double quotation marks ("). To enclose such a message in double quotation marks, directly edit the `jpccomm.ini` file, which is located on the host running the Action Handler server that executes the action. To specify whether the messages of JP1 user events are enclosed in quotes:

1. Stop the Action Handler service to be configured.

For the logical host environment, stop the Action Handler services of the logical host.

2. Edit the `jpccomm.ini` file.

The `jpccomm.ini` file is stored in the following locations:

On physical hosts:

```
/opt/jp1pc/
```

On logical hosts:

```
environment-directory/jp1pc/
```

The following table describes the section name, label name, and range of setting values that you can edit in the `jpccomm.ini` file.

**Table 12–4: Setting item for specifying whether the messages of JP1 user events are enclosed in quotes**

Section	Label name	Value range	Default value	Description
[Common Section]	JP1 Event Double Quote	0   1	1	Specify whether the messages of JP1 user events are enclosed in quotes. 0: Do not enclose in quotes 1: Enclose in quotes



This label is available only for UNIX. In Windows, the setting of the label is ignored.

3. Start the Action Handler service that has been configured.

### 12.3.3 Setup for linking with JP1/IM (settings for displaying reports from events in the integrated console)

Specify the following settings to display a report about the host on which a problem occurred, from a JP1 event displayed in the JP1/IM integrated console.

For details about the versions required to display reports for such hosts from JP1 events, see [12.3.1 Prerequisites for installation when linking with JP1/IM](#).

1. Copy the performance report definition file (`performance.conf`) from the PFM - Web Console installation directory to the location in JP1/IM - Manager as follows:

- The copy-source location is as follows:

In Windows:

`installation-directory-for-PFM-Web-Console\sample\imconf`

In UNIX:

`/opt/jp1pcwebcon/sample/imconf`

- The copy-destination location is as follows:

In Windows:

Physical host: `Console-path\conf\console\performance\`

Logical host: `environment-folder\jp1cons\conf\console\performance`

In UNIX:

Physical host: `/etc/opt/jp1cons/conf/console/performance/`

Logical host: `environment-directory/jp1cons/conf/console/performance`

2. Open the performance report definition file you stored in step 1. Then, on the second line, specify the URL for logging on to PFM - Web Console for the connection destination.

- For example, if the communication protocol is `http`, and PFM - Web Console for the connection destination has the host name `PFM-WebCon` and port number `20358`, specify as follows:

```
#the definition file for displaying performance reports
http://PFM-WebCon:20358/PFMWebConsole/login.do
```

- As the character encoding for saving the file you edited, use the language encoding specified for running JP1/IM - Manager. In Windows, use Shift JIS encoding (MS932). In UNIX, use the character encoding specified in the `LANG` environment variable in `/etc/opt/jp1base/conf/jp1bs_env.conf` on the host running JP1/IM - Manager.

3. Instances of PFM - Web Console other than the one specified in the performance report definition file in step 2 might also monitor the host on which the problem occurred. In this case, edit the initialization file (`config.xml`) on the PFM - Web Console host specified in the performance report definition file.

Items to edit

host, port, and `https` under the `<search-WebConsole>` tag under the `<vsa>` tag

## Editing method

Define the host name, port number, and encrypted communication setting for an instance of PFM - Web Console not specified in the performance report definition file. To define multiple instances of PFM - Web Console, define the `<search-WebConsole>` tag for the number of instances of PFM - Web Console.

## Example of a definition

```
<vsa>
  <search-WebConsole>
    <param name="host" value="PFMWebCon2"/>
    <param name="port" value="20358"/>
    <param name="https" value="ON"/>
  </search-WebConsole>
  <search-WebConsole>
    <param name="host" value="PFMWebCon3"/>
    <param name="port" value="20358"/>
    <param name="https" value="OFF"/>
  </search-WebConsole>
</vsa>
```

4. Use JP1/IM to map the host on which the problem (which triggered the JP1 event) occurred to the event-issuing event server.

This setting is required if the host on which the problem occurred is different from the event-issuing event server, and the JP1 event is issued by a product other than JP1/AJS3. For details, see the *JP1/Integrated Management - Manager Configuration Guide*.

5. In JP1/IM - Manager, restart the service or execute the `jco_spm�_reload` command.

If you are logged on to JP1/IM - View, exit JP1/IM - View, and then log on again.

6. Restart the PFM - Web Console service.

## 12.3.4 Releasing linkage with JP1/IM

To release linkage with JP1/IM, delete the definition files for JP1/IM linkage.

Delete all definition files you have copied to the JP1/IM directory. For details on the trigger applied to JP1/IM for deletion of a definition file, see the *JP1/Integrated Management - Manager Overview and System Design Guide*, *JP1/Integrated Management - Manager Configuration Guide*, and the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If reports for multiple instances of PFM - Web Console are displayed from the JP1/IM integrated console, comment out or delete the `<search-WebConsole>` tag in the initialization file (`config.xml`), and then restart the PFM - Web Console service.

## 12.4 Changing the configuration after linking with JP1/IM

---

This section describes the settings required to change a host name after linking with JP1/IM.

### 12.4.1 Changing a host name after linking with JP1/IM

For details about how to change a host name after linking with JP1/IM, see the chapter describing how to change a physical host name in the *JP1/Performance Management Planning and Configuration Guide*.

If you are running a cluster system, see *10.3.3 Changing logical host names after starting operation* or *10.5.3 Changing logical host names after starting operation* in this manual.

If the monitoring host name specified in Performance Management differs from the actual host name, another setting is required in addition to the standard procedure. That is, specify the settings so that the name of the Performance Management monitoring host matches the event server name on the host on which the problem (which triggered the JP1 event) occurred.

### 12.4.2 Changing an IP address after linking with JP1/IM

For details about how to change an IP address after linking with JP1/IM, see the chapter describing how to change IP address settings in the *JP1/Performance Management Planning and Configuration Guide*.

## 12.5 Operating the linkage with JP1/IM

---

This section describes the procedure for monitoring Performance Management from JP1/IM. For details on settings and operations of JP1/IM, see the *JP1/Integrated Management - Manager Overview and System Design Guide* and *JP1/Integrated Management - Manager Configuration Guide*.

### 12.5.1 Monitoring alarm events from the JP1/IM integrated console

The Event Console window of JP1/IM's integrated console displays information based on JP1 events sent from JP1 series programs. The information displayed in the Event Console window includes the severity of JP1 events, event reception time, and messages. This window is for monitoring alarm events.

### 12.5.2 Monitoring from the JP1/IM integrated scope

Once you have set up the function to monitor the status of Performance Management in the Monitoring tree window of the JP1/IM integrated scope, an icon representing status appears in the window. The color of the icon changes when an alarm event occurs. You can check a detailed description of events in the Event Console window.

### 12.5.3 Displaying a Performance Management report from the JP1/IM integrated console

1. In the event console window, select the JP1 event for which you want to display a report.
2. Right-click, and then select **Display Performance**.  
A PFM - Web Console window appears.  
Alternatively, to display this window, right-click, select **Event Details**, and then in the Event details window that appears, click the **Display Performance** button.
3. In the Select Report window, select the type of the report you want to display.  
A report about the host on which the problem (which triggered the JP1 event) occurred is displayed.

#### Important

- After starting PFM - Web Console from the JP1/IM integrated console, if you restart PFM - Web Console from the integrated console, an error occurs in the window that opened first. Then, the message (KAVJS0025-E) appears. If you want to open the window that opened first, close all PFM - Web Console windows, and then open the report again from the integrated console.
- If you display a report from the JP1/IM integrated console with the Firefox web browser, you cannot close the browser by clicking **Close** in the window. To close the browser, use the termination function of the browser.

#### Note

The window that appears after you click **Display Performance** depends on the Performance Management authentication mode and the permission level of the login user.

## 12.5.4 Starting PFM - Web Console from the JP1/IM integrated management menu

1. From **Options**, choose **Tool Launcher** on the Event Console window in the integrated console of JP1/IM.
2. In the Tool Launcher window, select the **Server Availability Management** folder in the tree of programs managed by JP1/IM.
3. From the expanded menu, choose **Server Availability Management**.  
The window that appears might vary depending on the Performance Management authentication mode.  
In PFM authentication mode:  
    The Login window of PFM - Web Console appears.  
In JP1 authentication mode:  
    The window of PFM - Web Console is started in order to perform user authentication automatically for previously logged-on JP1/IM users.

## 12.6 List of attributes of JP1 events issued when linking with JP1/IM

### 12.6.1 When alarm events occur

You can set up a configuration so that either JP1 system events or JP user events are issued when an alarm event occurs.

The following table lists the JP1 system events to be issued when an alarm event occurs.

Table 12–5: JP1 event attributes and contents

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	(Not applicable)	00004840
		Message	(Not applicable)	The value that has been specified in <b>Message</b> in the procedure for issuing JP1 events.
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information Alarm status: OK (The alarm status is Normal (green).)</li> <li>Warning Alarm status: WARNING (The alarm status is Warning (yellow).)</li> <li>Error Alarm status: EXCEPTION (The alarm status is Abnormal (red).)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM/ALARM_EVENT
		Object type	OBJECT_TYPE	ALARM
		Object name	OBJECT_NAME	Alarm name
		Registration type	ROOT_OBJECT_TYPE	ALARM_TABLE
		Registration name	ROOT_OBJECT_NAME	Alarm table name
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	NOTICE
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	<ul style="list-style-type: none"> <li>In PFM - Agent Host name of PFM - Agent where an alarm was issued</li> <li>In PFM-RM (remote agent) Monitored host name of a remote agent where an alarm was issued</li> <li>In PFM-RM (group agent) Primary host name of a group agent where an alarm was issued (<i>PFM-RM-host-name</i>)</li> </ul>

Attribute type		Item	Attribute name	Contents
Extended attribute	Specific information	Date and time of alarm occurrence	JPC_TIME	Date and time when the alarm occurred
		Displayed report ID	JPC_REPORTID	Report definition ID to be displayed when a JP1 event is selected
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination
		Event ID	JPC_USER_EVENTID	The value that has been specified in <b>Event ID</b> in the procedure for issuing JP1 events when an alarm event occurs.

The following table lists the JP1 user events to be issued when an alarm event occurs.

**Table 12–6: JP1 user events to be triggered by the occurrence of an alarm event**

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	Event ID
		Message	(Not applicable)	The value that has been specified in <b>Message</b> in the procedure for issuing JP1 events.
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information Alarm status: OK (The alarm status is Normal (green).)</li> <li>Warning Alarm status: WARNING (The alarm status is Warning (yellow).)</li> <li>Error Alarm status: EXCEPTION (The alarm status is Abnormal (red).)</li> </ul>
		Product name	PRODUCT_NAME	/PFM/ALARM_EVENT
		Object type	OBJECT_TYPE	ALARM
		Object name	OBJECT_NAME	Alarm name
		Registration type	ROOT_OBJECT_TYPE	ALARM_TABLE
		Registration name	ROOT_OBJECT_NAME	Alarm table name
		Object ID	OBJECT_ID	Agent name
		Event type	OCCURENCE	NOTICE
	Specific information	Agent host name	JPC_AGENT	<ul style="list-style-type: none"> <li>In PFM - Agent Host name of PFM - Agent where an alarm was issued</li> <li>In PFM-RM (remote agent) Monitored host name of a remote agent where an alarm was issued</li> <li>In PFM-RM (group agent)</li> </ul>

Attribute type		Item	Attribute name	Content
Extended attribute	Specific information	Agent host name	JPC_AGENT	Primary host name of a group agent where an alarm was issued ( <i>PFM-RM-host-name</i> )
		Manager host name	JPC_MGR	PFM - Manager host name
		Date and time of alarm occurrence	JPC_TIME	Date and time when the alarm occurred
		Displayed report ID	JPC_REPORTID	Report definition ID to be displayed when a JP1 event is selected

## 12.6.2 When Performance Management services start

When a Performance Management service starts, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–7: JP1 system events to be issued when Performance Management services start

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004800
		Message	(Not applicable)	KAVE00335-I message
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information (normal start)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	START
		Starting time	START_TIME	The time when the service started (time when an event is issued)
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	Name of the PFM - Agent host or PFM - RM host that issued the event
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination



## 12.6.3 When Performance Management services stop

When a Performance Management service stops, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–8: JP1 system events to be issued when Performance Management services stop

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004810
		Message	(Not applicable)	KAVE00336-I message (normal termination) KAVE00339-I message (abnormal termination)
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information (normal termination)</li> <li>Error (abnormal termination)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PMF
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	END
		Starting time	END_TIME	The time when the service stopped (time when an event is issued)
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	Name of the PFM - Agent host or PFM - RM host that issued the event
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

## 12.6.4 When the startup of Performance Management services fails

When a startup of Performance Management services fails, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–9: JP1 system events to be issued when the startup of Performance Management services fails

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004820
		Message	(Not applicable)	KAVE00337-E message

Attribute type		Item	Attribute name	Content
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Error (start failed)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	NOTSTART
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	Name of the PFM - Agent host or PFM - RM host that issued the event
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

## 12.6.5 When events for operation occur

When an event for operation occurs, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–10: JP1 system events to be issued when an event for operation occurs

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004830
		Message	(Not applicable)	Service-specific message <sup>#</sup>
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information: Normal status</li> <li>Warning: Error (no action required)</li> <li>Error: Error (action required)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	NOTICE

Attribute type		Item	Attribute name	Content
Extended attribute	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	Name of the PFM - Agent host or PFM - RM host that issued the event
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

#

An applicable message from among the following is output:

- A PFM - Manager message listed in the manual *JP1/Performance Management Reference* (for which a JP1 system event is specified as the destination in the destination list)
- A message listed in the appropriate PFM - Agent or PFM - RM manual (for which a JP1 system event is specified as the destination in the destination list)

## 12.6.6 When agent statuses are changed

If the status of an agent changes, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–11: JP1 system events issued when the status of an agent changes

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004850
		Message	(Not applicable)	One of the following is output: <ul style="list-style-type: none"> <li>• Agent event [Status Change]</li> <li>• KAVE00217-I message (when the status of an agent monitored for alarms changes to Normal)</li> <li>• KAVE00218-W message (when the status of an agent monitored for alarms changes to Warning)</li> <li>• KAVE00219-E message (when the status of an agent monitored for alarms changes to Abnormal)</li> <li>• KAVE00333-E message (when the operating status of an agent changes to Busy or Abnormal End)<sup>#</sup></li> <li>• KAVE00334-I message (when the operating status of an agent recovers from Busy or Abnormal End)</li> </ul>
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>• Information (when the status of an agent monitored for alarms changes to Normal or when the operating status of an agent recovers from Busy or Abnormal End)</li> <li>• Warning (when the status of an agent monitored for alarms changes to Warning)</li> </ul>

Attribute type		Item	Attribute name	Content
Extended attribute	Common information	Severity	SEVERITY	<ul style="list-style-type: none"> <li>Error (when the status of an agent monitored for alarms changes to Error)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM/STATE_EVENT
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID of the agent
		Object ID	OBJECT_ID	Service ID of the agent
		Event type	OCCURENCE	NOTICE
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	<ul style="list-style-type: none"> <li>In PFM - Agent Host name of PFM - Agent where a status is changed</li> <li>In PFM-RM (remote agent) Monitored host name of a remote agent where a status is changed</li> <li>In PFM-RM (group agent) Primary host name of a group agent where a status is changed (PFM RM host name)</li> </ul>
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
Monitor port number		JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination	

#

The Store service detects that the status of the Collector service has changed from active to Busy or Abnormal End. If the Store service has not received a collection event from the Collector service for more than 10 minutes, the Store service sends a heartbeat signal to the Collector service.

If the heartbeat check indicates that the Collector service is in Busy or Stopped status, the Agent Store service or RM Store service generates the JP1 event KAVE00333-E.

## 12.6.7 When the health check status changes

If the health check status changes, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–12: JP1 system events issued when the health check status changes

Attribute type	Item	Attribute name	Content
Basic attribute	Event ID	(Not applicable)	00004860
	Message	(Not applicable)	One of the following is output according to the settings of the health check agent:

Attribute type		Item	Attribute name	Content
Basic attribute		Message	(Not applicable)	<ul style="list-style-type: none"> <li>• KAVL15020-I message (when the setting of a JP1 Event changes to Information)</li> <li>• KAVL15021-W message (when the setting of a JP1 Event changes to Warning)</li> <li>• KAVL15022-E message (when the setting of a JP1 Event changes to Error)</li> </ul>
Extended attribute	Common information	Severity	SEVERITY	One of the following is output according to the settings of the health check agent: <ul style="list-style-type: none"> <li>• Information (when the status of a health check event changes to Normal)</li> <li>• Warning (when the status of a health check event changes to Warning)</li> <li>• Error (when the status of a health check event changes to Error)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>• In Windows: SYSTEM</li> <li>• In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM/HEALTHCHECK_EVENT
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID of the agent
		Object ID	OBJECT_ID	Service ID of the agent
		Event type	OCCURENCE	NOTICE
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	<ul style="list-style-type: none"> <li>• In PFM - Agent Host name of PFM - Agent where a status is changed</li> <li>• In PFM-RM (remote agent) Monitored host name of a remote agent where a status is changed</li> </ul>
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination <sup>#</sup>
Monitor port number		JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination <sup>#</sup>	

#  
When opened from JP1/IM, the main window of PFM - Web Console is displayed.

## 12.6.8 When monitoring is suspended with a host specified

If you suspend monitoring with a host specified, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–13: JP1 system events issued when monitoring is suspended with a host specified

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004870
		Message	(Not applicable)	KAVE00509-I message
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information (when monitoring for the host is suspended correctly)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	HOST
		Object name	OBJECT_NAME	The name of a host for which monitoring is suspended <sup>#</sup>
		Object ID	OBJECT_ID	Not specified
		Event type	OCCURENCE	SUSPEND
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	The name of a host for which monitoring is suspended <sup>#</sup>
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

#

A host name that PFM - Manager identifies is described. If the target host operates with an alias, the alias is described.

## 12.6.9 When monitoring is suspended with an agent specified

If you suspend monitoring with an agent specified, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–14: JP1 system events issued when monitoring is suspended with an agent specified

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004871
		Message	(Not applicable)	KAVE00510-I message
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information (when monitoring for the agent is suspended correctly)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>

Attribute type		Item	Attribute name	Content
Extended attribute	Common information	Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	The name of an agent for which monitoring is suspended (service ID)
		Object ID	OBJECT_ID	The name of an agent for which monitoring is suspended (service ID)
		Event type	OCCURENCE	SUSPEND
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	Host name of an agent for which monitoring is suspended <sup>#</sup>
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

#

A host name that PFM - Manager identifies is described. If the target host operates with an alias, the alias is described.

## 12.6.10 When monitoring is resumed with a host specified

If you resume monitoring with a host specified, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–15: JP1 system events issued when monitoring is resumed with a host specified

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004880
		Message	(Not applicable)	KAVE00511-I message
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information (when monitoring for the host is resumed correctly)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	HOST
		Object name	OBJECT_NAME	The name of a host for which monitoring is resumed <sup>#</sup>
		Object ID	OBJECT_ID	Not specified
		Event type	OCCURENCE	RESUME
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination <sup>#</sup>

Attribute type		Item	Attribute name	Content
Extended attribute	Specific information	Agent host name	JPC_AGENT	The name of a host for which monitoring is resumed <sup>#</sup>
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

#

A host name that PFM - Manager identifies is described. If the target host operates with an alias, the alias is described.

## 12.6.11 When monitoring is resumed with an agent specified

If you resume monitoring with an agent specified, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 12–16: JP1 system events issued when monitoring is resumed with an agent specified

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004881
		Message	(Not applicable)	KAVE00512-I message
Extended attribute	Common information	Severity	SEVERITY	Severity is set. <ul style="list-style-type: none"> <li>Information (when monitoring for the agent is resumed correctly)</li> </ul>
		User name	USER_NAME	<ul style="list-style-type: none"> <li>In Windows: SYSTEM</li> <li>In UNIX: root (user name whose user ID is 0)</li> </ul>
		Product name	PRODUCT_NAME	/HITACHI/JP1/PFM
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	The name of an agent for which monitoring is resumed (service ID)
		Object ID	OBJECT_ID	The name of an agent for which monitoring is resumed (service ID)
		Event type	OCCURENCE	RESUME
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	Host name of an agent for which monitoring is resumed <sup>#</sup>
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

#

A host name that PFM - Manager identifies is described. If the target host operates with an alias, the alias is described.



# 13

## Performance Monitoring Linked with JP1/Service Level Management (JP1/SLM)

This chapter describes the setup needed to link Performance Management with JP1/SLM and the procedures involved in system monitoring from JP1/SLM using Performance Management.

# 13.1 Overview of monitoring linked with JP1/Service Level Management (JP1/SLM)

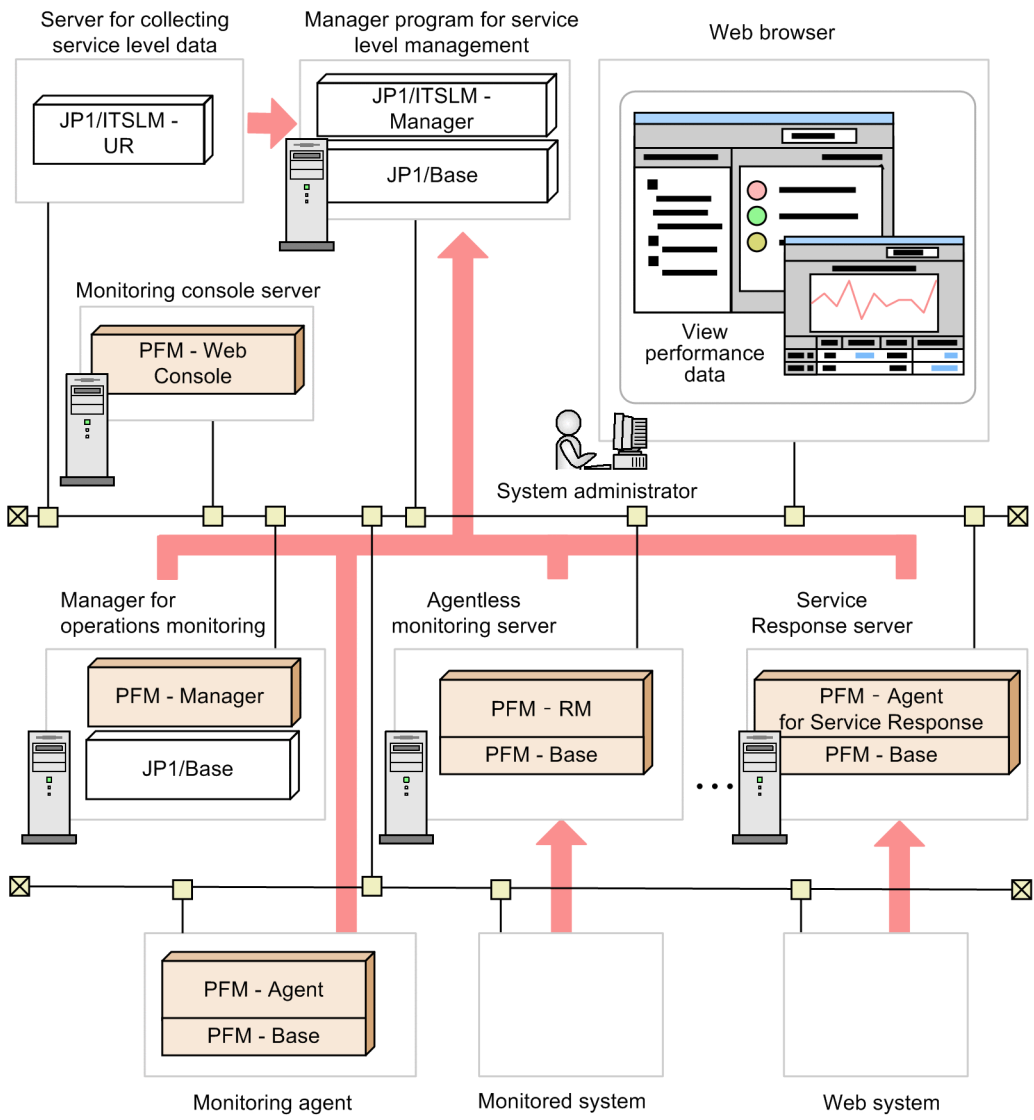
Performance Management can be linked with JP1/SLM for system monitoring.

Using Performance Management, you can analyze collected performance data and identify potential problems. Linking with JP1/SLM allows you to analyze performance data collected by Performance Management, detect signs of irregularities in service performance, and respond to events identified from past monitoring results.

You can also log on to PFM - Web Console as a JP1 user from JP1/SLM.

The following figure shows an example of monitoring with Performance Management linked with JP1/SLM.

Figure 13–1: Example of monitoring with Performance Management linked with JP1/SLM



Legend:

- : Flow of performance data
- : Program provided by Performance Management
- : Program required for linkage provided by another JP1 product

 **Note**

About JP1/SLM

JP1/SLM is a JP1-series product whose purpose is to monitor services so that service levels can be maintained.

An unexpected problem in a widely used or essential service can have major effects on users. JP1/SLM supports service level maintenance in the following ways:

- **Out-of-range value detection**  
A monitoring method that detects marked abnormalities in the service performance of a monitored service as indications of a problem.
- **Trend monitoring**  
A monitoring method that evaluates trends in the service performance of a monitored service and predicts from this data when a performance threshold will be exceeded.
- **Threshold value monitoring**  
A monitoring method that detects a problem when the service performance of a monitored service exceeds a set threshold value, and enables remedial measures based on past monitoring results.

### 13.1.1 Benefits of linking Performance Management with JP1/SLM

#### (1) Use performance data monitored by Performance Management in JP1/SLM monitoring

You can use the performance data monitored by Performance Management in JP1/SLM predictive error detection. Services, servers, and middleware can be linked into the monitoring process, which assists in cause investigation of warnings generated by predictive error detection.

The use of performance data in JP1/SLM threshold monitoring can also help in detecting errors related to services, servers, and middleware. You can use the data when investigating detected errors and preparing error prevention plans.

#### (2) Launch PFM - Web Console from JP1/SLM

When a problem is found or predicted by linking Performance Management with JP1/SLM, you can view the collected performance data in the JP1/SLM Troubleshoot window to find out what happened.

You can also launch PFM - Web Console from the JP1/SLM Troubleshoot window to view other Performance Management information in addition to the service and performance data collected by JP1/SLM.

 **Note**

Troubleshoot window

JP1/SLM displays potential and actual problems related to the set monitoring items as warnings and errors. The Troubleshoot window is for checking the time at which an event that caused a warning or error occurred. You can go back further to check past service performance.

## 13.2 Prerequisites for JP1/SLM linkage

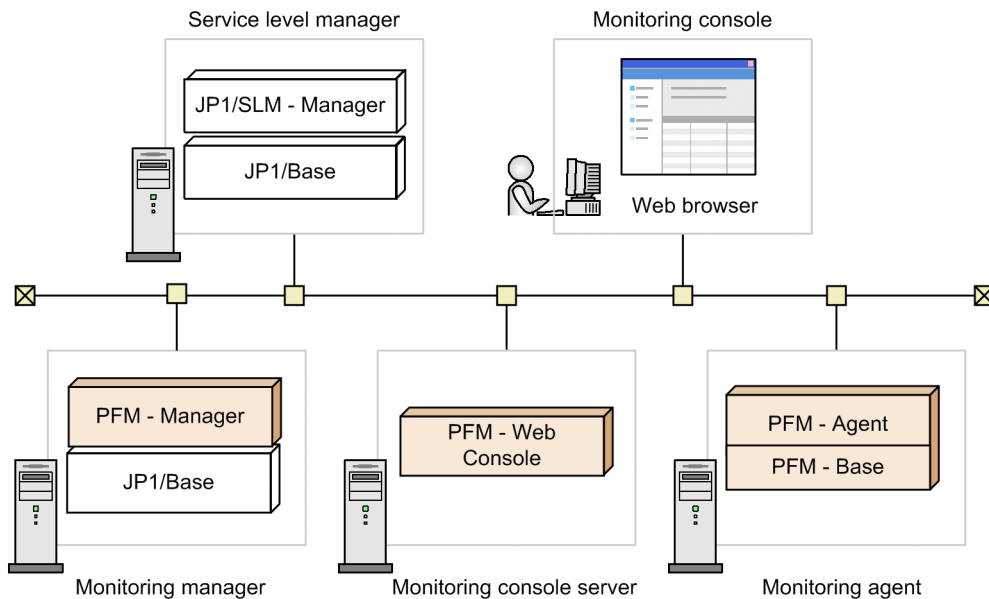
The following describes the prerequisites for linking with JP1/SLM.

### 13.2.1 Programs needed for JP1/SLM linkage



This subsection describes the programs needed to link Performance Management with JP1/SLM.

The following figure shows the required programs.

Figure 13–2: Program configuration for linking with JP1/SLM



Legend:

-  : Program provided by Performance Management
-  : Program required for linkage provided by another JP1 product

- All programs must be version 10-00 or later.  
PFM - Web Console version 09-00 or later will work, but the following operational restrictions apply to versions earlier than 10-00:
  - Record IDs of records collected in the Service Properties window are not displayed in bold type.
  - When you select an agent in JP1/SLM and then launch PFM - Web Console from the JP1/SLM window, that agent will not be highlighted automatically in the PFM - Web Console main window.

### 13.2.2 Number of linked JP1/SLM instances

Only one instance of JP1/SLM can be linked with one PFM - Manager. You must release the linked JP1/SLM if you want to link another JP1/SLM instance to the same PFM - Manager. In a large-scale configuration running multiple instances of JP1/SLM, a separate PFM - Manager is required for each JP1/SLM.

### 13.2.3 User authentication mode and business groups for JP1/SLM linkage

PFM authentication mode or JP1 authentication mode can be used for JP1/SLM linkage.

In JP1 authentication mode, JP1/SLM users and Performance Management users are centrally managed in JP1/Base. The user account is authenticated automatically when a user launches PFM - Web Console from JP1/SLM. Whichever authentication mode you use, you must assign the monitored hosts to business groups. By assigning JP1 resource groups to business groups, you can apply appropriate access controls to individual users.

### 13.2.4 JP1 user authority for JP1/SLM linkage

To link with JP1/SLM, you must assign Performance Management-related permissions to the JP1 user who logs on to JP1/SLM.

You can specify which resources each JP1 user is allowed to access by setting permission levels to JP1 resource groups.

The following JP1 permissions are required for linking to JP1/SLM:

- Administrator user permissions
  - JP1\_PFM\_Admin
  - JP1\_ITSLM\_Admin
- General user permissions
  - JP1\_PFM\_Operator
  - JP1\_ITSLM\_User

The following table describes the JP1 permission levels assigned to JP1 resource groups for specific purposes.

Table 13–1: JP1 permission levels assigned to JP1 resource group by purpose

Purpose	JP1/SLM permission	JP1 resource group	PFM - Manager permissions
JP1/SLM monitoring and settings when linked with JP1/SLM	JP1_ITSLM_Admin	JP1_PFM	JP1_PFM_Admin or JP1_PFM_Operator
		Any group	JP1_PFM_Operator
Launch PFM - Web Console from JP1/SLM	JP1_ITSLM_Admin or JP1_ITSLM_User	JP1_PFM	JP1_PFM_Admin or JP1_PFM_Operator
		Any group	JP1_PFM_Operator

For details on permissions, see [2.6 Setting operating permissions for JP1 users](#) or the chapter that describes Performance Management user setup (working with Performance Management) in the manual *Job Management Partner 1/Service Level Management*.

### 13.2.5 Recording performance data collected when linked with JP1/SLM

The performance data collected by Performance Management is stored by the Agent Collector service or Remote Monitor Collector service on a monitoring agent, and is recorded in the applicable Store database. When you link with JP1/SLM and start monitoring from JP1/SLM, the collected performance data will be sent to JP1/SLM.

In Performance Management, you can specify from the monitoring console or by command whether to record performance data in a Store database. In JP1/SLM, you can specify whether to record performance data by modifying a definition file.

The following table describes the relationship between data recording settings in JP1/SLM and Performance Management.

**Table 13–2: Recording of performance data according to settings in JP1/SLM and Performance Management**

JP1/SLM setting		Performance Management setting	
Start monitoring	Record performance data	Record performance data	
		Yes	No
Yes	Yes	StoreDB + SLM	StoreDB + SLM
	No	StoreDB + SLM	SLM
No		StoreDB	--

Legend:

StoreDB: Stored in a Store database.

SLM: Sent to JP1/SLM for use in predictive detection and analysis.

--: Not stored in a Store database and not sent to JP1/SLM. As a result, no data is collected.



### Note

- Sending of performance data might fail if there is a communication error, for example, or if JP1/SLM has not started and cannot receive the data.

When sending fails, routine data transfer from the applicable PFM - Agent and PFM - RM stops. The system retries every 30 seconds from the measured time at which sending failed until JP1/SLM can be reached.

At retry, the sent performance data includes the original data plus any additional data collected since the transmission failure. However, data older than the time during which JP1/SLM can receive past data (60 seconds) is discarded.

When sending succeeds on retry, routine transfer of performance data from the PFM - Agent and PFM - RM resumes.

- The Collection Interval and Collection Offset settings in Performance Management override settings in JP1/SLM related to the recording of performance data.
- If you edit a custom monitoring item to monitor a specific field only, the entire record containing that field will be stored in the Store database.

For details on settings for recording performance data, see [4.1.1 Modifying the recording options for performance data](#) or the manual *Job Management Partner 1/Service Level Management*.

## 13.2.6 Network settings for JP1/SLM linkage

This subsection describes how to set up port numbers and name resolution for IP addresses to link with JP1/SLM.

## (1) Setting IP addresses

Set host names that can be resolved into an IP address in communications from the JP1/SLM host to the PFM - Manager host, and from PFM - Agent and PFM - RM hosts to the JP1/SLM host. Host names and IP addresses defined in the `jpchosts` file are checked before the standard name resolution method is applied.

### Note

Performance Management supports static NAT with one-to-one IP address mapping.

Dynamic NAT and NAPT (which includes port translation) are not supported.

## (2) Setting port numbers

PFM - Manager and JP1/SLM use the port numbers listed in the table below. The port numbers are assigned by default.

If a firewall is installed, the port numbers in [Table 13-3 Port numbers for JP1/SLM linkage](#) must be open. If the port number being used varies according to a setting in the `httpsd.conf` file or in JP1/SLM, set that port number so that it is open on the firewall.

For details on how to set port numbers, see the chapter that describes changing the network configuration in the *JP1/Performance Management Planning and Configuration Guide*.

The following table lists the available port numbers for JP1/SLM linkage and their purpose.

Table 13–3: Port numbers for JP1/SLM linkage

Purpose	Port number	Direction of traffic
For setting up JP1/SLM linkage. Used by the ViewServer service of PFM - Manager.	22286	From JP1/SLM host to PFM - Manager host
For starting PFM - Web Console from JP1/SLM. Used by the Web Service service of PFM - Web Console.	20358	From Web browser to PFM - Web Console host
For receiving performance data on the JP1/SLM host. Set on the JP1/SLM host.	20905	From PFM - Agent and PFM - RM hosts to JP1/SLM host

## 13.2.7 Monitoring items for JP1/SLM linkage

Two performance items can be monitored from JP1/SLM.

The characteristics of each item are described below.

### (1) Default monitoring items

In a standard setup, JP1/SLM monitors the default monitoring items set in PFM - Agent and PFM - RM.

*Default monitoring items* are defined by default in PFM - Agent and PFM - RM.

These typical monitoring items are defined for each PFM - Agent and PFM - RM type and data model. You can use them like monitoring templates, to begin monitoring immediately with standard settings.

You cannot modify the default monitoring items.

For details on the default monitoring items for PFM - Agent or PFM - RM, see the documentation for these program products.

If you add PFM - Agent and PFM - RM as monitoring targets to PFM - Manager after setup, you must apply the default monitoring items for the monitoring agents that are added.

For details, see *13.4.3 Applying configuration changes in Performance Management after linking with JP1/SLM*.

## **(2) Custom monitoring items**

A *custom monitoring item* is a record field specified and defined by the user when a value not present in the default monitoring items needs to be analyzed in JP1/SLM.

You can define a maximum of 54 custom monitoring items for each PFM - Agent and PFM - RM type and data model.

Use a custom monitoring item when you need to customize a field to satisfy a particular monitoring requirement in Performance Management or JP1/SLM.

Define each custom monitoring item in a PFM - Manager definition file. This file is known as a *definition file for custom monitoring items*.

For details about the definition file for JP1/SLM-linkage custom monitoring items (`monitoringitems.cfg`), see the chapter that describes definition files in the manual *JP1/Performance Management Reference*.



## 13.3 Building a system linked with JP1/SLM

---

This section describes how to build an environment for linking Performance Management with JP1/SLM and how to release linkage with JP1/SLM.

### 13.3.1 Setup for JP1/SLM linkage

#### (1) Setup on the PFM - Manager side

1. Start PFM - Manager.
2. Assign business groups to the hosts to be monitored.
3. Log on to PFM - Web Console from the Web browser of the monitoring console.  
Log on with a user account that has administrator user permissions.
4. In the navigation frame of the main window, select the **Services** tab.
5. In the navigation frame of the Services window, expand the hierarchy under the **PFM - Manager** folder.  
PFM - Manager services are listed by service ID.
6. Select the Master Manager service.  
The Master Manager service is indicated by **M** or **<Master Manager>**.  
The selected Master Manager service is marked with a checkmark.
7. In the method frame, select **Properties**.
8. In the Service Properties window for the Master Manager service, select the **ITSLM Coordination Configuration/MANAGE ITSLSM COORDINATION** node.
9. In **ASSIGN ITSLSM COORDINATION** at the bottom of the information frame, type the JP1/SLM host name to be linked with Performance Management.  
If JP1/SLM is a logical host, specify the logical host name.
10. Click the **Finish** or **Apply** button.

Setup on the JP1/SLM side must be completed before you can start linkage with JP1/SLM.



#### Note

- If you need to link PFM - Manager to a different JP1/SLM instance, you must release the existing linkage first.
- If you are using a custom monitoring item, edit the definition file for custom monitoring items before setting up linkage on the PFM - Manager side.  
For details about custom monitoring items, see [13.2.7\(2\) Custom monitoring items](#) and the chapter that describes definition files in the manual *JP1/Performance Management Reference*.

## (2) Setup on the JP1/SLM side

1. Register the required services on the JP1/SLM host.
2. Register the required service groups on the JP1/SLM host.
3. On the JP1/SLM host, select the service groups to which the services to be monitored belong (JP1 resource group names registered with JP1/Base).
4. On the JP1/SLM host, edit the system definition file (`jp1itslm.properties`) to specify the link settings.
5. Make sure that PFM - Manager is running.
6. Make sure that all instances of PFM - Agent and PFM - RM are running on the monitoring target hosts.
7. Update the configuration information in the JP1/SLM Configuration information settings window.
8. Set monitoring items in the JP1/SLM Monitor settings window.
9. Start monitoring performance data in the JP1/SLM Settings window.

For details on setup on the JP1/SLM side, see the description about setting up monitoring items (working with Performance Management) or starting monitoring in the manual *Job Management Partner 1/Service Level Management*.

### 13.3.2 Releasing linkage with JP1/SLM

You can release the linkage between Performance Management and JP1/SLM by a standard procedure or by a contingency procedure in the event of a problem.

The following describes these two methods and the differences between them.

#### (1) Releasing linkage (standard procedure)

This is the normal way of releasing linkage with JP1/SLM.

In this procedure, you modify properties in the Services window of PFM - Web Console. This deletes PFM - Manager information about linkage with the JP1/SLM host. PFM - Agent and PFM - RM are disconnected from JP1/SLM, and the connection information is deleted.

#### (2) Contingency procedure

Use this procedure to release linkage with JP1/SLM if the standard procedure fails for some reason and PFM - Agent or PFM - RM cannot be released.

##### (a) Synchronizing JP1/SLM connections

You can release multiple instances of PFM - Agent and PFM - RM from JP1/SLM at the same time.

In this procedure, you modify properties in the Services window of PFM - Web Console. This disconnects PFM - Agent and PFM - RM connected to a different JP1/SLM host than the current settings. The connection information is deleted.

##### (b) Disconnecting a JP1/SLM connection

You can release a specified instance of PFM - Agent or PFM - RM.

In this procedure, you modify properties in the Services window of PFM - Web Console. This directly disconnects the specified PFM - Agent or PFM - RM from JP1/SLM. The connection information is deleted.

You can also delete the connection information management file on a particular PFM - Agent or PFM - RM instance.

For details on the PFM - Agent or PFM - RM connection information management file, see the PFM - Agent or PFM - RM documentation.

### 13.3.3 Procedures for releasing linkage with JP1/SLM

To release the linkage between Performance Management and JP1/SLM, you must modify settings on both JP1/SLM and PFM - Manager.

#### (1) Releasing linkage on the JP1/SLM side

1. Make sure that PFM - Manager is running.
2. Make sure that all instances of PFM - Agent and PFM - RM are running on the monitoring target hosts.
3. Delete the monitoring settings in the JP1/SLM Monitor settings window.

For details on the settings on the JP1/SLM side, see the manual *Job Management Partner 1/Service Level Management*.

#### (2) Releasing linkage (standard procedure)

1. Start PFM - Manager.
2. Start all instances of PFM - Agent and PFM - RM on the monitoring target hosts.  
The settings for releasing JP1/SLM linkage will not be applied to inactive instances of PFM - Agent or PFM - RM.
3. Log on to PFM - Web Console from the Web browser of the monitoring console.  
Log on with a user account that has administrator user permissions.
4. In the navigation frame of the main window, select the **Services** tab.
5. In the navigation frame of the Services window, expand the hierarchy under the **PFM - Manager** folder.  
PFM - Manager services are listed by service ID.
6. Select the Master Manager service.  
The Master Manager service is indicated by **M** or **<Master Manager>**.  
The selected Master Manager service is marked with a checkmark.
7. In the method frame, select **Properties**.
8. In the Service Properties window for the Master Manager service, select the **ITSLM Coordination Configuration/MANAGE ITSMLM COORDINATION** node.
9. In **RELEASE ITSMLM COORDINATION** at the bottom of the information frame, select the JP1/SLM host name to be released from linkage with Performance Management.
10. Click the **Finish** or **Apply** button.

Information about monitoring items and connection settings, and cached performance data that was to be sent to JP1/SLM, are discarded on all active instances of PFM - Agent and PFM - RM.

### (3) Contingency procedure

Use this procedure if PFM - Agent or PFM - RM could not be released because an error or other problem occurred during execution of the procedure described in *13.3.3(2) Releasing linkage (standard procedure)*.

To disconnect multiple instances of PFM - Agent and PFM - RM, see *13.3.3(3)(a) Synchronizing JP1/SLM connections*.

To disconnect a single instance of PFM - Agent or PFM - RM, see *13.3.3(3)(b) Disconnecting a JP1/SLM connection*.

#### (a) Synchronizing JP1/SLM connections

1. Start PFM - Manager.
2. Start all instances of PFM - Agent and PFM - RM on the monitoring target hosts.  
The settings for synchronized release will not be applied to inactive instances of PFM - Agent or PFM - RM.
3. Log on to PFM - Web Console from the Web browser of the monitoring console.  
Log on with a user account that has administrator user permissions.
4. In the navigation frame of the main window, select the **Services** tab.
5. In the navigation frame of the Services window, expand the hierarchy under the **PFM - Manager** folder.  
PFM - Manager services are listed by service ID.
6. Select the Master Manager service.  
The Master Manager service is indicated by **M** or **<Master Manager>**.  
The selected Master Manager service is marked with a checkmark.
7. In the method frame, select **Properties**.
8. In the Service Properties window for the Master Manager service, select the **ITSLM Coordination Configuration/MANAGE ITSLM COORDINATION** node.
9. In **SYNCHRONIZE ALL ITSLM CONNECTION** at the bottom of the information frame, select **ALL**.
10. Click the **Finish** or **Apply** button.  
Information about monitoring items and connection settings, and cached performance data that was to be sent to JP1/SLM, are discarded on all active instances of PFM - Agent and PFM - RM.

#### (b) Disconnecting a JP1/SLM connection

Disconnection procedure on the monitoring console

1. Start PFM - Manager.
2. Start the PFM - Agent or PFM - RM that you want to disconnect.  
You cannot disconnect PFM - Agent or PFM - RM if it is stopped.
3. Log on to PFM - Web Console from the Web browser of the monitoring console.  
Log on with a user account that has administrator user permissions.
4. In the navigation frame of the main window, select the **Services** tab.

5. In the navigation frame of the Services window, expand the hierarchy under the **PFM - Manager** folder.  
PFM - Manager services are listed by service ID.
6. Select the Agent Collector service or RM Collector service.  
The selected Agent Collector service or RM Collector service is marked with a checkmark.
7. In the method frame, select **Properties**.
8. In the Properties window for the Agent Collector service or RM Collector service, select the **ITSLM Connection Configuration/MANAGE ITSLSM CONNECTION** node.
9. In **DISCONNECT ITSLSM CONNECTION** at the bottom of the information frame, select the JP1/SLM host name to be disconnected.
10. Click the **Finish** or **Apply** button.  
Information about monitoring items and connection settings, and cached performance data that was to be sent to JP1/SLM, are discarded on the active PFM - Agent or PFM - RM.

#### Disconnection procedure on PFM - Agent or PFM - RM

1. Stop the PFM - Agent or PFM - RM that you want to disconnect.  
You cannot disconnect PFM - Agent or PFM - RM if it is running.
2. Delete the connection information management file (`jpccitslm.ini`) on the PFM - Agent or PFM - RM that you are disconnecting.  
The disconnection information will be applied the next time the inactive PFM - Agent or PFM - RM is started.

For details on the connection information management file on PFM - Agent or PFM - RM, see the PFM - Agent or PFM - RM documentation.

## 13.4 Changing the configuration after linking with JP1/SLM

---

This section describes the setup required to re-establish JP1/SLM linkage if you change the server and middleware configuration or if you create or add a logical host after linking with JP1/SLM.

### 13.4.1 Changing host names after linking with JP1/SLM

The following describes the procedure for changing the physical host name or logical host name of the PFM - Manager host, JP1/SLM host, PFM - Web Console host, PFM - Agent host, or PFM - RM host after linking with JP1/SLM.

For details on the standard procedure to change a host name in Performance Management, see the relevant chapter in the manual *JP1/Performance Management Planning and Configuration Guide*. If you are running a cluster system, see *10.3.3 Changing logical host names after starting operation* or *10.5.3 Changing logical host names after starting operation* in this manual.

#### (1) Changing the host name of PFM - Manager

1. Use the standard procedure to change the PFM - Manager host name.
2. Change the PFM - Manager host name in JP1/SLM.  
Perform the setup so that the new host name can be resolved from the JP1/SLM host.  
For details on changing the PFM - Manager host name in JP1/SLM, see the chapter that describes this procedure in the manual *Job Management Partner 1/Service Level Management*.

If you are using a definition file for custom monitoring items and a health check agent is linked with JP1/SLM, you must complete the task described in *13.4.1(4) Changing the host names of PFM - Agent and PFM - RM*.

#### (2) Changing the host name of JP1/SLM

1. Use the standard procedure to change the JP1/SLM host name.  
For details on the standard procedure to change a host name in JP1/SLM, see the relevant chapter in the manual *Job Management Partner 1/Service Level Management*.
2. In PFM - Manager, release linkage with the host on which JP1/SLM is running.
3. In PFM - Manager, set up linkage with the new JP1/SLM host.
4. In PFM - Agent and PFM - RM, set the new JP1/SLM host name.  
Perform the setup so that the new JP1/SLM host name can be resolved from all PFM - Agent and PFM - RM hosts in the linkage relationship.
5. In JP1/SLM, restart monitoring on all target hosts running PFM - Agent or PFM - RM.

For details about releasing and establishing linkage, see *13.3.3 Procedures for releasing linkage with JP1/SLM* and *13.3.1 Setup for JP1/SLM linkage*.

#### (3) Changing the host name of PFM - Web Console

1. Use the standard procedure to change the PFM - Web Console host name.
2. Change the PFM - Web Console host name in JP1/SLM.

Perform the setup so that the new PFM - Web Console host name can be resolved from the host on which you access the Web browser.

For details on changing the PFM - Web Console host name in JP1/SLM, see the chapter that describes this procedure in the manual *Job Management Partner 1/Service Level Management*.

## (4) Changing the host names of PFM - Agent and PFM - RM

Monitoring items set in JP1/SLM are not retained when you change a PFM - Agent or PFM - RM host name. For this reason, after changing a host name you must set up monitoring again in JP1/SLM, as follows:

1. Start PFM - Agent and PFM - RM on the target host.
2. In JP1/SLM, stop monitoring on the target PFM - Agent or PFM - RM host you intend to change.
3. Use the standard procedure to change the PFM - Agent or PFM - RM host name.
4. Update the configuration information in JP1/SLM.  
The previous PFM - Agent or PFM - RM information is deleted and the updated PFM - Agent or PFM - RM information appears.
5. In JP1/SLM, set monitoring information for the changed PFM - Agent or PFM - RM host.
6. In JP1/SLM, start monitoring on the new PFM - Agent or PFM - RM host.

If you proceed through these steps without stopping monitoring at step 2, you must disconnect PFM - Agent or PFM - RM from the monitoring console and re-execute step 6. If you skipped step 2 and executed step 3, complete the remaining three steps after disconnecting PFM - Agent or PFM - RM.

For details on JP1/SLM disconnection, see [13.3.3\(3\)\(b\) Disconnecting a JP1/SLM connection](#).

## (5) Process flow for changing a monitoring host name

1. Update the configuration information in JP1/SLM.

In PFM - Manager, change the business group settings for the new host if necessary.

## 13.4.2 Creating or deleting a PFM - Manager logical host after linking with JP1/SLM

You can link Performance Management with JP1/SLM even when the PFM - Manager is a logical host.

Linkage information is not inherited by the physical or logical host when you create or delete the PFM - Manager logical host after linking with JP1/SLM.

The following describes the setup required in Performance Management when you create or delete a PFM - Manager logical host.

### (1) When a logical host is created

- Information held by the physical host  
The settings for JP1/SLM linkage are invalidated. Set up linkage between PFM - Manager and JP1/SLM again.

You must also set the required configuration information and monitoring items in JP1/SLM.

- Information held by the logical host

The linkage information for the physical host is not inherited. Set up linkage between PFM - Manager and JP1/SLM.

You must also set the required configuration information and monitoring items in JP1/SLM.

## **(2) When a logical host is deleted**

- Information held by the physical host

The linkage information held by the logical host is not transferred to the physical host.

### **13.4.3 Applying configuration changes in Performance Management after linking with JP1/SLM**

If you make any of the following changes after linking with JP1/SLM, you must perform settings in JP1/SLM to apply the new configuration information:

- Add or delete a business group
- Add or delete PFM - Agent or PFM - RM
- Add or delete a monitoring target host
- Add or delete a monitoring item

If you do not apply the new configuration information in JP1/SLM, the configuration information held by JP1/SLM will be inconsistent with the information in PFM - Manager. An existing host might be missing from the configuration information displayed in JP1/SLM, or the JP1/SLM information might include a host that is inoperable because it has been deleted.

For details, see the chapters about setting monitoring items and setting configuration information for monitored services (working with Performance Management) in the manual *Job Management Partner 1/Service Level Management*.



## 13.5 Operations when linking with JP1/SLM

---

### 13.5.1 Starting monitoring from JP1/SLM

To start monitoring from JP1/SLM, you must perform the start procedure in the JP1/SLM Settings window.

### 13.5.2 Stopping monitoring from JP1/SLM

To change the monitoring item settings after starting monitoring from JP1/SLM, you must stop monitoring of the affected services.

Stop monitoring in the JP1/SLM Settings window.

### 13.5.3 Monitoring performance data in JP1/SLM

#### (1) Home window

In the Home window, you can check the status of all monitored services. Monitored services that have error or warning status are displayed in the **Caution service** area.

#### (2) Real-time Monitor window and Troubleshoot window

In these windows you can trace back through past service performance data to find out what caused a **Caution service** listing, and display the performance data and service performance at the time of the alert as a table or chart.

Results are shown hierarchically in the JP1/SLM windows, with a separate hierarchical level for each monitoring agent that collected the data.

### 13.5.4 Starting PFM - Web Console from JP1/SLM

You can launch PFM - Web Console from JP1/SLM to view information other than the performance data collected by JP1/SLM.

1. In the JP1/SLM Troubleshoot window, click **Log in to PFM**.

The displayed window differs according to which Performance Management authentication mode you are using.

If you are using PFM authentication mode or JP1 authentication mode without access permissions for Performance Management:

The Login window of PFM - Web Console appears.

If you are using JP1 authentication mode (with access permissions for Performance Management):

You are authenticated automatically as the logged-on JP1/SLM user, and the PFM - Web Console window appears.

The full range of Performance Management functions are available when you log on to PFM - Web Console from JP1/SLM. However, restrictions may apply depending on your user account, just as when not linked with JP1/SLM.

In the navigation frame of the PFM - Web Console main window, the agent selected in JP1/SLM will be highlighted and the tree display will depend on general-user operational restrictions on agent levels and on the permission level of the logged-on user.

### 13.5.5 Synchronizing monitoring settings after backing up and restoring PFM - Manager or JP1/SLM

If you back up and restore JP1/SLM or PFM - Manager, you must manually synchronize their respective monitoring settings.

To synchronize monitoring settings:

1. Start PFM - Manager.
2. Start JP1/SLM and log on.
3. Update the configuration information in the JP1/SLM Configuration information settings window.  
Synchronize the configuration information and monitoring items between PFM - Manager and JP1/SLM.
4. This step is required only when restoring JP1/SLM. Check the monitoring settings and whether monitoring is ON or OFF in the JP1/SLM Monitor settings window.

Check the following:

- Monitoring (ON or OFF) of monitoring items  
The node color indicates ON or OFF. Make sure that:  
Nodes that are supposed to be ON are not set to OFF.  
Nodes that are supposed to be OFF are not set to ON.
  - Monitoring settings for monitoring items:  
Make sure that the threshold values and predictive error detection settings for ON nodes are correct.
5. In the Start/Stop monitor window, synchronize the monitored status (**Start** or **Stop**) and monitoring settings with PFM - Manager.  
Set as follows according to whether each service is being monitored:
    - Service being monitored  
Start service monitoring and update PFM - Manager with the latest monitoring settings in JP1/SLM.
    - Service not being monitored  
Stop service monitoring and stop monitoring by PFM - Manager.

For details on the JP1/SLM operations, see the manual *Job Management Partner 1/Service Level Management*.

# 14

## Monitoring Linked with JP1/AJS3

This chapter describes operation monitoring by linking Performance Management with JP1/AJS3. The chapter covers the setup procedure for linking Performance Management with JP1/AJS3, and describes how to monitor a system by using Performance Management from JP1/AJS3.

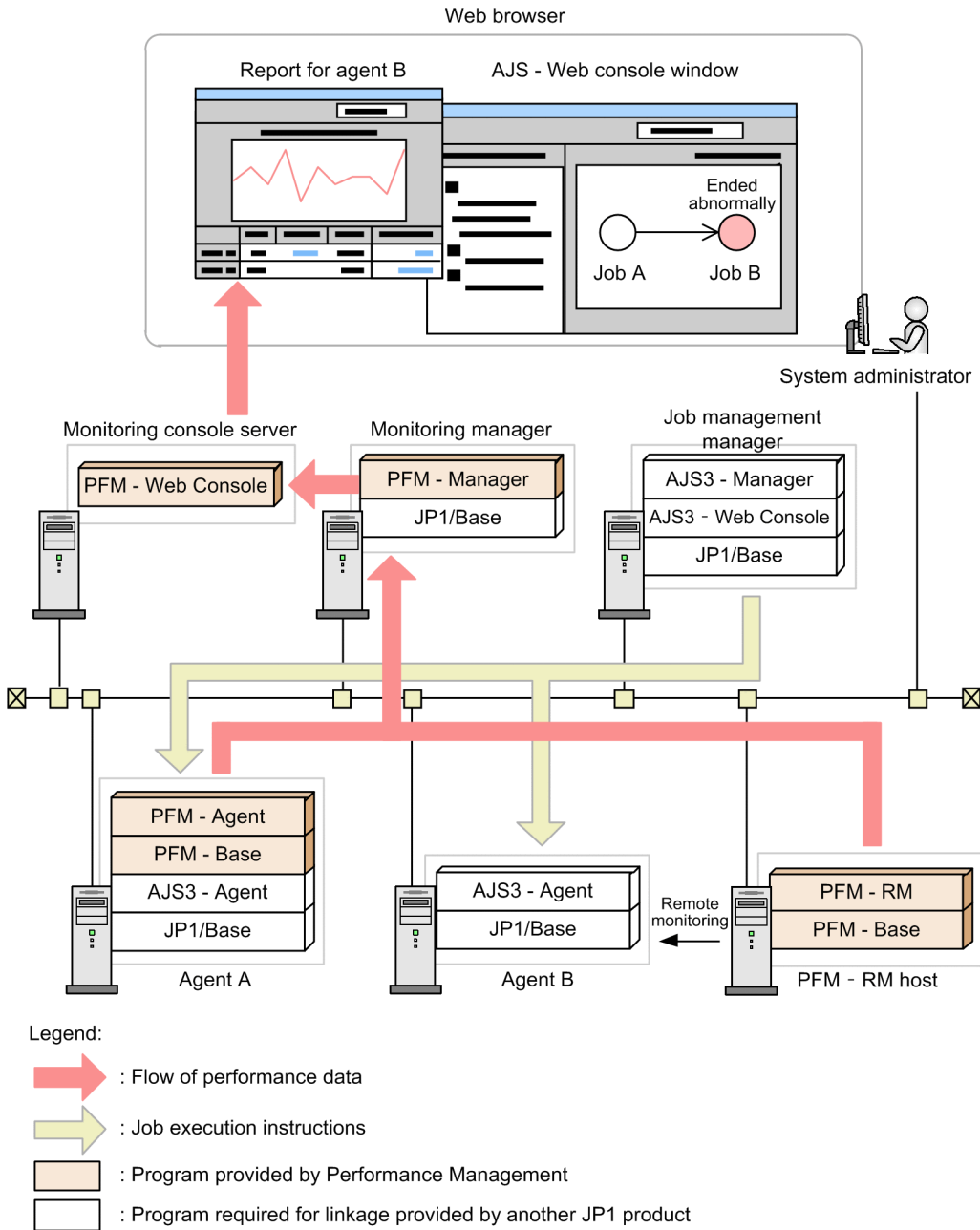
# 14.1 Overview of monitoring linked with JP1/AJS3

Performance Management can be linked with JP1/AJS3 for system monitoring.

Using Performance Management, you can check reports in which performance data collected from the monitoring targets is displayed in graphs and tables in an easy-to understand format. Linking with JP1/AJS3 allows you to directly display and check reports about the JP1/AJS3 execution agent (agent host) from a JP1/AJS3 window.

The following figure shows an example of monitoring with Performance Management linked with JP1/AJS3.

Figure 14–1: Example of monitoring with Performance Management linked with JP1/AJS3



## Note

About JP1/AJS3

JP1/AJS3 is a JP1-series product whose purpose is to automate regular and routine applications.

JP1/AJS3 allows you to automatically process multiple applications by defining the steps in the applications and their order of execution. Because you can define the time at which an application starts or define that an application is to start when a specific event occurs, complex applications can also be automated.

Automating applications with JP1/AJS3 provides the following benefits:

- Fewer operators are needed to run applications.  
Even if hosts are distributed in different locations, applications can run automatically and they can be operated and monitored from a single host. Thus, just a few operators are needed to run applications, which reduces costs and enables effective use of human resources.
- Reducing human error improves the reliability of operations.  
Routine tasks can be automated, reducing the risk of operator error.
- Errors can be handled promptly without a resident administrator.  
You can automate error handling procedures. For example, you can define a process to be performed only in the event of an error, or automatically send email if an error occurs. Thus, prompt error handling is possible even if an administrator is not resident.

### 14.1.1 Benefits of linking Performance Management with JP1/AJS3

Linking Performance Management with JP1/AJS3 allows you to directly display and check a report for the JP1/AJS3 execution agent (agent host) from a JP1/AJS3 window.

If a JP1/AJS3 job is delayed or terminates abnormally, a possible cause is degraded performance of the execution agent. You can view a report about the execution agent from the JP1/AJS3 window to check for performance information pertaining to a delay or abnormal termination of a job.

Note that the following reports cannot be displayed:

- Reports using target performance data that is collected with the **Do not save** setting enabled
- Reports that exceed the retention period for the target performance data

To display these reports, you need to change the settings for performance data. For details on how to specify settings for performance data, see the section that describes the management functionality for performance data and steps to specify settings in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

## 14.2 Prerequisites for linking with JP1/AJS3

The following prerequisite conditions must be satisfied to link Performance Management with JP1/AJS:

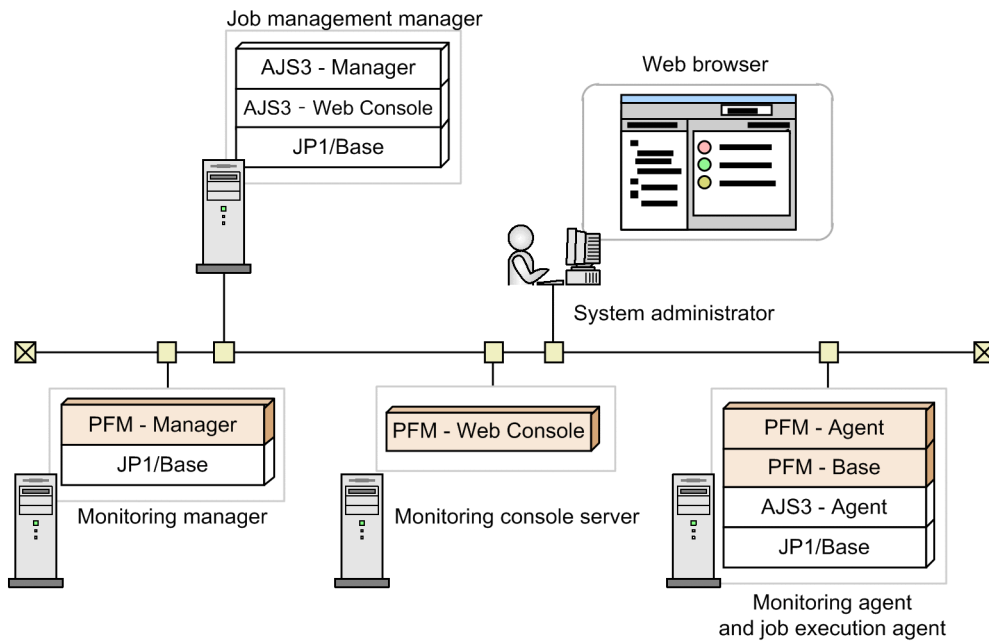
- The PFM - Manager host must have JP1/Base installed in order to log on to Performance Management as a JP1 user. Use JP1/Base to manage users.
- JP1 authentication mode must be used.
- The environment must allow you to establish a connection with PFM - Web Console from the host by which you are logged in to JP1/AJS3 - Web Console.
- PFM - Agent or PFM - RM must be monitoring the execution agents in the JP1/AJS3 system.  
To display an OS performance report for an execution agent, PFM - Agent for Platform or PFM - RM for Platform must be monitoring the agent.
- If the actual host name is used as the monitoring host name, and the result of the `uname -n` command differs from the result of the `hostname` command, take either of the following actions:
  - Change the method for acquiring the host name to `hostname`.
  - Configure the environment for monitored hosts so that the `uname -n` command and `hostname` command provide the same execution result.
- The name of the JP1/AJS3 execution host must match the monitoring host name in Performance Management. Names are case sensitive.
- If JP1/AJS3 - Manager and JP1/AJS3 - Agent run on a logical host, the name of that logical host must match the monitoring host name of JP1/PFM - Agent or JP1/PFM - RM used for monitoring.
- To link with JP1/AJS3, the following product versions are required.

No.	Product name		Version
1	JP1/Automatic Job Management System 3	JP1/AJS3 - Manager	11-00 or later
2		JP1/AJS3 - Agent	09-00 or later
3		JP1/AJS3 - Web Console	11-10 or later
4	JP1/Base	JP1/Base	11-00 or later <sup>#</sup>
5	JP1/Performance Management	JP1/PFM - Web Console	11-10 or later <sup>#</sup>

#  
If you are running multiple Performance Management systems, the products in all the Performance Management systems must have these versions or later. If an earlier-version product is included, reports might not be displayed because of unsuccessful connection with the PFM - Web Console instance for which reports are to be displayed.

The following figure shows the installation configuration.

Figure 14–2: Installation configuration for linking with JP1/AJS3



Legend:

- : Program provided by Performance Management
- : Program required for linkage provided by another JP1 product

## 14.3 Building a system linked with JP1/AJS3

This section describes how to build an environment for linking Performance Management with JP1/AJS3 and how to release linkage with JP1/AJS3.

### 14.3.1 Setup for linking with JP1/AJS3

1. Open the JP1/AJS3 - Web Console environment-settings file (`ajs3web.conf`), and then specify the URL for logging in to PFM - Web Console at the connection destination.

For the `PFM_URL` label, specify the URL with which you can log on correctly.

For example, if the communication protocol is `http`, and PFM - Web Console for the connection destination has the host name `PFM-WebCon` and port number `20358`, specify as follows:

```
; []
;HNTR_LOG_LEVEL=info
;HNTR_LOG_LANG=system
;SYS_LOG_LEVEL=info
;SYS_LOG_LANG=system
;COM_LOG_SIZE=128
;COM_LOG_LEVEL=info
;COM_LOG_NUM=2
;COM_LOG_LANG=system
;SERVER_LOG_SIZE=8192
;SERVER_LOG_LEVEL=info
;SERVER_LOG_NUM=2
PFM_URL=http://PFM-WebCon:20358/PFMWebConsole/login.do
```

2. If PFM - Web Console instances other than the one specified in the environment-settings file in step 1 also monitor the execution agent, edit the initialization file (`config.xml`) on the PFM - Web Console host.

Items to edit

`host`, `port`, and `https` under the `<search-WebConsole>` tag under the `<vsa>` tag

Editing method

Define the host name, port number, and encrypted communication setting for an PFM - Web Console instance not specified in the environment-settings file. To define multiple instances of PFM - Web Console, define the `<search-WebConsole>` tag for the number of instances of PFM - Web Console.

Example of a definition

```
<vsa>
  <search-WebConsole>
    <param name="host" value="PFMWebCon2"/>
    <param name="port" value="20358"/>
    <param name="https" value="ON"/>
  </search-WebConsole>
  <search-WebConsole>
    <param name="host" value="PFMWebCon3"/>
    <param name="port" value="20358"/>
    <param name="https" value="OFF"/>
  </search-WebConsole>
</vsa>
```



### Important

For `https`, specify a value that matches the communication protocol specified in the JP1/AJS3 - Web Console environment-settings file (`ajs3web.conf`). If a different value is specified, the browser's security warning is displayed in the window.

If the browser is Firefox, even if you attempt to continue the operation in the window with the security warning, access will be blocked due to mixed content blocking. To continue the operation, disable mixed content blocking in Firefox.

3. Restart the JP1/AJS3 - Web Console service.
4. Restart the PFM - Web Console service.

## 14.3.2 Releasing linkage with JP1/AJS3

1. In the environment-settings file (`ajs3web.conf`), comment out the items `PFM_URL` and `HOSTNAME_ALIAS_FOR_PFM`, which were edited during setup.
2. Restart the JP1/AJS3 service.
3. If a report for multiple instances of PFM - Web Console is displayed from the JP1/AJS3 window, comment out or delete the `<search-WebConsole>` tags in the initialization file (`config.xml`), and then restart the PFM - Web Console service.

## 14.4 Changing the configuration after linking with JP1/AJS3

---

This section describes the settings required to change a host name after Performance Management is linked with JP1/AJS3.

### 14.4.1 Changing a host name after linking with JP1/AJS3

For details about how to change a host name after linking with JP1/AJS3, see the chapter describing how to change a physical host name in the *JP1/Performance Management Planning and Configuration Guide*.

If you are running a cluster system, see [10.3.3 Changing logical host names after starting operation](#) or [10.5.3 Changing logical host names after starting operation](#) in this manual.

If the monitoring host name specified in Performance Management differs from the actual host name, perform the following in addition to the standard procedure.

#### **If the monitoring host name of the job execution host differs from the actual host name:**

1. Specify the settings in the `jp1hosts` information file or `jp1hosts2` information file on the JP1/AJS3 - Manager host so that the monitoring host name of the target JP1/AJS3 - Agent host can be resolved.  
For details about the `jp1hosts` information file and `jp1hosts2` information file, see the *JP1/Base User's Guide*.
2. Change the execution agent name in the execution agent definition so that jobs can be executed with the monitoring host name.  
For details on the execution agent definition of the JP1/AJS3 - Manager host, see the *JP1 Version 11 JP1/Automatic Job Management System 3 Configuration Guide*.

#### **If the monitoring host name of the JP1/AJS3 - Manager host differs from the actual host name:**

1. In the environment settings file (`ajs3web.conf`) of the JP1/AJS3 - Manager host, set `HOSTNAME_ALIAS_FOR_PFM` to the monitoring host name of the Performance Management instance that is monitoring the JP1/AJS3 - Manager host.  
Note that you must define `HOSTNAME_ALIAS_FOR_PFM` for each connectiondestination JP1/AJS3 - Manager host that is to be specified when you log in to JP1/AJS3 - Web Console.  
For details on the environment settings file (`ajs3web.conf`) of the JP1/AJS3 - Manager host, see the *JP1 Version 11 JP1/Automatic Job Management System 3 Configuration Guide*.

### 14.4.2 Changing an IP address after linking with JP1/AJS3

For details about how to change an IP address after linking with JP1/AJS3, see the chapter describing how to change IP address settings in the *JP1/Performance Management Planning and Configuration Guide*.

## 14.5 Operations when linking with JP1/AJS3

---

This section describes the operations when Performance Management is linked with JP1/AJS3.

### 14.5.1 Displaying Performance Management reports from the monitor window of JP1/AJS3 - Web Console

1. In the Dashboard window of JP1/AJS3 - Web Console, select a job unit, and then click the **Monitor** button.
2. In the Monitor dialog box, select the job for which you want to display a report, and then click **Detail**.
3. In the Detail Information dialog box, click the **Open PFM Report** button.  
A window of PFM - Web Console appears.
4. If the window for switching to PFM - Web Console appears, click the **Select Reports** button for JP1/AJS3 - Agent or JP1/AJS3 - Manager.
5. In the Select Report window, select the type of report you want to display.  
The report for the execution agent appears.



#### Note

The window that appears after you click the **Open PFM Report** button depends on the Performance Management authentication mode and the permission level of the login user.

## 14.6 Notes on linking with JP1/AJS3

---

- If the time setting on the host differs between JP1/AJS3 and Performance Management, the report display period is determined based on the time information for JP1/AJS3. We recommend that you match the host time settings for both JP1/AJS3 and Performance Management beforehand in order to prevent reports from being displayed in an unintended range.
- After starting PFM - Web Console from JP1/AJS3, if you restart PFM - Web Console from JP1/AJS3, an error occurs in the window that opened first. Then, the message (KAVJS0025-E) appears. If you want to open the window that opened first, close all PFM - Web Console windows, and then open the report again from the JP1/AJS3 window.

# 15

## Monitoring Linked with the IT Service Management Product (JP1/Service Support)

This chapter describes operation monitoring by linking Performance Management with JP1/SS. The chapter covers the setup procedure for linking Performance Management with JP1/SS, and describes how to monitor a system by using Performance Management from JP1/SS.

## 15.1 Overview of monitoring linked with JP1/SS

---

Performance Management can be linked with JP1/SS for system monitoring.

Using Performance Management, you can check reports in which performance data collected from the monitoring targets is displayed in graphs and tables in an easy-to-understand format.

When Performance Management is linked with JP1/SS, you can view reports about the host on which a problem occurred from the JP1/SS interface. To do so, you need to use JP1/IM - Manager to register JP1 event information and PFM - Web Console URLs as Items in JP1/SS.



### Note

About JP1/SS

JP1/SS has its conceptual basis in ITIL (Information Technology Infrastructure Library) practices, and was developed with the goal of reducing the workload and improving the efficiency of service support operations in the context of IT service management. ITIL is a set of guidelines seeing widespread adoption, especially in Europe, that systematize the building and operation of IT systems.

The features of JP1/SS allow its users to visualize the flow of system construction and operation in an ITIL context, and lets specialists engaged in the construction and operations of the system share information about the work they perform. You can also exercise control over information sharing by using access permissions to limit the information available to each user.

### 15.1.1 Benefits of linking Performance Management with JP1/SS

Linking Performance Management with JP1/SS, you can view reports about the hosts on which problems occurred, which are recorded in Items registered in JP1/SS, directly from the JP1/SS interface.

By viewing these reports from the JP1/SS interface, you can investigate whether the problems are caused by performance issues.

Note that the following reports cannot be displayed:

- Reports using target performance data that is collected with the **Do not save** setting enabled
- Reports that exceed the retention period for the target performance data

To display these reports, you need to change the settings for performance data. For details on how to specify settings for performance data, see the section that describes the management functionality for performance data and steps to specify settings in the *JP1/ Performance Management Planning and Configuration Guide*.

## 15.2 Prerequisites for linking with JP1/SS

---

The following prerequisite conditions must be satisfied to link Performance Management with JP1/SS:

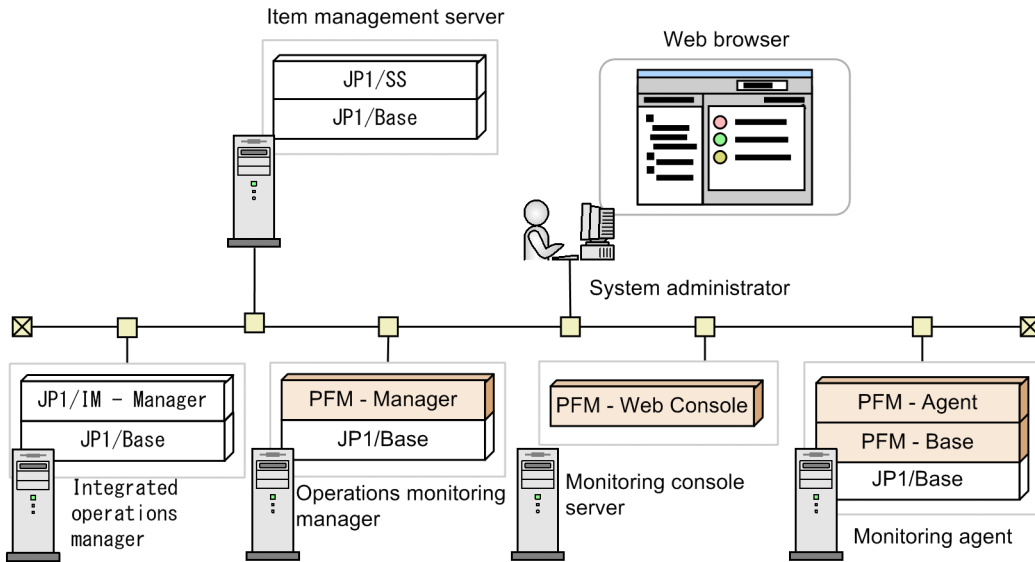
- The PFM - Manager host must have JP1/Base installed in order to log on to Performance Management as a JP1 user. Use JP1/Base to manage users.
- JP1 authentication mode must be used.
- If the OS of a monitored host is UNIX, the actual host name is used as the monitoring host name in Performance Management. The result of the `uname -n` command must match the result of the `hostname` command. If it does not, take either of the following actions:
  - Change the method for acquiring the host name to `hostname`.
  - Configure the environment for monitored hosts so that the `hostname` command and `uname -n` command produce the same output.
- The name of the event server that issues a JP1 event must match the name of the monitoring host in Performance Management. Names are case sensitive.
- When a JP1 event is issued, Agent must be monitoring the host on which the problem occurred.
- To link with JP1/SS, the following product versions are required.

No.	Product name		Version
1	JP1/Service Support	JP1/SS	11-10 or later
2	JP1/Integrated Management - Manager	JP1/IM	09-00 or later
3	JP1/Base	JP1/Base	09-00 or later <sup>#</sup>
4	JP1/Performance Management	JP1/PFM - Web Console	11-10 or later <sup>#</sup>

#  
If you are running multiple Performance Management systems, the products in all the Performance Management systems must have these versions or later. If an earlier-version product is included, reports might not be displayed because of unsuccessful connection with the PFM -Web Console instance for which reports are to be displayed.

The following figure shows the installation configuration.

Figure 15–1: Installation configuration for linking with JP1/SS



Legend:

- : Program provided by Performance Management
- : Program required for linkage provided by another JP1 product



## 15.3 Building a system linked with JP1/SS

This section describes how to build an environment for linking Performance Management with JP1/SS and how to release linkage with JP1/SS.

### 15.3.1 Setup for linking with JP1/SS

1. Open the JP1/SS system property file (`hptl_jp1_imss_main_setting.properties`), and then specify the appropriate values for the settings in the following table.

Table 15–1: Settings to be specified in the JP1/SS system property file

Specification key	Value
<code>hptl_jp1_imss_add_item_info_url_num</code>	The number of URLs to which you want to add Item information <sup># 1</sup>
<code>hptl_jp1_imss_add_item_info_product_\$n</code>	<code>jp1_pfm</code>
<code>hptl_jp1_imss_add_item_info_url_\$n</code>	<i>the URL for logging on to PFM - Web Console</i>
<code>hptl_jp1_imss_add_item_info_\$n<sup>#2</sup></code>	Specify the following three values, separated by commas: <ul style="list-style-type: none"><li>• <code>JIMSD_LOGIN_USER_ID</code> (The element ID that inherits the login user ID)</li><li>• <i>element-ID-that-inputs-the-name-of-the-host-on-which-the-event-occurred</i></li><li>• <i>element-ID-that-inputs-the-date-and-time-when-the event-occurred</i></li></ul>

#1

If you have already specified the number of URLs to which you want to add Item information, add 1 to the previously specified value, and then save the settings.

#2

If you specify the same element ID more than once, Performance Management cannot link with JP1/SS.

If this happens, a login window appears when you attempt to start PFM - Web Console from JP1/SS. Correct the settings and try again.

In the above elements, for `$n`, specify a numeric value from 1 to the value specified for the specification key `hptl_jp1_imss_add_item_info_url_num`. You must specify the same number for `$n` in all of these elements.

For details on the JP1/SS system property file, see the JP1/Service Support manuals.

Example settings:

For example, suppose that you want to use one linkage product (Performance Management) with JP1/SS. The communication protocol used for *the URL for*

*logging on to PFM - Web Console* is HTTP, the host name is PFM-Web Console, and the port number to be used to connect with PFM - Web Console is 20358. Furthermore, the element ID that inputs the name of the host on which the event occurred is "User-added text element 1" (ID: `JIMSD_FORM_USERTEXT01`), and the element ID that inputs the date and time when the event occurred is "Occurrence date and time" (ID:

`JIMSD_FORM_ACCRUALDATE`). To set up linkage with JP1/SS under these conditions, specify the settings as follows:

```
#Other Products Cooperation
#hptl_jp1_imss_jp1_aim=
hptl_jp1_imss_add_item_info_url_num=1
hptl_jp1_imss_add_item_info_url_1=http://PFM-WebCon:20358/PFMWebConsole/
login.do
#hptl_jp1_imss_np_item_info_$n=
#hptl_jp1_imss_ao_item_info_$n=
hptl_jp1_imss_add_item_info_1=JIMSD_LOGIN_USER_ID,JIMSD_FORM_USERTEXT01,JI
MSD_FORM_ACCRUALDATE
hptl_jp1_imss_add_item_info_product_1=jp1_pfm
```

```
#hptl_jp1_imss_add_item_info_key_list_$p=  
hptl_jp1_imss_jp1base_virtual_hostname=JP1_DEFAULT
```

## 2. Set up Single Sign-On.

In JP1/SS, configure the environment to enable Single Sign-On.

For details, see the JP1/SS documentation.

## 3. Edit the initialization file (`config.xml`) for the PFM - Web Console host specified in the JP1/SS system property file. Only perform this step if the host on which the problem occurred is being monitored in JP1/IM from a different instance of PFM - Web Console than the one you specified in the JP1/SS system property file in step 1.

### Items to edit

host, port, and https under the `<search-WebConsole>` tag under the `<vsa>` tag

### Editing method

Define the host name, port number, and encrypted communication setting for an instance of PFM - Web Console instance not specified in the JP1/SS system property file. To define multiple instances of PFM - Web Console, define the `<search-WebConsole>` tag for the number of instances of PFM - Web Console.

### Example of a definition

```
<vsa>  
  <search-WebConsole>  
    <param name="host" value="PFMWebCon2"/>  
    <param name="port" value="20358"/>  
    <param name="https" value="ON"/>  
  </search-WebConsole>  
  <search-WebConsole>  
    <param name="host" value="PFMWebCon3"/>  
    <param name="port" value="20358"/>  
    <param name="https" value="OFF"/>  
  </search-WebConsole>  
</vsa>
```

### Important

The value specified for the parameter `https` must match the communication protocol specified in the JP1/SS system property file. If they do not match, a browser security warning appears in the interface.

## 4. Use JP1/IM to map the host on which the problem (which triggered the JP1 event) occurred to the event-issuing event server.

This setting is required if the problem that triggered the JP1 event registered as an Item in JP1/SS occurred on a host that is not the event-issuing event server.

For details, see the *JP1/Integrated Management - Manager Configuration Guide*.

## 5. Restart the JP1/SS service.

## 6. Restart the PFM - Web Console service.

## 15.3.2 Releasing linkage with JP1/SS

1. In the JP1/SS system property file (`hptl_jp1_imss_main_setting.properties`), comment out the settings you edited during the setup process.

Comment out the following elements (specification keys):

- `hptl_jp1_imss_add_item_info_product_$n`
- `hptl_jp1_imss_add_item_info_url_$n`
- `hptl_jp1_imss_add_item_info_$n`

2. Restart the JP1/SS service.

3. If a report for multiple instances of PFM - Web Console is displayed from the JP1/SS window, comment out or delete the `<search-WebConsole>` tags in the initialization file (`config.xml`), and then restart the PFM - Web Console service.

## 15.4 Changing the configuration after linking with JP1/SS

---

This section describes the settings required to change a host name after Performance Management is linked with JP1/SS.

### 15.4.1 Changing a host name after linking with JP1/SS

To change a host name after linking with JP1/SS, you need to perform the following steps in addition to the usual procedure for changing the physical PFM -Web Console host.

Note that you must perform these steps after the PFM - Web Console service starts.

1. Change the PFM -Web Console host name specified in the JP1/SS system property file.
2. Restart the JP1/SS service.

For details on the procedure for changing the physical PFM - Web Console host, see the chapter describing how to change a physical host name in the *JP1/Performance Management Planning and Configuration Guide*.

If you are running a cluster system, see [10.3.3 Changing logical host names after starting operation](#) or [10.5.3 Changing logical host names after starting operation](#) in this manual.

If the monitoring host name specified in Performance Management differs from the actual host name, perform the following in addition to the standard procedure. In this case, you also need to set the Performance Management monitoring host name to match the event server name of the host on which the problem occurred, as recorded in the JP1 event.

### 15.4.2 Changing an IP address after linking with JP1/SS

For details about how to change an IP address after linking with JP1/SS, see the chapter describing how to change IP address settings in the *JP1/Performance Management Planning and Configuration Guide*.

## 15.5 Link with JP1/SS in a multiple-monitoring environment

---

When a Performance Management report for the host (on which the problem occurred) is displayed, a connection with PFM - Web Console specified in the JP1/SS system property file (`hptl_jp1_imss_main_setting.properties`) is established. This connection is required irrespective of whether the monitoring manager is primary or secondary. The report is not displayed if a connection with the specified PFM - Web Console cannot be established. In this case, edit the PFM - Web Console settings in the JP1/SS system property file so that a connection can be established correctly.

## 15.6 Operations when Performance Management linking with JP1/SS

This section describes the operations when Performance Management is linked with JP1/SS.

### 15.6.1 Entering information for Item elements

When creating an Item in JP1/SS, enter the appropriate information for the Item elements shown in the following table.

Table 15–2: Elements to be specified when creating Items in JP1/SS

Item element in which to enter information	Information to enter
The element corresponding to <i>element-ID-that-inputs-the-name-of-the-host-on-which-the-event-occurred</i> that you set in <i>Table15-1 Settings to be specified in the JP1/SS system property file</i>	Name of the host on which the event occurred
Related information	<i>The URL for logging on to PFM - Web Console</i> you set up in <i>Table15-1 Settings to be specified in the JP1/SS system property file</i> and its display name
The element corresponding to <i>element-ID-that-inputs-the-date-and-time-when-the-event-occurred</i> that you set in <i>Table15-1 Settings to be specified in the JP1/SS system property file</i>	Date and time when the event occurred

For details on how to set up each element, see the JP1/Service Support manuals.

### 15.6.2 Viewing Performance Management reports from the JP1/SS interface

1. In the main window (Item list) of JP1/SS, in the Item list, select the title of the Item for which you want to view a report.
2. In the main window (Item list), from the **Action** menu, select **View item**.
3. In the related information in the View Item window, click the display name you specified for the PFM -Web Console URL.



#### Note

You can also view reports from an Item preview in the main window (Item list).

There are also other ways to display the View Item window.

For details on the other methods by which you can display the View Item window, see the JP1/Service Support manuals.

The window that appears after you click the display name for the PFM - Web Console URL depends on the authentication mode used for Performance Management and the permissions of the logged-in user.

## 15.7 Notes on linking with JP1/SS

---

If you attempt to open PFM - Web Console from JP1/SS when another PFM - Web Console window is already open, KAVJS0025-E error message appears in the original window. If you want to open the original window, close all PFM - Web Console windows and then open the window again.

# 16

## Detecting Problems Within Performance Management

This chapter describes how to detect problems within Performance Management.



## 16.1 Overview of detecting problems within Performance Management

---

By using the health check function, you can detect problems within Performance Management itself. The health check function monitors the operating status of monitoring agents and their hosts, and makes the user aware of changes in the operating status by displaying the results in PFM - Web Console. If you use PFM - RM, you can check whether each monitoring host is running.

Also, you can use the PFM service automatic restart functionality to automatically restart a PFM service if it stops abnormally, or to schedule it to restart.

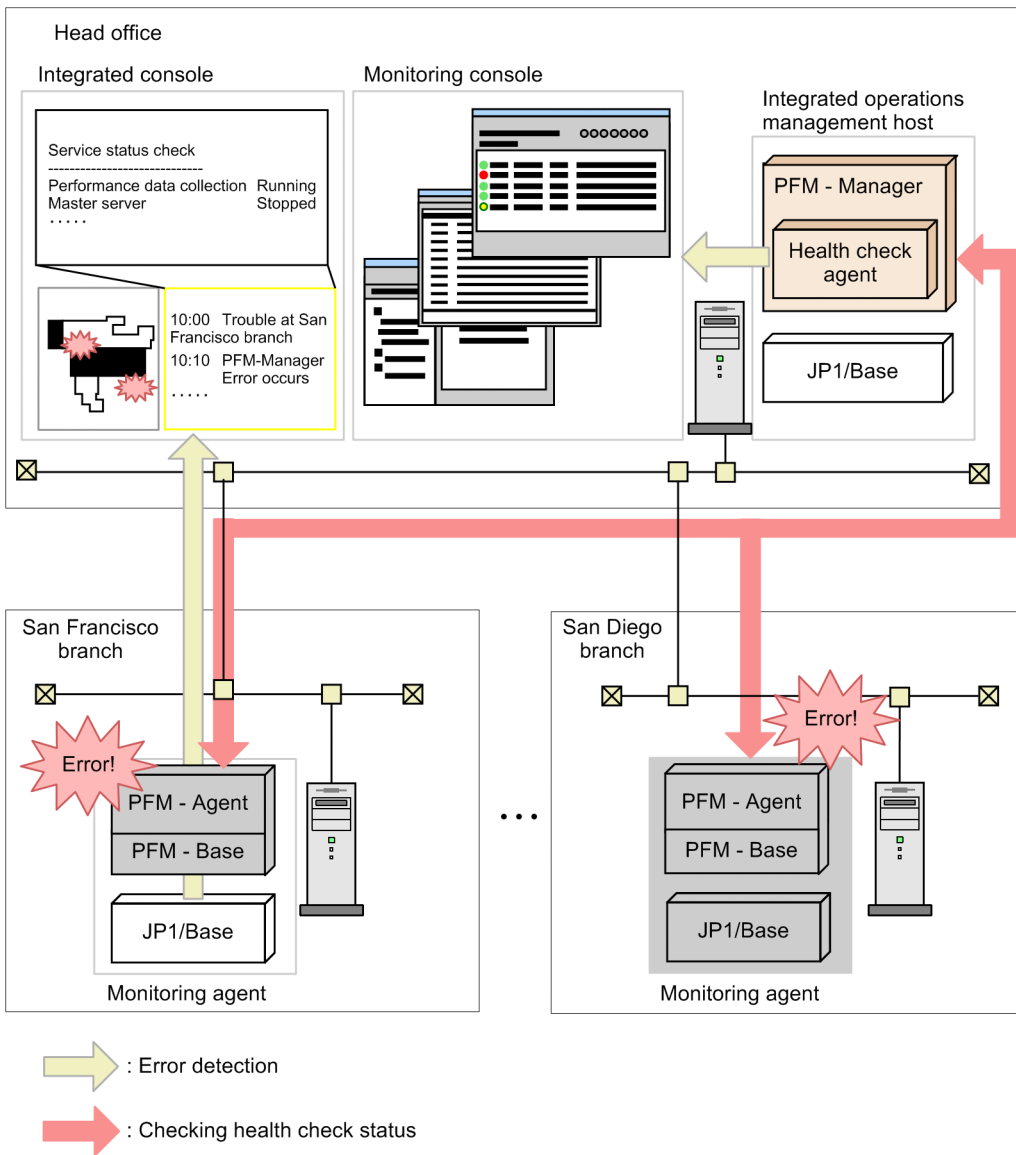
To use the health check function to monitor the operating status of monitoring agents, or to use the PFM service automatic restart functionality, use the status management function to monitor detailed information about Performance Management services.

For this reason, the version of the monitoring agent monitored by the health check function must support the status management function, and the status management function must be active. There are no prerequisites associated with monitoring the operating status of a host. To monitor the operating status of a host monitored by PFM - RM, you must enable the status management function on the PFM - RM host. Versions of PFM - Agent or PFM - RM that support the status management function differ for each Agent product. For details on the versions of PFM - Agent or PFM - RM that support the status management function, see [16.3 Using the status management function to check service status](#).

You can also detect problems within Performance Management by using the integrated systems monitoring product JP1/Base to monitor the Performance Management log files. By using this feature, the system administrator can be made aware of problems in the system, identify the cause of the problem, and take the appropriate measures to resolve it.

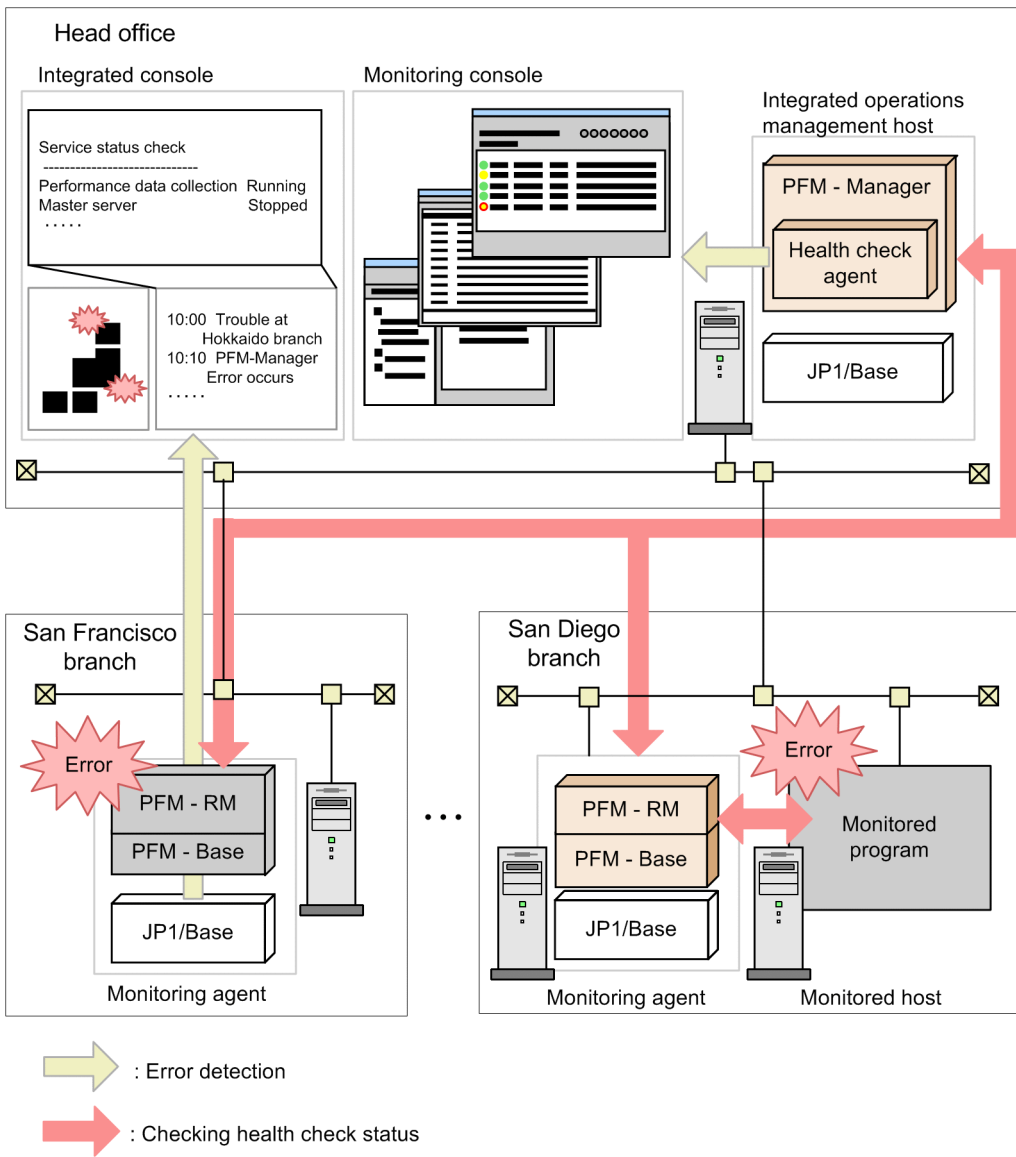
The following figure shows an example of using Performance Management to detect problems with the PFM - Agent at the San Francisco branch, and the host at the San Diego branch on which PFM - Agent is running.

Figure 16–1: Example of detecting problems in Performance Management itself (PFM - Agent)



The following figure shows an example of using Performance Management to detect problems with the PFM - RM at the San Francisco branch, and the host at the San Diego branch on which PFM - RM is running.

Figure 16–2: Example of detecting problems in Performance Management itself (PFM - RM)



## 16.2 Using the health check function to check the operating status of monitoring agents and their hosts

### Note

You cannot use the health check function to monitor the status of group agents or agents that actually no longer exist after either of the following measures were taken:

- The service information of an agent was deleted, and deletion of the service information was reported to PFM - Web Console by using the `jpccconf service sync` command.
- Because the configuration of business groups was changed, the user reference permission for an agent was deleted.

The health check status of these agents is always `Not Supported`.

### 16.2.1 Configuring the health check function

#### (1) Setting up the health check function

The following prerequisites must be met prior to using the health check function. If these prerequisite conditions are not met, you will not be able to use the health check function.

##### Name resolution

The monitoring host name<sup>#</sup> of the PFM - Agent host must be resolved to an IP address available for communication in the `jpchosts` or `hosts` file on the PFM - Manager host, or the domain name server.

<sup>#</sup>: `hostname` for Windows, `uname -n` for UNIX, or an alias if the functionality for setting monitoring-host names is used

##### Monitoring the operating status of the host running the monitoring agent:

- Version 08-11 or later of PFM - Manager and PFM - Web Console
- Any version of PFM - Agent or PFM - RM

To monitor the operating status of a host monitored by PFM - RM, you must enable the status management function on the PFM - RM host. If the status management function is not enabled, the status of the remote agent is not recognized correctly.

##### Monitoring the operating status of the monitoring agent service:

The health check function uses the status management function to monitor the operating status of PFM - Agent services. For this reason, the product being monitored by the health check function must support the status management function. The prerequisite conditions for using the function are as follows. Any version of PFM - RM can be used.

- Version 08-11 or later of PFM - Manager and Web Console
- The version of PFM - Agent used supports the status management function.
- The status management function on the PFM - Agent or PFM - RM host is enabled.

Unless the second and third conditions are satisfied, the health check function will be unable to check the status of PFM - Agent or PFM - RM. For details on the versions of PFM - Agent that support the status management function,

see [16.3 Using the status management function to check service status](#). The following table describes support for operating status monitoring of services by PFM - Agent version.

Table 16–1: Support for operating status monitoring of services by PFM - Agent version

Status management function on monitored agent host	Version of monitored agent	Operating status monitoring of services
Enabled	08-00 or later	Can be used
Enabled	07-00 or earlier <sup>#1</sup>	Cannot be used <sup>#2</sup>
Disabled	n/a	Cannot be used <sup>#3</sup>

Legend:

n/a: Not applicable.

#1

When PFM - Agent 07-00 or earlier is installed on the same host as PFM - Agent 08-00 or later or PFM - Base 08-00 or later, and the status management function is enabled on the target PFM - Agent host

#2

The operating status monitoring of the agent service appears as `Not Supported`.

#3

The operating status monitoring of the agent service appears as `Unconfirmed`.

For details on how to configure the status management function, see [16.3.1 Configuring the status management function](#).

To monitor the status of a host monitored by PFM - RM, you must enable polling with an appropriate PFM - RM property. For details on settings for PFM - RM polling, see [16.2.1\(1\)\(d\) Setting PFM - RM polling](#).

## (a) Enabling the health check function

To enable the health check function on the PFM - Manager host:

1. Stop Performance Management services.

If Performance Management services are running on a physical host, stop the services by using the following command:

```
jpcspm stop -key jplpc
```

To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpccconf hc enable` command

To enable the health check function, use the following command:

```
jpccconf hc enable
```

3. Check the status of the health check function.

To confirm that the status of the health check function is `available`, use the following command:

```
jpccconf hc display
```

4. Start Performance Management services.

To start all Performance Management services on a physical host, use the following command:

```
jpcspm start -key jplpc
```

To start all Performance Management services on a logical host, use the cluster software.

The service ID is `0A1host-name` or `0S1host-name`.

Note:

When one of the services you are starting is PFM - Manager, and the health check function is enabled on the PFM - Manager host, the health check agent starts as one of the PFM - Manager services when you execute the `jpcspm start` command. When you execute the `jpcspm stop` command to stop the PFM - Manager services, the health check agent also stops.

You cannot specify `agt0` as the service key when you execute the `jpcspm start` or `jpcspm stop` commands.

 **Tip**

The health check function provides two monitoring levels. One level is `Service`, which allows monitoring of the operating status of services. The other level is `Host`, which allows monitoring of the operating status of agent hosts. The default level is `Host`.

For details on how to configure a monitoring level, see [16.2.1\(2\) Setting the health check agent properties](#).

## (b) Disabling the health check function

To disable the health check function on the PFM - Manager host:

1. Stop Performance Management services.

If Performance Management services are running on a physical host, stop the services by using the following command:

```
jpcspm stop -key jplpc
```

To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpccconf hc disable` command.

To disable the health check function, use the following command:

```
jpccconf hc disable
```

3. Check the status of the health check function.

To confirm that the status of the status management function is `unavailable`, use the following command:

```
jpccconf hc display
```

If PFM - Manager is running in a logical host environment, execute the `jpccconf hc display` command on the PFM - Manager host on the executing or standby node.

4. Start Performance Management services.

To start all Performance Management services on a physical host, use the following command:

```
jpcspm start -key jplpc
```

To start all Performance Management services on a logical host, use the cluster software.

For details on each command, see the manual *JPI/Performance Management Reference*.

## (c) Checking the status of the health check agent

Use the `jpctool service list` command to check the status of the health check agent. You can also use the health check function to check the operating status of the health check agent. If the Agent Collector or Remote Monitor Collector service of the health check agent has terminated abnormally, the wrong health check results might be displayed.

## (d) Setting PFM - RM polling

To monitor the status of a host monitored by PFM - RM, you must enable polling of the monitored host with an appropriate PFM - RM property. The following table describes the property to be set.

Table 16–2: Setting the polling property

Folder name	Property name	Description
Health Check Configurations	Health Check for Target Hosts	Specifies whether to perform polling to the monitored hosts. The default is <code>No</code> . <code>Yes</code> : Performs polling. <code>No</code> : Does not perform polling.

If polling is disabled, the operating status of the monitored host appears as `Not Supported`.

## (2) Setting the health check agent properties

When the health check function is enabled, you can make settings related to the health check function, such as the collection interval for operation monitoring data and the monitoring level, by setting the properties of the health check agent from the Services tree of PFM - Web Console. The following table lists the health check agent properties you can set.

Table 16–3: Health check agent properties

Folder name	Property name	Description
Detail Records - HC	Description	Displays <code>Health Check Detail</code> as a description for the record.
	Log	Specifies whether to collect performance data. The default is <code>No</code> . <code>Yes</code> : Collects performance data. <code>No</code> : Does not collect performance data.
	Collection Interval	Specifies the collection interval in seconds, as a value in the range from 0 to 2147483647. The default is 300. This value serves as the polling interval of the health check function. <sup>#4</sup>
	Collection Offset	Specifies the offset of the collection start time in seconds, as a value in the range from 0 to 32767. The default is 0.
	LOGIF	Specifies the conditions for acquiring logs.
Health Check Configurations <sup>#1</sup>	Monitoring Level <sup>#2</sup>	Specifies the monitoring level. To monitor the operating status of the agent service, specify <code>Service</code> . To monitor the operating status of the agent host, specify <code>Host</code> . The default is <code>Host</code> .  This property cannot be specified when there is a host or agent for which monitoring is suspended.
	Polling Interval	Displays the polling interval. This value is taken from the Collection Interval in the <code>PD_HC</code> record.
	Incl. Action Handler	Specifies whether to include the Action Handler service when monitoring service operating statuses. The default is <code>No</code> . <code>Yes</code> : The Action Handler service is monitored.

Folder name	Property name	Description	
Health Check Configurations <sup>#1</sup>	Incl. Action Handler	No: The Action Handler service is not monitored.	
	Busy as Inactive	Specify whether agents whose service status remains Busy for extended periods should be considered inactive. The default is No. If you specify Yes, the Time to Busy as Inactive setting takes effect. Yes: The agent is considered inactive <sup>#3</sup> . No: The agent is not considered inactive. You can check the service status of an agent in the Status column in the output of the <code>jpctool service list</code> command.	
	Time to Busy as Inactive Collector	Specifies how long <sup>#3</sup> busy statuses should persist for the Agent Collector and Remote Monitor Collector services before the services are considered inactive. Specify this item in seconds. The default is 300.	
	Time to Busy as Inactive Store	Specifies how long <sup>#3</sup> busy statuses should persist for the Agent Store and Remote Monitor Store services before the services are considered inactive. Specify this item in seconds. The default is 300.	
	Time to Busy as Inactive AH	Specifies how long <sup>#3</sup> a busy status should persist for the Agent Handler service before the service is considered inactive. Specify this item in seconds. The default is 300.	
	JP1 Event	-	Specifies whether to issue health check events as JP1 events. The default is No. Yes: Health check events are issued as JP1 events. No: Health check events are not issued as JP1 events.
		Not Supported	Not Supported health check event. The default is None. None: This health check event is not issued as a JP1 event. Information: This health check event is issued as a JP1 event with Information as SEVERITY. Warning: This health check event is issued as a JP1 event with Warning as SEVERITY. Error: This health check event is issued as a JP1 event with Error as SEVERITY.
		Running	Running health check event. The default is Information. None: This health check event is not issued as a JP1 event. Information: This health check event is issued as a JP1 event with Information as SEVERITY. Warning: This health check event is issued as a JP1 event with Warning as SEVERITY. Error: This health check event is issued as a JP1 event with Error as SEVERITY.
		Incomplete	Incomplete health check event. The default is Warning. None: This health check event is not issued as a JP1 event. Information: This health check event is issued as a JP1 event with Information as SEVERITY. Warning: This health check event is issued as a JP1 event with Warning as SEVERITY. Error: This health check event is issued as a JP1 event with Error as SEVERITY.
		Stopped	Stopped health check event. The default is Error. None: This health check event is not issued as a JP1 event.



Folder name	Property name		Description
Health Check Configurations <sup>#1</sup>	JP1 Event	Stopped	Information: This health check event is issued as a JP1 event with Information as SEVERITY. Warning: This health check event is issued as a JP1 event with Warning as SEVERITY. Error: This health check event is issued as a JP1 event with Error as SEVERITY.
		Unconfirmed	Unconfirmed health check event. The default is Error. None: This health check event is not issued as a JP1 event. Information: This health check event is issued as a JP1 event with Information as SEVERITY. Warning: This health check event is issued as a JP1 event with Warning as SEVERITY. Error: This health check event is issued as a JP1 event with Error as SEVERITY.
		Host Not Available	Host Not Available health check event. The default is Error. None: This health check event is not issued as a JP1 event. Information: This health check event is issued as a JP1 event with Information as SEVERITY. Warning: This health check event is issued as a JP1 event with Warning as SEVERITY. Error: This health check event is issued as a JP1 event with Error as SEVERITY.

#1

When you change a setting in the Health Check Configurations folder, the new setting takes effect from the next polling interval.

#2

When you change the Monitoring Level setting, the health check results displayed in a realtime report of the health check agent differ according to whether polling under the new setting had taken place by the time the report was displayed.

Monitoring agent	Displayed health check results
Monitoring agent for which polling under the new setting has completed	The newest health check results recorded under the new setting
Monitoring agent for which polling under the new setting has not yet taken place	The newest health check results recorded under the old setting

For this reason, the report may briefly display results from both the old and new settings.

#3

The length of time a service is in Busy status is calculated from the difference between the time when polling occurred (the time on the host running PFM - Manager) and the time when the status of the service changed to Busy (the time on the host running PFM - Agent or PFM - RM). Make sure that the clocks are synchronized on all hosts that run Performance Management services.

#4

Specify the default value or a value that is at least 60 seconds and that is a divisor of 3,600. If you are specifying a record collection interval that exceeds 3,600 seconds (1 hour), ensure that the specified value is a multiple of 3,600 and a divisor of 86,400 (24 hours). If the specified record collection interval is smaller than the default value or shorter than 60 seconds, collected performance data might not be saved because of too heavy a workload on the Agent Collector service and the Agent Store service on the health check agent host.

## 16.2.2 Checking operating statuses

You can check the health check status of an agent by its icon in the agents tree of PFM - Web Console, as well as in the Event Monitor and Event History window. You can also view more detailed information about the health check status by using the reports generated by the health check agent. Because health check agent reports only show information from monitoring agents for which polling has completed, you cannot display reports before polling has taken place. For details on the content of each window, see the chapters that describe the windows in the manual *JP1/Performance Management Reference*.

Legend:

Y: Operating

I: Operating with reduced capacity

P: Not polled

C: Communication failed.

NS: The Agent Collector service does not support the health check function.

N: Inactive

n/a: Not applicable to determination of status

### (1) In PFM - Agent

#### (a) Events issued when monitoring the operating status of the host running PFM - Agent

The following table describes the events that can occur when monitoring the operating status of the host on which the PFM - Agent is running.

Status	Description
Running	The health check function can communicate with the host where the monitoring agent is running.
Host Not Available	The health check function cannot communicate with the host where the monitoring agent is running.
Suspended	Monitoring for the host where the monitoring agent is running is suspended.

You cannot check the status of the service when monitoring the operating status on a host level. When you want to see detailed information about the service, use the `jpctool service list` command.

#### (b) Events issued when monitoring the operating status of the PFM - Agent service

The following table describes the events that can occur when monitoring the operating status of the PFM - Agent service.

Table 16–4: Events issued when monitoring the operating status of the PFM - Agent service

Status	Description
Running	<i>The agent is fully functional and working normally</i> This status appears when the Agent Collector service and Agent Store service on the agent are both running. If you have configured the health check function to also monitor the Action Handler service on the host, then this status appears when all three services are running.
Incomplete	<i>The agent is only partially functional</i> This status appears in the following cases: <ul style="list-style-type: none"><li>When the monitored agent allows the Action Handler service on the same host to be added as a monitoring target in the properties of the health check agent but the Action Handler service is not monitored, this status appears when the Agent Collector service is running and the Agent Store service is stopped<sup>#</sup>.</li></ul>

Status	Description
Incomplete	<p>If the Action Handler service is added as a monitored service, this status appears when the Agent Collector service is running but the Agent Store service or Action Handler service is stopped<sup>#</sup>.</p> <ul style="list-style-type: none"> <li>The Agent Collector service on the agent is working in standalone mode</li> </ul>
Not Supported	<p><i>The agent does not support the status management function</i></p> <p>This status appears when software that provides the status management function such as PFM - Base version 08-00 or later is installed on the host and the status management function is enabled, but the agent version is one that does not support the status management function, such as PFM - Agent 07-00.</p> <p>If the status management function is disabled on the host, Unconfirmed appears as the status.</p>
Stopped	<p><i>The agent functionality is stopped</i></p> <p>This status appears when the Agent Collector service on the agent is stopped<sup>#</sup>.</p>
Unconfirmed	<p><i>The status of the agent cannot be confirmed</i></p> <p>This status appears when the health check function cannot communicate with the Status Server service on the host where the agent is located. This may be because the status management function is disabled, or PFM - Agent 07-00 is running alone.</p>
Host Not Available	<p><i>The host where the agent is located is stopped</i></p> <p>This status appears when the health check function cannot communicate with the host where the agent is located.</p>
Suspended	<p><i>Monitoring for the agent is suspended</i></p>

#

A service is judged to have stopped when it has any status other than Active or Busy. However, you can configure the health check function to consider a service stopped if the Busy status persists for longer than the period of time that you specify in the properties of the health check agent.

The following table describes the operating statuses of the host and monitoring agent services for each status other than Suspended status.

Table 16–5: Health check status, host operating status and monitoring agent operating status

Status	Host where monitoring agent is running	Status Server	Agent Collector	Agent Store or Action Handler
Running	Y	Y	Y	Y
	Y	Y	Y	Y <sup>#</sup>
Incomplete	Y	Y	Y	N
	Y	Y	Y <sup>#</sup>	n/a
Not Supported	Y	Y	NS	n/a
Stopped	Y	Y	N	n/a
Unconfirmed	Y	N	n/a	n/a
Host Not Available	N	n/a	n/a	n/a

#:

When running in standalone mode

## (2) In PFM-RM

### (a) Events issued when monitoring the operating status of the host running PFM - RM

The following table describes the events that can occur when monitoring the operating status of the host on which PFM - RM is running.

Table 16–6: Events issued when monitoring the operating status of the host running PFM - RM

Status	Description
Running	The health check function can communicate with the host where the monitoring agent is running.
Host Not Available	The health check function cannot communicate with the host where the monitoring agent is running.
Suspended	Monitoring for the host where the monitoring agent is running is suspended.

You cannot check the status of the service when monitoring the operating status on a host level. When you want to see detailed information about the service, use the `jpctool service list` command.

### (b) Events issued when monitoring the operating status of the PFM - RM service

The following table describes the events that can occur when monitoring the operating status of the PFM - RM service.

Table 16–7: Events issued when monitoring the operating status of the PFM - RM service

Status	Description
Running	<i>The PFM - RM is fully functional and working normally</i> This status appears when the Remote Monitor Collector service and Remote Monitor Store service on the PFM - RM are both running. If you have configured the health check function to also monitor the Action Handler service on the host, then this status appears when all three services are running.
Incomplete	<i>The PFM - RM is only partially functional</i> This status appears in the following cases: <ul style="list-style-type: none"><li>When the PFM - RM allows the Action Handler service on the same host to be added as a monitoring target in the properties of the health check agent but the Action Handler service is not monitored, this status appears when the Remote Monitor Collector service is running and the Remote Monitor Store service is stopped<sup>#</sup>. If the Action Handler service is added as a monitored service, this status appears when the Remote Monitor Collector service is running but the Remote Monitor Store service or Action Handler service is stopped<sup>#</sup>.</li><li>The Remote Monitor Collector service on the PFM - RM is working in standalone mode</li></ul>
Stopped	<i>The PFM - RM functionality is stopped</i> This status appears when the Remote Monitor Collector service on the PFM - RM is stopped <sup>#</sup> .
Unconfirmed	<i>The status of the PFM - RM cannot be confirmed</i> This status appears when the health check function cannot communicate with the Status Server service on the host where the PFM - RM is located. This may be because the status management function is disabled.
Host Not Available	<i>The host where the PFM - RM is located is stopped</i> This status appears when the health check function cannot communicate with the host where the PFM - RM is located.
Suspended	<i>Monitoring for the PFM - RM is suspended</i>

#

A service is judged to have stopped when it has any status other than `Active` or `Busy`. However, you can configure the health check function to consider a service stopped if the `Busy` status persists for longer than the period of time that you specify in the properties of the health check agent.

The following table describes the operating statuses of the host and monitoring agent services for each status other than `Suspended` status.

Table 16–8: Health check status, host operating status and monitoring agent operating status

Status	Host where monitoring agent is running	Status Server	Remote Monitor Collector	Remote Monitor Store or Action Handler
Running	Y	Y	Y	Y
	Y	Y	Y	Y <sup>#</sup>
Incomplete	Y	Y	Y	N
	Y	Y	Y <sup>#</sup>	n/a
Stopped	Y	Y	N	n/a
Unconfirmed	Y	N	n/a	n/a
Host Not Available	N	n/a	n/a	n/a

#:

When running in standalone mode

### (c) Events issued when monitoring the operating status of the host monitored by PFM - RM

When the operating status of the PFM - RM monitoring host is monitored, different events are output depending on the monitoring level settings for the health check function.

The timing for the polling of the PFM - RM host by the health check agent is different from the timing for the polling of the monitored host by the PFM - RM host. If polling of the monitored host has not been performed yet, the operating status of the monitored host appears as `Not Supported`.

#### ■ When the status management function is disabled

The following table describes the events that can occur when monitoring the operating status of the host monitored by PFM - RM.

Table 16–9: Events when monitoring PFM - RM-monitored host operating status (when polling is disabled)

Status	Description
Not Supported	<i>The PFM - RM monitoring host and the Status Service are operating normally.</i>
Unconfirmed	<i>Cannot communicate with the PFM - RM monitoring host or the Status Server service.</i>
Suspended	<i>Monitoring for the monitored host is suspended.</i>

The following table describes the operating statuses of the monitored host and PFM - RM services for each status other than `Suspended` status.

Table 16–10: Health check statuses and operating statuses of PFM - RM services and the monitored host

Status	PFM-RM host	Status Server	Remote Monitor Collector	Monitored host
Not Supported	Y	Y	n/a	n/a
Unconfirmed	N	n/a	n/a	n/a
	Y	N	n/a	n/a

■ **When the monitoring level is Host and polling is enabled**

The following table describes the events that can occur when monitoring the operating status of the host monitored by PFM - RM.

Table 16–11: Events when monitoring PFM - RM-monitored host operating status (when the monitoring level is Host and polling is enabled)

Status	Description
Running	<i>The monitored host is fully functional and working normally</i>
Not Supported	<i>The monitored host has not been polled.</i>
Unconfirmed	<p><i>The status of the monitored host cannot be confirmed</i></p> <p>This status appears in the following cases:</p> <ul style="list-style-type: none"> <li>• This status appears when the health check function cannot communicate with the PFM - RM monitoring host.</li> <li>• This status appears when the health check function cannot communicate with the Status Server service on the PFM - RM monitoring host. This may be because the status management function is disabled.</li> <li>• The Remote Monitor Collector service for the monitoring PFM - RM is not running.</li> <li>• Polling of the monitored host failed.</li> </ul>
Host Not Available	<i>The monitored host is stopped.</i>
Suspended	<i>Monitoring for the monitored host is suspended.</i>

The following table describes the operating statuses of the monitored host and PFM - RM services for each status other than Suspended status.

Table 16–12: Health check status, PFM - RM service status and monitored host operating status

Status	PFM-RM host	Status Server	Remote Monitor Collector	Monitored host
Not Supported	Y	Y	Y	P
Running	Y	Y	Y	Y
Unconfirmed	N	n/a	n/a	n/a
	Y	N	n/a	n/a
	Y	Y	N	n/a
	Y	Y	Y	C
Host Not Available	Y	Y	Y	N

■ **When the monitoring level is Service and polling is enabled**

The following table describes the events that can occur when monitoring the operating status of the host monitored by PFM - RM.

Table 16–13: Events when monitoring PFM - RM-monitored host operating status (when the monitoring level is Service and polling is enabled)

Status	Description
Running	<i>The monitored host is fully functional and working normally</i>
Incomplete	<p><i>The monitoring PFM - RM service is only partially functional</i></p> <p>This status appears in the following cases:</p> <ul style="list-style-type: none"> <li>• The Remote Monitor Collector service on the monitoring PFM - RM is in <code>Incomplete</code> status.</li> <li>• This status appears when the Remote Monitor Collector service on the monitoring PFM - RM is stopped<sup>#</sup>. If the Action Handler service is added as a monitored service, this status appears when the Remote Monitor Collector service is running but the Remote Monitor Store service or Action Handler service is stopped<sup>#</sup>.</li> </ul>
Not Supported	<i>The monitored host has not been polled.</i>
Unconfirmed	<p><i>The status of the monitored host cannot be confirmed</i></p> <p>This status appears in the following cases:</p> <ul style="list-style-type: none"> <li>• This status appears when the health check function cannot communicate with the PFM - RM monitoring host.</li> <li>• This status appears when the health check function cannot communicate with the Status Server service on the PFM - RM monitoring host. This may be because the status management function is disabled.</li> <li>• The Remote Monitor Collector service for the monitoring PFM - RM is not running.</li> <li>• Polling of the monitored host failed.</li> </ul>
Host Not Available	<i>The monitored host is stopped.</i>
Suspended	<i>Monitoring for the monitored host is suspended.</i>

#

A service is judged to have stopped when it has any status other than `Active` or `Busy`. However, you can configure the health check function to consider a service stopped if the `Busy` status persists for longer than the period of time that you specify in the properties of the health check agent.

The following table describes the operating statuses of the monitored host and PFM - RM services for each status other than `Suspended` status.

Table 16–14: Health check status, PFM - RM service status and monitored host operating status

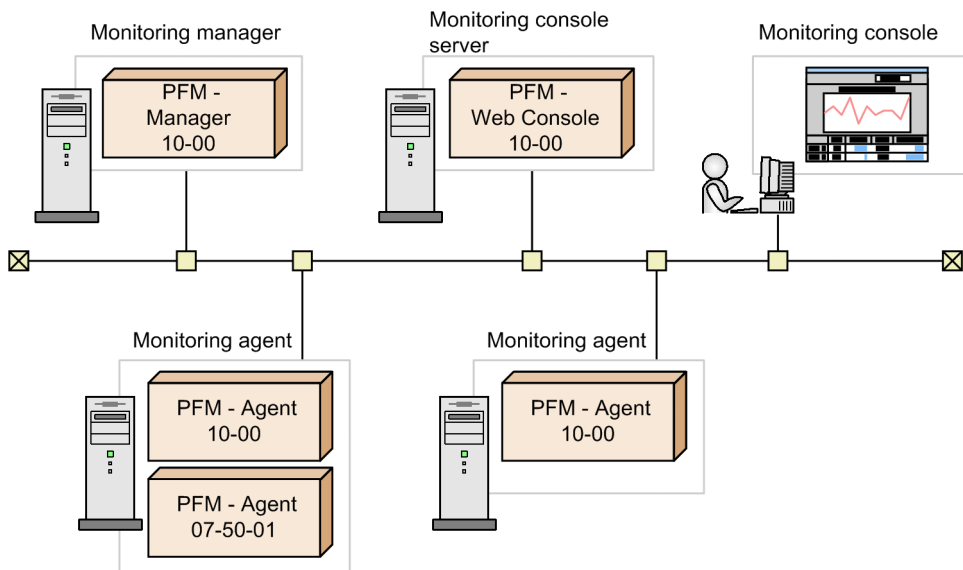
Status	PFM-RM host	Status Server	Remote Monitor Collector	Monitored host	Remote Monitor Store or Action Handler
Not Supported	Y	Y	Y or I	P	n/a
Running	Y	Y	Y	Y	Y or I
Incomplete	Y	Y	I	Y	n/a
	Y	Y	Y	Y	N
Unconfirmed	N	n/a	n/a	n/a	n/a
	Y	N	n/a	n/a	n/a
	Y	Y	N	n/a	n/a
	Y	Y	Y or I	C	n/a
Host Not Available	Y	Y	Y or I	N	n/a

## 16.2.3 Examples of using the health check function

### (1) Using the health check function with service-level monitoring of operating statuses as the monitoring level

The health check function can be used to its full potential by using a monitoring level that provides service-level monitoring of operating statuses, in a Performance Management system where all instances of PFM - Agent and PFM - RM meet the conditions that allow this monitoring level. The following figure shows an example of a system where all instances of PFM - Agent and PFM - RM meet the conditions under which the health check function can perform service-level monitoring of operating statuses.

Figure 16–3: Example of a system where all instances of PFM - Agent and PFM - RM meet the requirements for service-level monitoring of operating statuses



To use the health check function with service-level monitoring of operating statuses as the monitoring level:

1. Enable the health check function.

Execute the `jpccconf hc enable` command on the PFM - Manager host.

2. Configure the health check function.

Start PFM - Manager, and display the properties of the health check agent in PFM - Web Console. Set the monitoring level to **Service**, and set the other properties as required.

3. Start using the health check function.

In the Agents tree of PFM - Web Console, you can check the operating status of the services of each agent. You can also monitor the Event Monitor window or the Event History window for changes in the health check status. The status of each agent is derived from the results of the health check function checking the operating status of each of the agent's services. You can also view more detailed information about the health check status in the form of a report. Some health check reports are provided as monitoring templates. For details on the monitoring template of the health check function, see the overview of the monitoring template in the appendixes of *JP1/Performance Management Planning and Configuration Guide*.

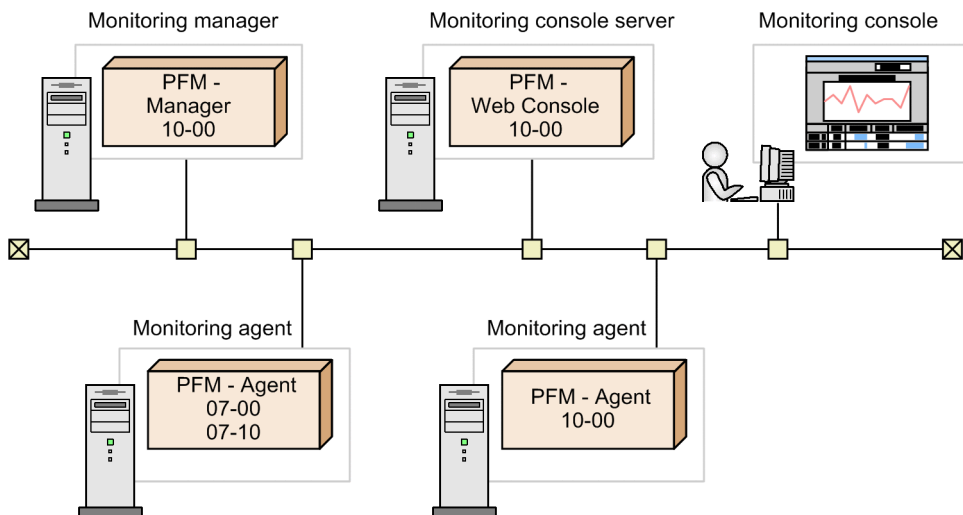
When the health check status of an agent is reported as abnormal, take action to resolve the problem such as restarting the agent.



## (2) Using the health check function with host-level monitoring of operating statuses as the monitoring level

In a system where some instances of PFM - Agent or PFM - RM in the Performance Management system do not meet the conditions that allow service-level monitoring, you can monitor the status of the host instead by using the monitoring level that provides host-level monitoring of operating statuses. If you use the monitoring level that provides service-level monitoring, the operating status of the instances of PFM - Agent or PFM - RM that do not meet the conditions will not be accurate. Polling will also take longer than normal. The following figure shows an example of a system where some instances of PFM - Agent or PFM - RM do not meet the conditions under which the health check function can perform service-level monitoring of operating statuses.

Figure 16–4: Example of a system where not all instances of PFM - Agent or PFM - RM meet the requirements for service-level monitoring of operating statuses



To use the health check function with service-level monitoring of operating statuses as the monitoring level:

1. Enable the health check function.

Execute the `jpccconf hc enable` command on the PFM - Manager host.

2. Configure the health check function.

Start PFM - Manager, and display the properties of the health check agent in PFM - Web Console. Set the properties as required.

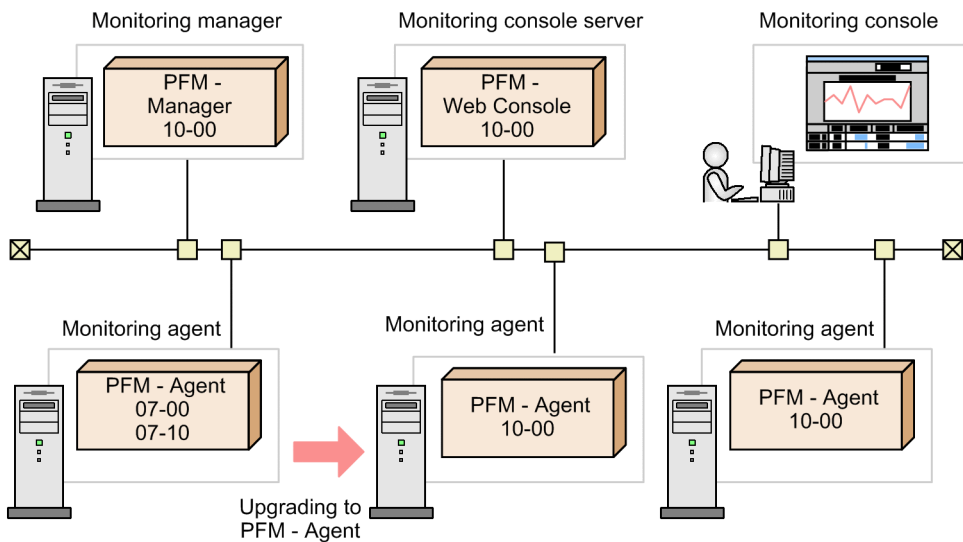
3. Start using the health check function.

In the Agents tree of PFM - Web Console, you can check the operating status of the host for each agent. You can also monitor the Event Monitor window or the Event History window for changes in the health check status. The status of each agent is derived from the results of the health check function checking the status of the host. You can also view more detailed information about the health check status in the form of a report. Some health check reports are provided as monitoring templates. For details on the monitoring template of the health check function, see the overview of the monitoring template in the appendixes of *JP1/Performance Management Planning and Configuration Guide*.

When the health check status of an agent is reported as abnormal, take action to resolve the problem such as restarting the host.

You can switch to service-level monitoring as soon as all instances of PFM - Agent or PFM - RM in the system support it. The following figure shows an example of switching from host-level monitoring to service-level monitoring.

Figure 16–5: Switching from host-level monitoring to service-level monitoring



### (3) When monitoring operating statuses by linking with JP1/IM

By linking with JP1/IM, you can be made aware of problems related to the operating status of Performance Management via the JP1/IM interface. Also, by displaying the reports that are associated with alarms, you can analyze and view detailed information about the operating status of Performance Management.

Health check events are issued when the health check status of agents changes. If you enable the function for issuing health check events as JP1 events, JP1 system events are issued when health check events are issued. For details, see [16.2.1 Configuring the health check function](#).

If you want to notify JP1/IM of the changes in health check status, use alarms. The monitoring template includes three alarms, each of which provides a different level of detail. Use the alarm that best suits your purpose. When linking with JP1/IM, copy the chosen alarm from the monitoring template and configure it to issue a JP1 event as an action. For details on how to do so, see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

### (4) Using the health check function in a firewall or NAT environment

The health check agent must be able to communicate with the Status Server service on each host running PFM - Agent or PFM - RM. For this reason, when you use the health check function in a firewall or NAT environment, the firewall or NAT must be set up so that the health check agent's traffic can be routed through the firewall or NAT. For details on the settings, see the description of firewall routing in the appendixes of the manual *JP1/Performance Management Reference*. The following table describes the port numbers used by the health check agent.

Table 16–15: Port numbers used by the health check agent

Service name	Parameter	Port number	Note
Agent Collector (health check agent)	jp1pcagt0	Automatic <sup>#</sup>	This port is used for such tasks as binding alarms and acquiring realtime reports.
Agent Store (health check agent)	jp1pcsto0	Automatic <sup>#</sup>	This port is used for such tasks as recording performance data and acquiring historical reports.

#:

Each time the service restarts, it is automatically allocated a port number that is not already in use in the system.

A PFM - RM host uses the ICMP protocol to poll monitored hosts. To check the operating status of a PFM - RM monitored host, configure the firewall so that the PFM - RM host can communicate with the monitored host using the ICMP protocol. For details, see the appendixes of the appropriate PFM - RM manual.

## (5) Using the health check function in a cluster system

You can use the health check function in the same manner as in a non-cluster system. The health check function must be set up on the host where PFM - Manager is installed.

If you set up PFM - Manager version 09-00 or later in a new logical host environment, that PFM - Manager inherits the health check function settings of the physical host environment. Change the health check function settings as necessary.

For details on how to configure the health check function for use in a cluster system, for Windows see *10.2.2 Installing and setting up PFM - Manager*, and for UNIX see *10.4.2 Installing and setting up PFM - Manager*.

### 16.2.4 Notes on the health check function

This subsection contains notes on the health check function.

Legend:

↓ ... ↓: The digits after the decimal point are cut off.

#### (1) Polling-related settings of the health check function

The health check function polls each agent host to check whether it is active. The following table describes how the number of hosts that can be polled simultaneously, the polling interval for each agent host, and the polling timeout time are determined for polling by the health check function.

Table 16–16: Polling-related settings of the health check function

Polling-related setting	PFM - Manager is 10-00 or later and the parallel check mode is enabled	PFM - Manager is 09-00 or earlier or 10-00 or later and the parallel check mode is disabled
Number of hosts that can be polled simultaneously	Usually, the setting does not need to be changed. To change the setting, use the <code>Parallel Confirmation Count</code> property. Default: 10 (hosts)	1 (cannot be changed)
Polling interval	Usually, the setting does not need to be changed. To change the setting, use the <code>Minimum Period per Host</code> property. Default: 0 (seconds)	The polling interval is automatically calculated based on the value of the <code>Collection Interval</code> property and the number of hosts in the system (the minimum is 2 seconds). If you want to change the polling interval, you need to change the value of the <code>Collection Interval</code> property.
Polling timeout time	Usually, the setting does not need to be changed. To change the setting, use the <code>Timeout Period per Host</code> property. Default: 30 (seconds)	The polling timeout time is automatically calculated based on the polling interval (2 to 10 seconds). If you want to change the polling timeout time, you need to change the value of the <code>Collection Interval</code> property.

When the parallel check mode is enabled, a sufficient polling timeout time is allocated regardless of the number of monitored hosts in the system. When the parallel check mode is disabled, a sufficient value must be set for the `Collection Interval` property for the number of monitored hosts in the system because the polling timeout time

is automatically calculated based on the value of the `Collection Interval` property and the number of monitored hosts in the system.

If an inappropriate polling interval is set, PFM - Agent or PFM - RM might be frequently considered as inactive, polling might not be completed for all agent hosts within the set interval<sup>#</sup>, or other problems might occur. This subsection describes how to check the currently set polling interval and how to correct the polling interval if it is inadequate.

#

For details on the behavior of the health check function if polling is not completed within the set interval for all agent hosts, see *16.2.4(2) Behavior of the health check function if polling is not completed for all agent hosts within the specified interval* and *16.2.4(3)(b) Occasions for storing data and evaluating alarms if polling is not completed for all agent hosts within the specified interval*.

### (a) When the parallel check mode is enabled

When the parallel check mode is enabled, you can configure the properties described in the table below. Usually, you do not need to change the values of the properties. However, you can tune the operation of the health check function by changing the values of the properties if incorrect operating statuses are frequently detected or polling does not complete within the interval specified for the `Collection Interval` property.

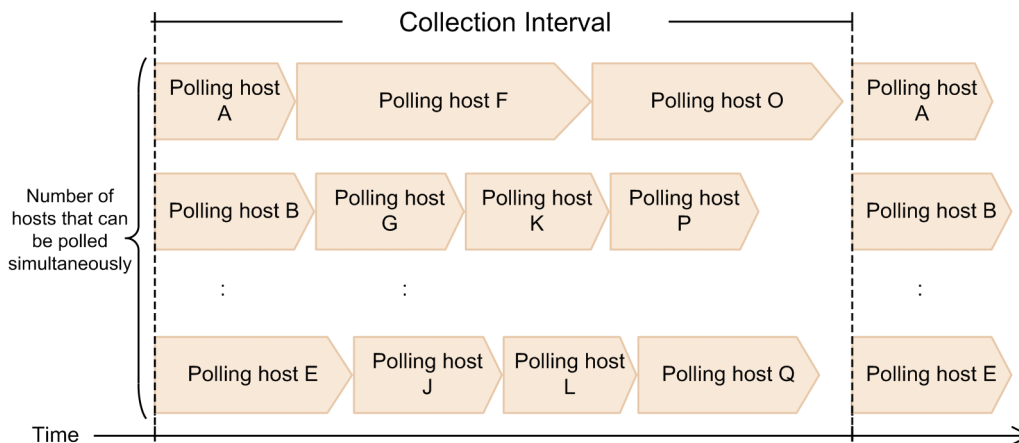
Table 16–17: Properties to be configured when the parallel check mode is enabled

Property	Description	Purpose for using this property
Parallel Confirmation Count	Number of hosts that can be polled simultaneously when the parallel check mode is enabled	Set a large value when many monitored hosts exist in the system and you want to reduce the length of time required for checking all the hosts in the system. Because the health check function checks as many hosts as specified for this property at one time, setting a large value for this property reduces the length of time required for checking all the hosts in the system.  Set a small value if you want to reduce the load of communication for checking. When you set a small value, the amount of communication performed for parallel checking is reduced, decreasing the amount of communication per unit time.
Minimum Period per Host	Minimum polling interval (seconds) per host when the parallel check mode is enabled	Specify the length of time to wait between the beginning of polling for a host and the beginning of polling for the next host if you want to avoid congested communication for checking at the same time. When you specify 0, the next host is immediately polled after polling for the previous host ends.  Note that polling is performed simultaneously for the number of hosts specified for the <code>Parallel Confirmation Count</code> property even if the <code>Minimum Period per Host</code> property is set. Use the <code>Minimum Period per Host</code> property to increase the interval between the successive polling for hosts.
Timeout Period per Host	Polling timeout time (seconds) per host when the parallel check mode is enabled	If polling a monitored host takes too long and times out due to heavy load on the network or the monitored host, the health check function might incorrectly detect the operating status of the host (such as <code>Unconfirmed</code> ). If timeout frequently occurs, set a large value for this property.  If you set a large value, it takes a long time to check all the hosts in the system. You need to increase the polling interval as well.

The following describes the purpose of each property.

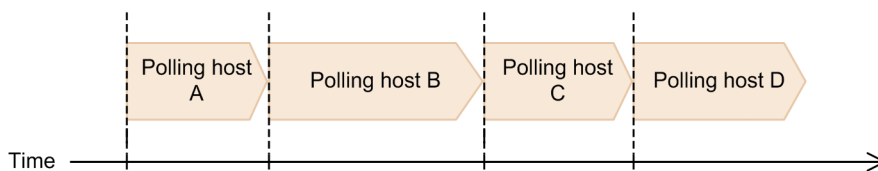
■ **Purpose of the number of hosts that can be polled simultaneously (Parallel Confirmation Count property)**

This property enables parallel polling for the specified number of hosts. See the following figure for an example.

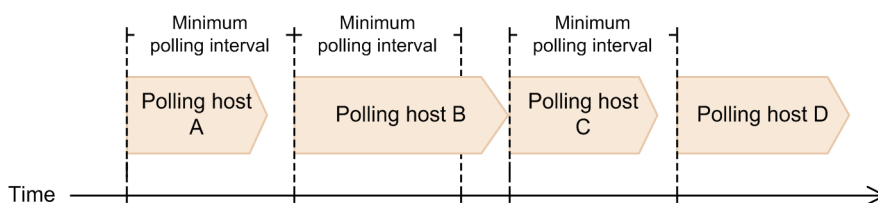


■ **Purpose of the minimum polling interval (Minimum Period per Host property)**

When 0 is set for the Minimum Period per Host property, the health check function immediately polls the next host when polling for the previous host ends. See the following figure for an example.

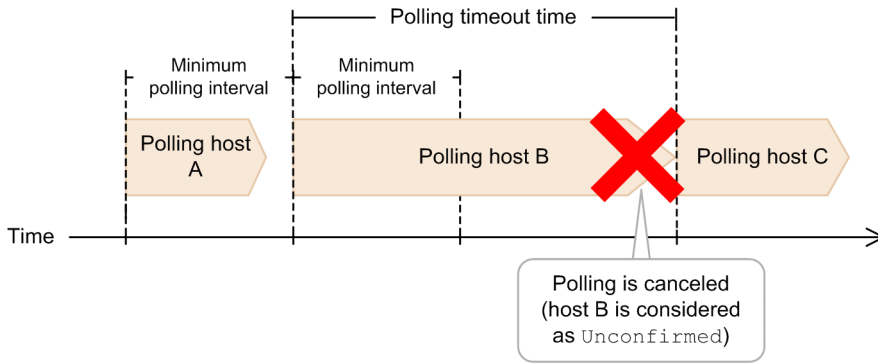


If a value greater than 0 is set for the Minimum Period per Host property, polling for the next host waits until the length of time set for the Minimum Period per Host property elapses from the beginning of polling for the previous host. This applies even if polling for the previous host is completed before the length of time set for the Minimum Period per Host property expires. If polling for a host ends after the length of time set for the Minimum Period per Host property ends, the health check function immediately starts to poll the next host. See the following figure for an example.



■ **Purpose of the polling timeout time (Timeout Period per Host property)**

If polling a host takes too long and exceeds the timeout time set for this property, the health check function determines the status of the host as `Unconfirmed`, cancels polling, and starts to poll the next host. See the following figure for an example.



## (b) If the parallel check mode is disabled

To set an appropriate polling interval for all agent hosts, you need to carefully determine the polling interval and the polling timeout time for each agent host. The following describes how to check the polling interval and the polling timeout time for each agent host.

### ■ Polling interval for each agent host

The health check agent automatically calculates the interval of polling for each agent host based on the number of agent hosts connected to PFM - Manager. If multiple instances of PFM - Agent or PFM - RM are running on the same host, the health check agent combines all the intervals of polling as one interval of polling for the host.

The following formula describes how to calculate the polling interval for each host. Use the formula if you want to check the polling interval for each agent host in the system you are using:

*Polling interval for each host (in seconds) =*

$$\downarrow (0.7 \times \text{polling interval value}^{\#1}) \div \text{total number of hosts}^{\#2} \downarrow$$

#1

This value is displayed for the `Polling Interval` property under the `Health Check Configurations` folder of the health check agent.

#2

Number of hosts running PFM - Agent or PFM - RM connected to PFM - Manager. The number of hosts is 1 if multiple instances of PFM - Agent or PFM - RM are installed on the same host or multiple instance environments exist.

The minimum polling interval for each host is 2 seconds. If the result of the above formula is less than 2 seconds, polling is performed every 2 seconds.

#### Note

The value set for the monitoring level of the health check function (value specified for the `Monitoring Level` property under the `Health Check Configurations` folder of the health check agent) does not affect polling intervals. For this reason, you do not need to take the value set for the monitoring level into consideration when you check the polling interval for each agent host.

### ■ Polling timeout time

When the health check function performs polling, the function communicates with the Status Server service on the host the function intends to check for its activation status. The health check function monitors the status of an agent based on the response from the Status Server service. If the health check function receives no response from the connected

Status Server service within the specified timeout time, a timeout error occurs. The timeout time is determined based on the polling interval. When you check the timeout time in the system that is currently running, make sure that the timeout time is either of the following:

- If the polling interval is 10 seconds or longer, the timeout time must be 10 seconds.
- If the polling interval is shorter than 10 seconds, the timeout time must be the same as the value of the polling interval (in seconds).

The minimum timeout time is 2 seconds.

### ■ Criteria for determining whether the polling interval for all agent hosts is adequate

To determine whether the specified polling interval for all agent hosts is adequate, check the following points with the previously specified items in mind: the polling interval for each host described in *Polling interval for each agent host* and the polling timeout time described in *Polling timeout time*.

- Whether the polling interval for each agent host is 10 seconds or longer
- Whether a polling timeout time suitable for the operating environment is set

Generally, as the number of agent hosts increases, the polling interval for each host and the length of time before occurrence of a timeout error become shorter. When a short timeout time is set, the health check function is more likely to determine that PFM - Agent or PFM - RM has stopped. When the specified polling interval for all agent hosts is too short, polling for all agent hosts does not complete within the specified interval. To prevent this problem, specify a polling interval for all agent hosts that allows at least 10 seconds as the polling interval for each agent host.

The following example describes how to check the polling interval and the polling timeout time for each host and how to determine whether the settings are adequate.

#### Prerequisites

- Number of hosts running PFM - Agent or PFM - RM: 50
- Value for the `Polling Interval` property: 300

#### Calculating the polling interval for each host

*Polling interval for each host*

=  $\downarrow 0.7 \times 300 \div 50 \downarrow$

= 4.2  $\downarrow$

= 4 (seconds)

#### Polling timeout time

The polling timeout time is 4 seconds because the polling interval for each host is 4 seconds.

#### Determining whether the settings are adequate

- The polling interval for each host is 4 seconds: The interval is less than 10 seconds, which is too short.
- The polling timeout time is 4 seconds: Depends on the operating environment.

As a result, you can see that the polling interval for all agent hosts needs to be changed to a more adequate value.

### ■ Procedure for calculating an adequate polling interval for all agent hosts

Perform the following procedure to calculate an adequate polling interval for all agent hosts. When the interval is determined, set the value for the `Collection Interval` property for the Health Check Detail (PD\_HC) record of the health check agent, which is correlated with the value of the `Polling Interval` property.

To calculate an adequate polling interval for all agent hosts:



1. Calculate the value of the `Polling Interval` property from the polling interval for each agent host.
2. A polling interval for all agent hosts must be a multiple of 60 (seconds). Round to the nearest multiple of 60 (seconds) the determined value of the `Polling Interval` property.

The following example describes how to estimate an adequate polling interval for all agent hosts by using the formula described in *Polling interval for each agent host*.

#### Prerequisites

- Number of hosts running PFM - Agent or PFM - RM: 50
- Polling interval for each host: 10 seconds

#### Calculating the polling interval for all agent hosts

$$10 = (0.7 \times \text{polling interval}) \div 50$$

*Polling interval*

$$= 50 \times 10 \div 0.7$$

$$= 714.2$$

$$\approx 720 \text{ (round to the nearest multiple of 60)}$$

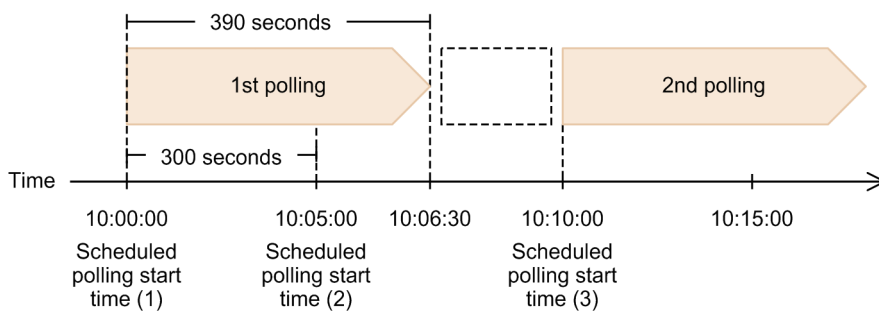
As a result, 720 is the value to be specified for the `Collection Interval` property for the Health Check Detail (PD\_HC) record as the polling interval for all agent hosts.

## (2) Behavior of the health check function if polling is not completed for all agent hosts within the specified interval

If the specified polling interval for all agent hosts is too short, polling for all agent hosts might not be completed within the specified interval. If that occurs, polling continues until it is completed for all agents. The next polling, which is scheduled to be performed during the extended previous polling, will be skipped.

The figure below describes this case. In the example, the specified polling interval for all agent hosts is 300 seconds, but polling actually takes 390 seconds.

Figure 16–6: Behavior of the health check function if polling is not completed for all agent hosts within the specified interval



Because the polling that starts at scheduled polling start time (1) does not finish when scheduled polling start time (2) is reached, the scheduled second polling is skipped. The next polling starts at scheduled polling start time (3) after the first polling is completed.

## (3) Storing health check results and evaluating alarms

Like the usual functions of PFM - Agent and PFM - RM, you can store the history data of health check results and evaluate alarms for the health check function. The following are notes on storing history data and evaluating alarms for the health check agent.

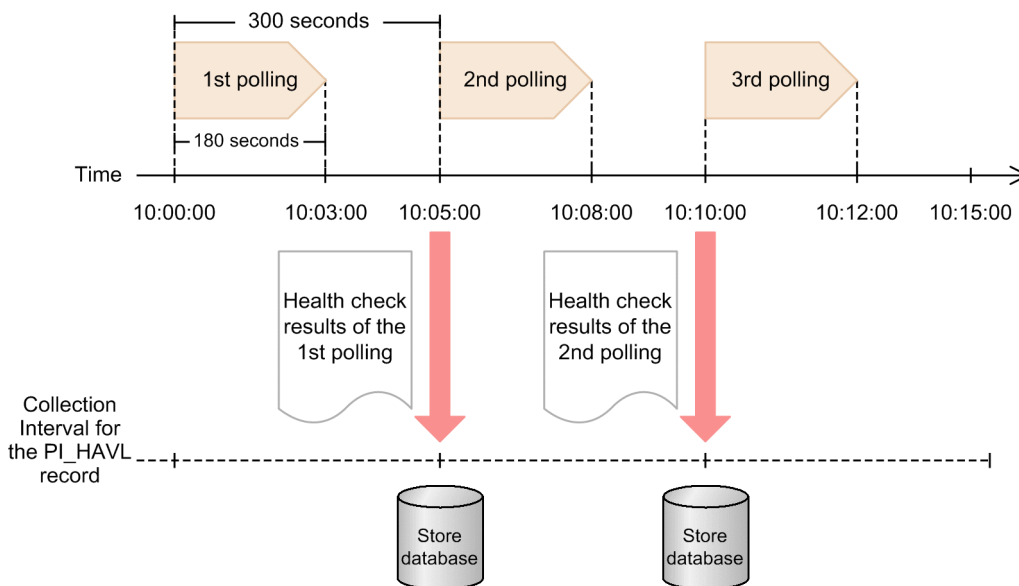


## (a) Occasions for storing data and evaluating alarms

To store history data of health check results, enable the record collection setting of the health check agent. You can evaluate alarms by defining alarms for the health check agent. Storage of history data and alarm evaluation are performed after polling for all agent hosts (which are the target of health checking) is completed, which is when the next polling starts. This means that storage of history data and alarm evaluation are not completed at the time when polling is completed.

The figure below describes this case. In the example, the Host Availability (PI\_HAVL) record is collected. The polling interval for all agent hosts is 300 seconds, but polling actually takes 180 seconds.

Figure 16–7: Occasions for storing data and evaluating alarms



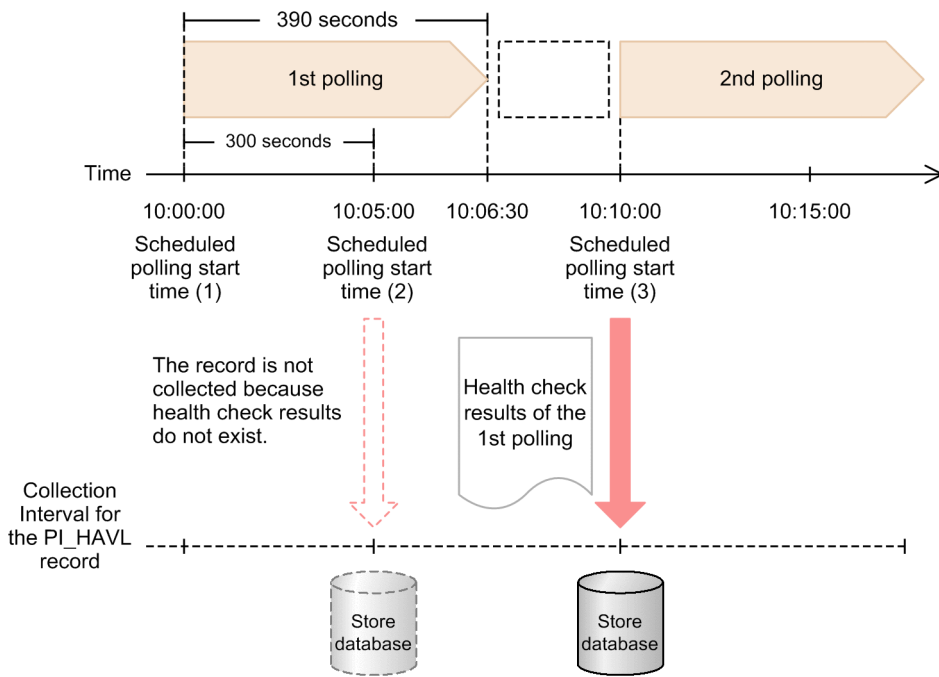
The first polling is completed at 10:03:00 and the second polling is completed at 10:08:00. At 10:03:00 and 10:08:00, the next polling is not started yet. For this reason, history data is not stored and alarms are not evaluated at these points. History data is stored and alarms are evaluated at 10:05:00 and 10:08:00 when the next polling starts.

## (b) Occasions for storing data and evaluating alarms if polling is not completed for all agent hosts within the specified interval

If polling does not complete within the polling interval for all agent hosts, history data of records is not stored and alarms are not evaluated. History data of records is stored and alarms are evaluated after polling for all agent hosts is completed when the next polling starts.

The figure below describes this case. In the example, the Host Availability (PI\_HAVL) record is collected. The polling interval for all agent hosts is 300 seconds, but polling actually takes 390 seconds.

Figure 16–8: Occasions for storing data and evaluating alarms if polling is not completed for all agent hosts within the specified interval



At 10:05:00, which is the start time for the second polling, the first polling is not completed. As a result, history data is not stored and alarms are not evaluated. History data is stored and alarms are evaluated at 10:10:00 when the second polling starts after the first polling is completed.

## 16.3 Using the status management function to check service status

This section describes the status management function, which is used to check the status of Performance Management services when PFM - Manager is starting or stopping or if PFM - Manager stops due to a problem.

The version from which support for the status management function was added differs between agent types. The following table describes which versions of each agent type support the status management function.

Table 16–18: Support for the status management function by agent type

Agent	Supported in
PFM - Agent for DB2	07-50-01 or later
PFM - Agent for Domino	07-50-01 or later
PFM - Agent for Enterprise Applications	08-00 or later
PFM - Agent for Exchange Server	08-10 or later
PFM - Agent for HiRDB	07-50-02 or later
PFM - Agent for WebSphere Application Server	08-11 or later
PFM - Agent for IBM WebSphere MQ	08-11 or later
PFM - Agent for IIS	08-10 or later
PFM - Agent for JP1/AJS	08-00 or later
PFM - Agent for Microsoft SQL Server	07-50-02 or later
PFM - Agent for OpenTP1 (for AIX and Linux)	07-50-02 or later
PFM - Agent for OpenTP1 (for Windows (IPF))	07-50 to 08-50
PFM - Agent for OpenTP1 (for Windows)	07-50-01 or later
PFM - Agent for Oracle	07-50-02 or later
PFM - Agent for Platform (UNIX) (for HP-UX, AIX, Solaris, and Linux)	07-50 or later
PFM - Agent for Platform (Windows)	07-50-01 or later
PFM - Agent for Service Response	08-00 or later
PFM - Agent for Cosminexus	08-00 or later
PFM - Agent for WebLogic Server	08-00 or later
PFM - Agent for Virtual Machine	08-51 or later
All PFM - RMs	All versions

## 16.3.1 Configuring the status management function

### (1) Setting up the status management function

The status management function is a function provided by PFM - Manager and PFM - Base.

The status management function is enabled by default if PFM - Base or PFM - Manager version 08-00 or later is newly installed. However, the setting prior to installation is used in the following cases:

- When PFM - Manager version 06-70 to 07-10 is upgraded to version 08-00 or later
- When a new installation of version 08-00 or later of PFM - Manager or PFM - Base is performed in an environment where version 06-70 to 07-00 of PFM - Agent is installed

Because Performance Management versions 06-70 to 07-00 do not have the status management function, the setting is disabled.

The following describes how to enable and disable the status management function.

Note:

The Status Server service for the status management function is assigned a fixed port number by default.

#### (a) Enabling the status management function

To enable the status management:

1. Stop Performance Management services.

If Performance Management services are running on a physical host, stop the services by using the following command:

```
jpcspm stop -key jplpc
```

To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpccconf stat enable` command.

To enable the status management function, use the following command:

```
jpccconf stat enable
```

3. Check the status of the status management function.

To confirm that the status of the status management function is available, use the following command:

```
jpccconf stat display
```

4. Start Performance Management services.

To start all Performance Management services on a physical host, use the following command:

```
jpcspm start -key jplpc
```

To start all of Performance Management's services on a logical host, use the cluster software.

## (b) Disabling the status management function

To disable the status management function:

1. Stop Performance Management services.

If Performance Management services are running on a physical host, stop the services by using the following command:

```
jpcspm stop -key jplpc
```

To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpccconf stat disable` command.

To disable the status management function, use the following command:

```
jpccconf stat disable
```

3. Check the status of the status management function.

To confirm that the status of the status management function is `unavailable`, use the following command:

```
jpccconf stat display
```

4. Start Performance Management services.

To start all of Performance Management services on a physical host, use the following command:

```
jpcspm start -key jplpc
```

To start all of Performance Management services on a logical host, use the cluster software.

Note:

The service key that can be specified by the `jpcspm start` and `jpcspm stop` commands differs depending on whether the status management function is enabled or disabled.

For details on each command, see the manual *JPI/Performance Management Reference*.

### 16.3.2 How to check the service status

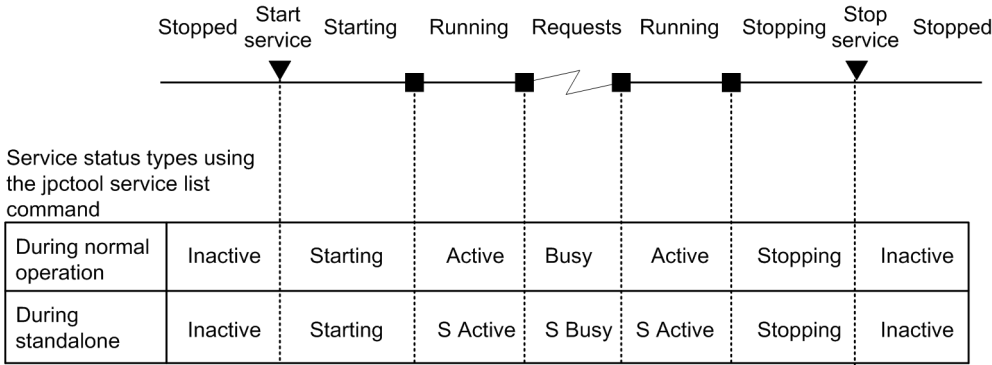
The service status information that can be checked by the `jpctool service list` command differs depending on whether the status management function is enabled or disabled. The following subsections indicate the different situations in which service status information can be checked.

#### (1) When the status management function is enabled

If the status management function is enabled, the `jpctool service list` command can be used to check detailed status information while a service is running or stopped.

Figure 16–9: Status information if the status management function is enabled

Service status



The following figures show an example configuration when the status management function is enabled in PFM - Manager and PFM - Agent or PFM - RM and an example of output of the `jpc tool service list` command.

Figure 16–10: Example of system configuration if the status management function is enabled

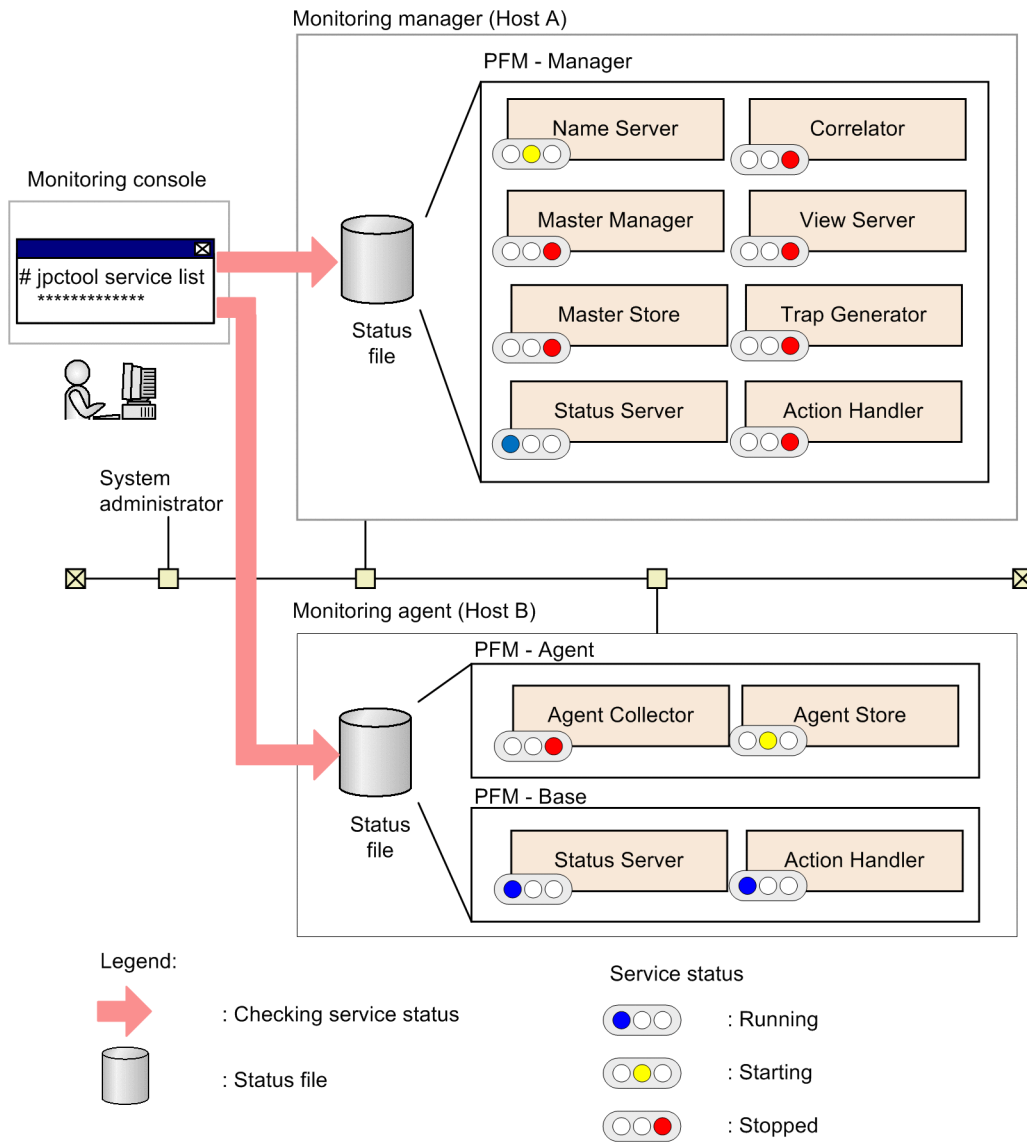


Figure 16–11: Example of output of the `jpctool service list` command

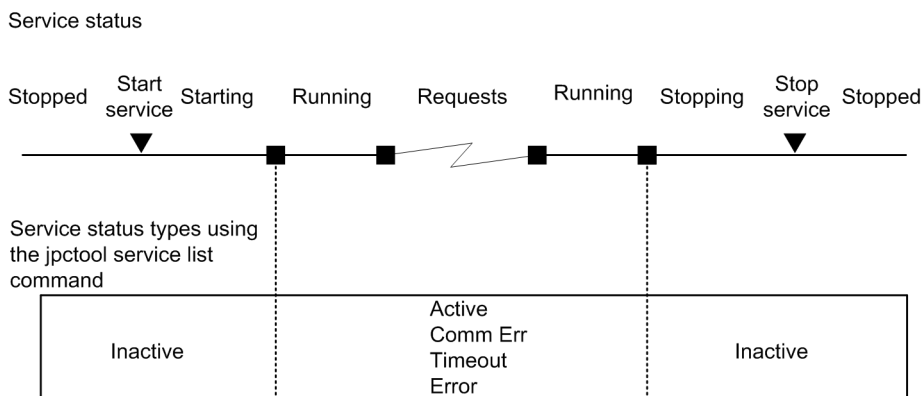
```
# jpctool service list -id * -host *
Host Name      ServiceID      Service Name    PID    Port    Status
-----
HOSTA          PT1HOSTA      Status Server   483    8206    Busy
HOSTA          PN1001        Name Server     6588
HOSTA          PM1001        Master Manager
HOSTA          PS1001        Master Store
HOSTA          PE1001        Correlator
HOSTA          PC3HOSTA     Trap Generator
HOSTA          PP1HOSTA     View Server
HOSTA          PH1HOSTA     Action Handler
HOSTB          PT1HOSTB     Status Server   9876   22291   Busy
HOSTB          PH1HOSTB     Action Handler   4872   1116    Active
HOSTB          OS1inst1[HOSTB] Agent Store     4321
HOSTB          OA1inst1[HOSTB] Agent Collector

KAVE06003-I List processing of the service information terminated normally.
```

## (2) When the status management function is disabled

If the host has a version installed that does not support the status management function or if the function is disabled on the host, when the `jpctool service list` command is executed, a message is displayed explaining that the status management function is not supported. When this happens, the following status information is displayed. The service status cannot be checked, however, if PFM - Manager is not running.

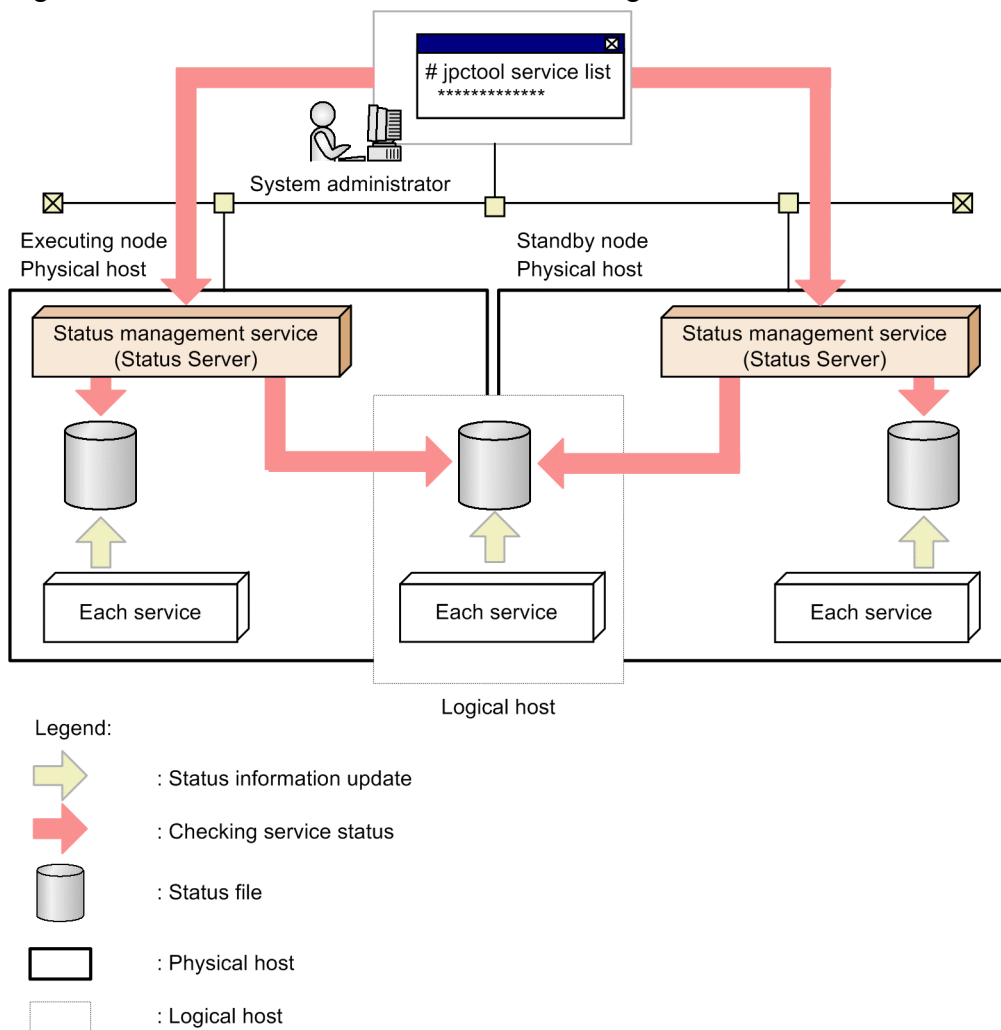
Figure 16–12: Status information if the status management function is disabled



### 16.3.3 Status management during cluster system operation

Only one Status Server service is started per host. As a result, when the cluster system is running, the status of the services on the physical and logical hosts is managed by the Status Server service on the physical host.

Figure 16–13: Overview of the status management function when the cluster system is used



Note:

If the cluster system is in an active-active configuration, configure the Status Server service so that the service does not failover or so that the service always starts up.

### 16.3.4 When a problem occurs within the status management function

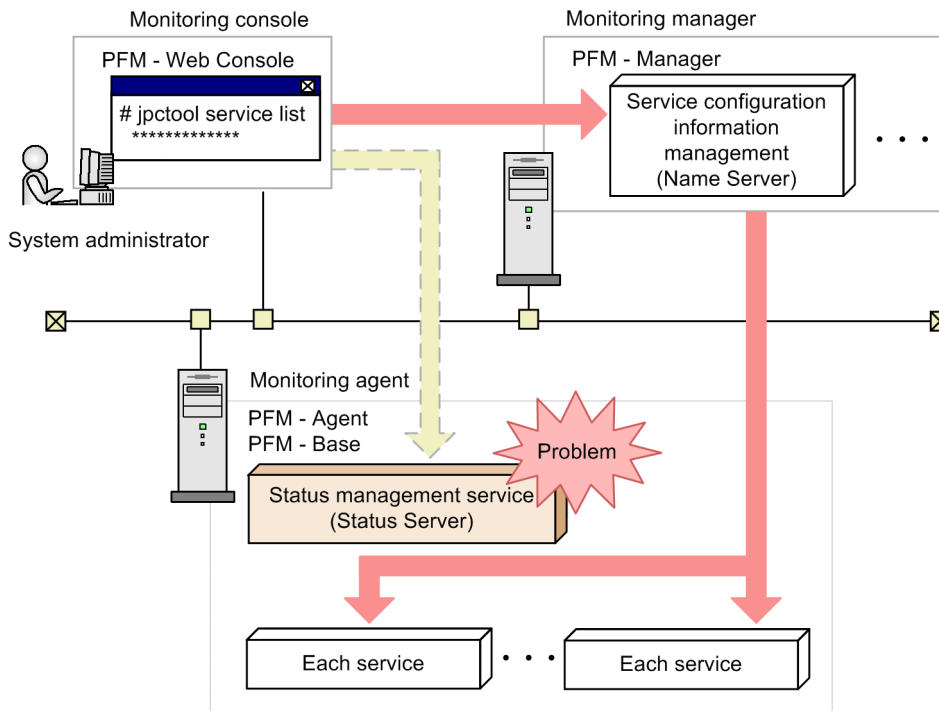
This section gives details about checking the service status when a problem occurs within the status management function.

#### (1) When the Status Server service stops abnormally



When the Status Server service is stopped, the KAVE00203-W message is output to the common message log. In this case, the detailed service status cannot be checked, but the service status can be checked with the same method as when the status management function is disabled. The service status cannot be checked, however, when PFM - Manager is not running.



Figure 16–14: Example of when the Status Server service stops abnormally



Legend:

-  : Checking status using the status management function
-  : Checking status using PFM - Manager

## (2) When a service other than the Status Server service stops abnormally

If a service other than the Status Server service stops abnormally, the status file contents might not be properly updated. In this case, the status management function determines the service status based on the internal file generated by each service. As a result, the service status can be checked in the same manner as when the status management function is enabled.

## 16.4 Using the PFM service automatic restart functionality to restart PFM services

This section describes the PFM service automatic restart functionality, which is used to automatically restart PFM services that have stopped abnormally.

Performance Management provides the PFM service automatic restart functionality, which you can use you to automatically restart a PFM service in the unlikely event that it stops abnormally for some reason. The PFM service automatic restart functionality has the following two functionalities:

### Automatic restart functionality

If a PFM service stops abnormally for some reason, the PFM service automatic restart functionality restarts the PFM service so that it continues monitoring. If you are not using a cluster system, which provides high system availability, we recommend that you consider using this functionality.

### Scheduled restart functionality

The scheduled restart functionality allows you to schedule the restart of a PFM service so that it continues monitoring even if there is a problem with the OS or the service itself (such as a memory or handle leak) that prevents the service from running for an extended period of time. This functionality is typically not used.

### 16.4.1 Prerequisites for using the PFM service automatic restart functionality

You must install version 09-00 or later of PFM - Base or PFM - Manager on the host and enable the status management function. For PFM-RM, any version of the program can be used. To restart PFM - Agent services, the PFM - Agent version must be 08-00 or later. Even if other versions of PFM - Agent are installed on the host, the PFM service automatic restart functionality can automatically restart the PFM - Agent services and the Action Handler service that match the criteria. The following table describes possible product combinations on the same host and support for automatic service restart for each PFM service.

Table 16–19: Possible product combinations on the same host and support for automatic service restart

PFM - Manager or PFM - Base version	Whether automatic restart of the service is available								
	PFM - Agent 08-00 or later, or PFM - RM			Earlier version than PFM - Agent 08-00			No PFM - Agent		
	M	A	AH	M	A	AH	M	A	AH
PFM - Manager 09-00 or later	Y	Y	Y	Y	N	Y	Y	n/a	Y
Earlier version than PFM - Manager 09-00	N	N	N	N	N	N	N	n/a	N
PFM - Base 09-00 or later	n/a	Y	Y	n/a	N	N	n/a	n/a	N
Earlier version than PFM - Base 09-00	n/a	N	N	n/a	N	N	n/a	n/a	N
None	n/a	n/a	n/a	n/a	N	N	n/a	n/a	n/a

Legend:

M: PFM - Manager service

A: PFM - Agent service

AH: Action Handler service

Y: Available

N: Not available

n/a: Not applicable or impossible combination

The only PFM services that the PFM service automatic restart functionality can restart are the ones running on physical hosts. The functionality cannot restart the Status Server service. When Performance Management is used in a cluster system, use cluster software to control the PFM services running on logical hosts. The PFM service automatic restart functionality does not restart the services running on logical hosts.

## 16.4.2 Service startup unit for the PFM service automatic restart functionality

The service startup unit for the PFM service automatic restart functionality is the minimum unit that can be specified in the `jpcspm start` command. The following table lists the service startup units of the PFM service automatic restart functionality.

Table 16–20: Service startup unit for the PFM service automatic restart functionality

Service	Service startup unit
PFM - Manager service	<ul style="list-style-type: none"><li>Name Server service</li><li>Master Manager service</li><li>Master Store service</li><li>Correlator service</li><li>Trap Generator service</li><li>View Server service</li></ul>
PFM - Agent service	<ul style="list-style-type: none"><li>Agent Collector service</li><li>Agent Store service</li></ul> <p>However, for a multi-instance agent, the instances can be started individually. For a health check agent, the PFM - Manager services are started as well.</p>
PFM - RM service	<ul style="list-style-type: none"><li>Remote Monitor Collector service</li><li>Remote Monitor Store service</li></ul>
Action Handler service	Action Handler service

## 16.4.3 Configuring the PFM service automatic restart functionality

In the **Services** tree of PFM - Web Console, you can specify the property to configure the PFM service automatic restart functionality for each service. For a health check agent, use the Agent Collector service to set the automatic restart functionality for the agent. If a service does not meet any of the above prerequisite conditions, the property for this setting is not displayed. The following table lists the properties to be set for each target service.

Table 16–21: Correspondence between the service names targeted for automatic restart and the service names to be used for setting the service properties

Supported service	Use this for setting the service property
PFM - Manager service <ul style="list-style-type: none"><li>Name Server</li></ul>	Master Manager

Supported service	Use this for setting the service property
<ul style="list-style-type: none"> <li>• Master Manager</li> <li>• Master Store</li> <li>• Correlator</li> <li>• Trap Generator</li> <li>• View Server</li> </ul>	Master Manager
PFM - Agent service <ul style="list-style-type: none"> <li>• Agent Collector</li> <li>• Agent Store</li> </ul>	Agent Collector
PFM - RM service <ul style="list-style-type: none"> <li>• Remote Monitor Collector</li> <li>• Remote Monitor Store</li> </ul>	Remote Monitor Collector
Action Handler service <ul style="list-style-type: none"> <li>• Action Handler</li> </ul>	Master Manager, Agent Collector, and Remote Monitor Collector <sup>#</sup>

#:

The property settings for each of these services are shared across the same host, regardless of which program is used to make the property settings.

If there are multiple instances of PFM - Agent or PFM - RM that are of the same type and that use the same data model, you can distribute the property settings to these multiple hosts.

The following table lists the setting items for each target service.

**Table 16–22: Setting items for the service automatic restart functionality**

Folder name	Property name	Description
Restart Configurations	Restart when Abnormal Status <sup>#1</sup>	Specifies whether the service is to be restarted when the automatic restart functionality detects an <code>Abnormal Status</code> <sup>#2</sup> . This setting is applied to all services on the host. The default is <code>Yes</code> . <code>Yes</code> : Restarts <code>No</code> : Does not restart
	Restart when Single Service Running <sup>#1</sup>	Specifies whether the service is to be restarted when the automatic restart functionality detects a <code>Single Service Running</code> <sup>#3</sup> . This setting is applied to all services on the host. The default is <code>No</code> . <code>Yes</code> : Restarts <code>No</code> : Does not restart
<i>Service-name</i> <sup>#4</sup>	Auto Restart	Specifies whether to use the automatic restart functionality for the target service. The default is <code>No</code> . <code>Yes</code> : Uses the automatic restart functionality. <code>No</code> : Does not use the automatic restart functionality.
	Auto Restart - Interval(Minute)	Specifies, in minutes, how often the automatic restart functionality checks the operating status when the function is used. You can specify an integer value from 1 to 1440. The default is 10 (minutes).
	Auto Restart - Repeat Limit	Specifies how many times the automatic restart functionality attempts to restart the service when the functionality is used. You can specify an integer value from 1 to 10. The default is 5 (times).

Folder name	Property name	Description
<i>Service-name</i> <sup>#4</sup>	Scheduled Restart	Specifies whether to use the scheduled restart functionality for the service. The default is No. Yes: Uses the scheduled restart functionality. No: Does not use the scheduled restart functionality.
	Scheduled Restart - Interval	Specify an integer value from 1 to 1,000 for the interval between restarts when you use the scheduled restart functionality. The default is 1. The units for the interval are specified in the Scheduled Restart - Interval Unit.
	Scheduled Restart - Interval Unit	Specifies the restart interval units (Month/Week/Day/Hour) used by the scheduled restart functionality for restarting the service when the functionality is used. The default is Month. Month Week Day Hour
	Scheduled Restart - Origin - Year	Specifies the calendar year from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 1971 to 2035 <sup>#5</sup> . The default is the current year <sup>#6</sup> .
	Scheduled Restart - Origin - Month	Specifies the month of the year from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 1 to 12 <sup>#5</sup> . The default is the current month <sup>#6</sup> .
	Scheduled Restart - Origin - Day	Specifies the day of the month from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 1 to 31 <sup>#5</sup> . The default is the current date <sup>#6</sup> .
	Scheduled Restart - Origin - Hour	Specifies the hour of the day from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 0 to 23. The default is the current hour <sup>#6</sup> .
	Scheduled Restart - Origin - Minute	Specifies the minute of the hour from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 0 to 59. The default value is the current minute <sup>#6</sup> .

#1:

The property settings for each of these services are shared across the same host, regardless of which program is used to make the property settings.

#2:

Indicates that the Status Server service cannot obtain the status of the PFM service normally (for example, because the PFM service has ended abnormally due to an exception).

#3:

Indicates that only one of the PFM - Agent or PFM - RM services is running.

#4:

The Master Manager services shown are the PFM - Manager and Action Handler services. The Agent Collector or Remote Monitor Collector services shown are the PFM - Agent or PFM - RM and Action Handler services.

#5:

If a non-existing date (such as 2007/2/30) is specified, the last day of the month is assumed.

#6:

The date and time displayed for the property is based on the time zone setting of the host running the service.

Note:

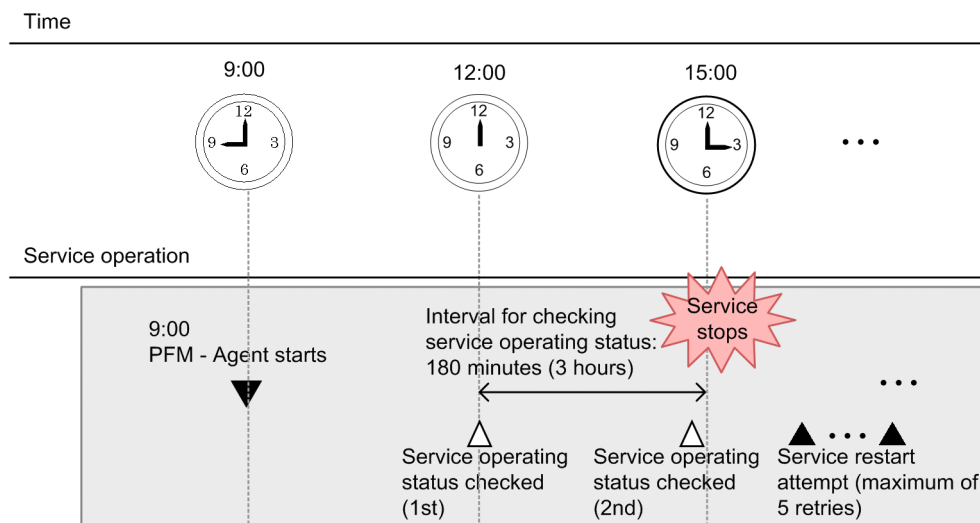
Placing priority on continued monitoring, the PFM service automatic restart functionality restarts only specific services. The PFM - Manager services link with each other at a high level, so if only particular services are restarted, some of these links may fail. If you use the scheduled restart functionality for a PFM - Manager service, you should also set any PFM - Manager services that usually start after that service to restart. Adjust the restart time so that the services are restarted in the correct order. For details on the start sequence for PFM - Manager services, see [1.1.1 Start sequence for the entire Performance Management system](#). If you use the automatic restart functionality for a PFM - Manager service, after you restart the service you should select a time when there will be the least impact on system operation and stop all PFM - Manager services, and then restart them. To realize high availability of the PFM - Manager services, we recommend you use a cluster system.

## 16.4.4 Using the PFM service automatic restart functionality

### (1) Automatic restart functionality

The following figure shows an example of operating a system by using the automatic restart functionality. In this example, the automatic restart functionality checks the operating status of the Agent Collector service every three hours, and if the service stops, it restarts the service.

Figure 16–15: Example of using the automatic restart functionality



Legend:

- ▼ : PFM - Agent starts
- △ : Service operating status is checked
- ▲ : Service is restarted by the automatic restart function

#### Restart Configurations settings

Restart when Abnormal Status: Yes (default)

## Agent Collector service settings

Auto Restart: Yes

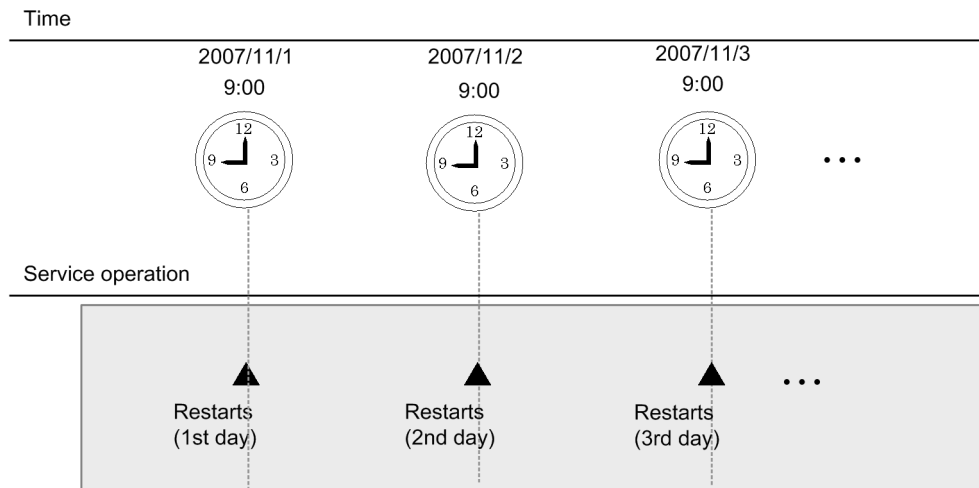
Auto Restart - Interval (minute): 180

Auto Restart - Interval (minute): 5 (default)

## (2) Scheduled restart functionality

The following figure shows an example of operating a system by using the scheduled restart functionality. In this example, a PFM - Agent service is restarted at 9:00 every day.

Figure 16–16: Example of using the scheduled restart functionality



Legend:

▲ : Service is restarted by the periodic restart function

## Agent Collector service settings

Scheduled Restart: Yes

Scheduled Restart - Interval: 1 (default)

Scheduled Restart - Interval Unit: Day

Scheduled Restart - Origin - Year: 2007 (year)

Scheduled Restart - Origin - Month: 11 (month)

Scheduled Restart - Origin - Day: 1 (day)

Scheduled Restart - Origin - Hour: 9 (hour)

Scheduled Restart - Origin - Day: 0 (minute)

## 16.5 Detecting problems by linking with the integrated system monitoring product

The JP1/Base log file trapping function can be used to change the contents of Performance Management's common message log to JP1 events. Therefore, when a problem occurs within Performance Management, the problem can be detected with JP1/IM by issuing a JP1 event.

However, to detect problems other than those that occur within Performance Management, we recommend that you use the health check function. For details on the health check function, see [16.2 Using the health check function to check the operating status of monitoring agents and their hosts](#).

The following subsections describe the steps to link Performance Management with the JP1/Base log file trapping function and issue a JP1 event.

### 16.5.1 Configuring the output method of the common message log

In order to link with the JP1/Base log file trapping function, the output method of Performance Management's common message log must be configured.

The following table shows the log file output methods Performance Management supports:

Table 16–23: Log file output format supported by Performance Management

Log file output method	Description	Output log file name
Sequential file method	This method always writes the newest log information to a file called <code>jpcllog01</code> . When the log file size reaches the set value, the file is renamed from <code>jpcllog01</code> to <code>jpcllog02</code> , and the file is saved. Then a file named <code>jpcllog01</code> is created, and the newest log information is written to this file.	<code>installation-folder\log\jpcllog{01 02}</code>
Wrap-around file method	When the log file size reaches the set value, the next log file contents are cleared, and the newest log information is written in the next log file. The file to be written to changes in the following manner: the file after <code>jpcllogw01</code> is <code>jpcllogw02</code> and the file after <code>jpcllogw02</code> is <code>jpcllogw01</code> .	<code>installation-folder\log\jpcllogw{01 02}</code>

Note:

- With the wrap-around file method, the time of the most recent update for the log file is used to determine the newest log information. Therefore, an error might occur if the time is changed on the host on which Performance Management is running or if the most recent update time for the log file is modified.
- Because versions earlier than 08-00 do not support the wrap-around file method, the log is output using the sequential file method even if the wrap-around file method is specified for the common message log's output method. In this case, versions earlier than 08-00 output the log to `jpcllog` and versions 08-00 and later output the log to `jpcllogw`.
- The sequential file method used is SEQ2 and the wrap-around file method used is WRAP2.

To configure the log output method:

1. Stop all Performance Management services on the host on which the log output method is to be changed.



2. Open the file `jpccomm.ini` with a program such as a text editor.
3. Change the log file trapping method of the common message log.  
Correct the shaded part indicated below:

```

:
[Common Section]

```

```
Common Msglog Type=0|1
```

```

:
```

Table 16–24: Items to edit in the file `jpccomm.ini`

Section	Label	Values	Default value	Description
[Common Section]	Common Msglog Type	0 1	0	Log file output method for the common message log. <ul style="list-style-type: none"> <li>• 0: Sequential file method</li> <li>• 1: Wrap-around file method</li> </ul>

Note the following when editing the file `jpccomm.ini`:

- Do not enter a space at the beginning of a line or before or after an equal sign.
  - The file `jpccomm.ini` contains definition information in addition to the common message log file size. Do not change any values other than `Common Msglog Type` in the section `Common Section`. Performance Management might not run properly if values other than that for the required item are changed.
4. Save, and then close the file `jpccomm.ini`.
  5. Start Performance Management services.

Notes:

- The settings for the common message log file are shared by the Performance Management programs on the same host.
- Backup the file `jpccomm.ini` as necessary.

## 16.5.2 Example of creating a definition file for the JP1/Base log file trapping function

For example, if the message `KAVE00116-E` is output to the common message log with the wrap-around method (WRAP2), the action definition file for issuing a JP1 event with a severity of `Abnormal` and event ID of `999` is described below.

Figure 16–17: Example of configuring the JP1/Base action definition file

```

:
```

```
FILETYPE=WRAP2
```

```
HEADLINE=0
```

```
RECTYPE=VAR '\n'
```

```
ACTDEF=<Error>999 "KAVE00116-E"
```

```

:
```

For details on the JP1/Base action definition file, see *JP1/Base User's Guide*.

### 16.5.3 Starting the JP1/Base log file trapping function

Execute the following commands to start the JP1/Base log file trapping function:

- For Windows:

```
jp1/base-installation-directory\bin\jevlogstart -r -f action-definition-  
file-name performance-management-installation-directory\  
log\jpclogw01 performance-management-installation-directory\log\jpclogw02
```

- For UNIX:

```
jp1/base-installation-directory/bin/jevlogstart -r -f action-definition-  
file-name performance-management-installation-directory/  
log/jpclogw01 performance-management-installation-directory/log/jpclogw02
```

For details on the JP1/Base log file trapping function, see *JP1/Base User's Guide*.

# 17

## Error Handling Procedures

This chapter explains how to handle any errors that might occur while you are using Performance Management.

## 17.1 Error handling procedures

---

### Checking the event

Check the following:

- Context in which the problem occurred
- Content of the message (when a message is output)
- Common message logs and other log information

For details on the messages and how to respond to each message, see the chapter that describe the messages in the manual *JP1/Performance Management Reference*. For details on the log information output by Performance Management, see *17.4 Log information to be output when Performance Management is used*.

### Data to be collected

Collect data to determine the cause of an error. For details on collecting the necessary data, see *17.5 Data to be collected in the event of trouble* and *17.6 Procedures for collecting data in the event of trouble*.

### Determining the cause

Use the collected data to determine the cause and the extent of the error, as well as the range of its consequences.

## 17.2 Troubleshooting

If an error occurs while you are using Performance Management, you should first check to see if any of the events described in this section have occurred.

Table 17–1: Errors

Classification	Error	Reference
Setting up and starting service	<ul style="list-style-type: none"> <li>• A Performance Management program service (other than PFM - Web Console) does not start.</li> <li>• The PFM - Web Console service does not start.</li> <li>• A service takes a long time to start once startup is requested.</li> <li>• Immediately after a Performance Management program service is stopped, another program starts service and communication is not performed properly.</li> <li>• After the message <code>The disk capacity is insufficient</code> is output, the Master Store service, Agent Store service, or Remote Monitor Store service stops.</li> <li>• The Correlator service takes a long time to start after PFM - Manager restarts.</li> <li>• The Agent Collector service or Remote Monitor Collector service does not start.</li> <li>• Multiple agents that start simultaneously take a long time to recover from stand-alone mode.</li> </ul>	<a href="#">17.2.1</a>
Connecting to agents	An error message, such as <code>Cannot connect to an agent</code> is output to PFM - Web Console.	<a href="#">17.2.3</a>
Logging on to PFM - Web Console	<ul style="list-style-type: none"> <li>• The specified Performance Management user name is not recognized during logon.</li> <li>• A connection from PFM - Web Console to PFM - Manager (View Server service) cannot be established.</li> <li>• The login window is not displayed in the web browser.</li> <li>• A security warning window is displayed in the web browser.</li> </ul>	<a href="#">17.2.4</a>
Executing commands	<ul style="list-style-type: none"> <li>• When the <code>jpctool service list</code> command is executed, the names of services not operating are output.</li> <li>• When the <code>jpctool db dump</code> command is executed, the output data does not match the data in the specified Store database.</li> <li>• Deleted agents are displayed.</li> </ul>	<a href="#">17.2.5</a>
Agent management	<ul style="list-style-type: none"> <li>• No agent is displayed in the Agents window of PFM - Web Console.</li> <li>• The operating status of the server or agent is <code>Unconfirmed</code> or <code>Not Supported</code>.</li> </ul>	<a href="#">17.2.6</a>
Report definition	<ul style="list-style-type: none"> <li>• There is a time period not indicated on the history report.</li> <li>• A memory shortage can occur with the View Server service when a large number of reports are displayed simultaneously.</li> </ul>	<a href="#">17.2.7</a>
Alarm definition	<ul style="list-style-type: none"> <li>• The program defined to be executed by an action does not work properly.</li> <li>• No alarm event is displayed.</li> <li>• Although the threshold value for an alarm is exceeded, the color of the alarm icon that is displayed in the Display Alarm Status window in the Agents tree remains green.</li> <li>• Many alarms are generated when an alarm table is deleted.</li> </ul>	<a href="#">17.2.8</a>

Classification	Error	Reference
Collecting and managing performance data	<ul style="list-style-type: none"> <li>• Even if the data storage time is set for a shorter period, the size of the Store database for the Agent Store service and the Remote Monitor Store service does not become smaller.</li> <li>• The KAVE00128-E message (Illegal data was detected in the Store database) or KAVE00163-E message (The database type is illegal) is output to the common message log and startup of the Store service fails.</li> <li>• Collection of performance data is skipped and the KAVE00213-W message is output.</li> </ul>	17.2.9
Monitoring suspension function	<ul style="list-style-type: none"> <li>• The KAVJS6570-I message is output to the Monitoring Suspension Settings window.</li> <li>• The KAVE06189-W message is output during command execution.</li> </ul>	17.2.10
Linking with other programs	<ul style="list-style-type: none"> <li>• JP1 events are not reported when linking with JP1/IM.</li> <li>• Monitored PFM - Agent or PFM - RM is not displayed in the monitoring tree window when linking with a monitored object function of JP1/IM.</li> <li>• The display color of the monitored object does not change when linking with a monitored object function of JP1/IM.</li> <li>• Startup of the JP1 system event monitor fails.</li> <li>• Performance Management reports cannot be displayed from the console of JP1/IM or JP1/AJS3.</li> </ul>	17.2.11
Multiple monitoring	<ul style="list-style-type: none"> <li>• When the <code>jpctool config mgrimport</code> command is executed, an error is output.</li> </ul>	17.3.1
	<ul style="list-style-type: none"> <li>• The host name is not distributed to agents when the <code>jpccconf primmgr notify</code> command is executed.</li> </ul>	17.3.2
	<ul style="list-style-type: none"> <li>• The host name is not distributed to the primary Manager when the <code>jpccconf primmgr notify</code> command is executed.</li> </ul>	17.3.3
	<ul style="list-style-type: none"> <li>• A connection from PFM - Web Console to PFM - Manager cannot be established.</li> </ul>	17.3.4
	<ul style="list-style-type: none"> <li>• No agent is displayed on the secondary Manager.</li> </ul>	17.3.5
	<ul style="list-style-type: none"> <li>• Multiple actions are executed in one event.</li> <li>• No events are sent to the secondary Manager.</li> <li>• Events are sent to the secondary Manager but actions are not executed.</li> <li>• Events are sent to both the primary Manager and the secondary Manager but actions are executed only on the primary Manager.</li> <li>• When the primary Manager is down, no action is executed in response to an event notification.</li> </ul>	17.3.6
	<ul style="list-style-type: none"> <li>• A connection from the time the JP1/IM's Event Console starts monitoring to PFM - Web Console cannot be established.</li> </ul>	17.3.7
	<ul style="list-style-type: none"> <li>• PFM-related settings cannot be specified from JP1/SLM.</li> </ul>	17.3.8

## 17.2.1 Troubleshooting problems related to setup and service startup

### (1) A Performance Management program service (other than PFM - Web Console) does not start

Possible causes and solutions:

- PFM - Manager stopped

If PFM - Manager and PFM - Agent or PFM - RM are installed on the same host, the PFM - Agent or PFM - RM service cannot start when PFM - Manager is stopped. Determine whether the PFM - Manager service has started. If the PFM - Manager service has not started, start the service. For details on service startup, see [1. Starting and Stopping Performance Management](#).

- The same port number is set for multiple Performance Management program services.

When the same port number is set for multiple Performance Management program services, none of the Performance Management program services can start. Since port numbers are allocated automatically by default, they cannot be duplicated. When port numbers for Performance Management program services are fixed during Performance Management setup, check the port number settings. If the same port number is set for more than one Performance Management program service, you must make appropriate corrections in the port number settings. For details on how to set a port number, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

- There is an error in a setting for a Store database installation directory.

If any of the following directories are set to a directory that cannot be accessed or a directory that does not exist, the Agent Store or Remote Monitor Store service cannot start. Review the directory name and attributes, and correct the settings if necessary.

- Store database installation directory
- Store database backup directory
- Store database partial backup directory
- Store database export directory
- Store database import directory

In addition, if one of these directories is set for multiple Agent Store or Remote Monitor Store services, the Agent Store or Remote Monitor Store service cannot start. Review the directory settings and correct the settings if necessary.

- The host name of the machine was changed using a non-permitted procedure.

For details on how to change the host name of the machine, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*. Under some circumstances when the host name is changed using a procedure other than those permitted, a Performance Management program service might not start. This is the reason why the following issues might occur.

- The KAVE00493-E message is output to the common message log and services cannot start.  
For details on how to recover from this event, see [17.2.2 Recovery method when the KAVE00493-E message is output and services cannot start](#).
- If you execute the `jpctool service list -id * -host *` command on a host where the service has not started, a service with a duplicate service ID will appear in the *Service Name* column.

For details on the `jpctool service list` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

- When you stopped the PFM - Agent and changed the PFM - Agent host name while the PFM - Agent was not connect to PFM - Manager.

Each Performance Management service registers its own service information (IP address, host name, and port number) in PFM - Manager when it is starting and deletes the information when it is stopping. If a service is not able to delete its service information when it was stopping because it could not communicate with PFM - Manager for some reason, the service information remains on the PFM - Manager side. Then, if the service tries to start using the same service information it used the previous time it started, the attempt will fail. This is because Performance Management does not allow a duplicate service instance to be started. (KAVE00133-E is output to the common message log on the host where the attempt to start the service failed.) In such a case, perform the following procedure to change the service information:

1. Execute the `jpcconf port define` command to unlock the PFM - Agent port (if it is locked).
2. Restart the PFM - Agent service.
3. Execute the `jpcconf port define` command again to relock the PFM - Agent port (if necessary).

For details on the `jpcconf port define` command, see the chapters that describe commands in the manual *JPI/Performance Management Reference*.

- A previously started process still exists.

If a previously started process still exists, the service of the process cannot be started, because Performance Management does not allow a duplicate service instance to be started. Use Task Manager (for Windows) or the `ps` command (for UNIX) to check whether a process exists for a service that could not start successfully. If such a process exists, terminate it.

- An error has occurred in the service control manager.

When the `jpcspm start` command is executed in Windows, the KAVE05163-E message is output and the service might not start. Take the corrective action shown in the message.

## (2) The PFM - Web Console service does not start

Possible causes and solutions are provided below. If only causes are provided, take the corrective action provided in *17.2.1(1) A Performance Management program service (other than PFM - Web Console) does not start*.

- The same port number is set for multiple Performance Management program services.
- A previously started process still exists.
- An error has occurred in the service control manager.
- If encrypted communication is enabled, required files are not stored in the folder for storing encrypted communication files.

Make sure that the files required for encrypted communication are correctly stored. For details, see the procedure that describes where to store encrypted communication files in the *JPI/Performance Management Planning and Configuration Guide*.

- If encrypted communication is enabled, the wrong files are stored in the folder for storing encrypted communication files.

If the required files are correctly stored but the service does not start, the files might be invalid. Check the log and replace the erroneous files with valid files.

The log storage destination is as follows:

- Windows

`PFM-Web-Console-installation-folder\CPSB\httpsd\log\error.xxx#`

- UNIX

`/opt/jplpcwebcon/CPSB/httpsd/log/error.xxx#`

#: xxx is a sequential number that begins with 001.



The log is displayed in the format shown below. Check the line that shows `crit` in the *error-level* column.

```
[date-and-time] [error-level] [message]
```

The following shows the messages and the causes:

No.	Message	Cause
1	The private key doesn't match the public key	The private key file is not paired with a server certificate file (or a self-signed certificate file).
2	Bad password for the private key	The private key file is not paired with a private key password file.

### (3) A service takes a long time to start once startup is requested

It might take a long time for service to actually start once you execute the `jpcspm start` command or start a service by selecting **Services** in Windows. If the following factors are the reason for this, subsequent service startups should take less time.

- Starting a service in standalone mode might slow down the startup of the service.
- During initial startup after the Store database is restored, the indexes of the Store database must be rebuilt. This might slow startup of the service.
- During initial startup after an Agent is newly added, the indexes of the Store database must be created. This might slow startup of the service.
- If normal end processing for the Store service cannot be performed due to a power interruption or other reason, the indexes of the Store database are rebuilt at restart; therefore, it might take a long time for the Store service to start.

### (4) Immediately after a Performance Management program service is stopped, another program starts service and communication is not performed properly

Immediately after stopping a Performance Management program service, another program service might start that uses the same port that the stopped service was using. In this case, communication might not be performed properly. You can use either of the following techniques to avoid this problem:

- Fix the port numbers to be allocated to the Performance Management program services.  
Allocate a fixed port number to each Performance Management program service. For details on how to set a port number, see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

- Set the `TCP_TIMEWAIT` value.

Use the `TCP_TIMEWAIT` value to set a connection wait time.

For HP-UX or AIX, specify a connection wait time of at least 75 seconds, as follows:

- In HP-UX: `tcp_time_wait_interval:240000`
- In AIX: `tcp_timewait:5`

In Windows or Solaris, use the default connection wait time setting. The default settings are:

- In Solaris: 4 minutes
- In Windows: 2 minutes

In Linux, you cannot change the connection wait time setting from the default of 60 seconds. If this problem occurs in Linux, use the technique to fix the port numbers of the Performance Management program services.

## (5) After the message "The disk capacity is insufficient" is output, the Master Store service or Agent Store service stops

If there is insufficient space on the disk used by the Store database, the storing of data to the Store database is cancelled. In this case, after the message `The disk capacity is insufficient` is output, the Master Store service, Agent Store service, or Remote Monitor Store service stops.

If this message appears, use either of the following techniques to solve this problem.

- Allocate sufficient disk space.  
Estimate the disk usage of the Store database and change the storage location of the Store database to a disk with sufficient space. For details on how to estimate the disk usage of the Store database, see the system requirements in an appendix of each PFM - Agent or PFM - RM manual.  
For details on how to change the storage location of the Store database for event data, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*. For details on how to change the storage location of performance data, see each PFM - Agent or PFM - RM manual.
- Modify the data retention conditions of the Store database.  
Modify the data retention conditions of the Store database and adjust the upper limit for the amount of data in the Store database. For details on how to change the retention conditions of the Store database, see [4.1.2 Modifying the retention conditions for performance data \(in Store 2.0\)](#), [4.1.3 Modifying the retention conditions for performance data \(in Store 1.0\)](#), or [4.2.1 Changing the maximum number of records for event data](#).

If the Master Store service, the Agent Store service, or the Remote Monitor Store service does not start even after taking these actions, there may be some unrecoverable logical errors in the Store database. In this case, you must restore the Store database from the backup data, and then restart the Master Store service, the Agent Store service, or the Remote Monitor Store service. If you have no backup data, you must initialize the Store database, and then start the Master Store service, the Agent Store service, or the Remote Monitor Store service. To initialize the Store database, delete all of the following files in the installation directories of the Store database:

When the Store database version is 1.0

- Files with the extension `.DB`
- Files with the extension `.IDX`

When the Store database version is 2.0

- Files with the extension `.DB`
- Files with the extension `.IDX`

Delete the files in the STPI, STPD, and STPL directories.

(Do not delete the STPI, STPD, and STPL directories themselves.)

The following shows the default installation directories of the Store database.

Store database installation directory for performance data:

For details, see the appropriate PFM - Agent or PFM - RM manual.

Store database installation directory for event data:

When PFM - Manager is in a non-cluster environment

- In Windows:  
`installation-folder\mgr\store\`
- In UNIX:  
`/opt/jp1pc/mgr/store/`

When PFM - Manager is in a cluster environment

- In Windows:  
*environment-directory\jplpc\mgr\store\*
- In UNIX:  
*environment-directory/jplpc/mgr/store/*

## (6) The Correlator service takes a long time to start after PFM - Manager restarts

The Correlator service checks alarm status on agents when it starts. If you restart PFM - Manager without stopping agents, the Correlator service might take some time to start. If you want to prevent this, consider enabling the Correlator quick start function.

When you enable the Correlator quick start function, the Correlator service checks alarm status on agents after it starts when necessary. As a result, the Correlator service requires less time to start. When the Correlator service reports checked alarm status, PFM - Manager might issue agent events containing one of the following messages.

Message	Description
State information	The Correlator service received an alarm event from an agent and successfully checked the alarm status.
State information (Unconfirmed)	The Correlator service received an alarm event from an agent but could not check the alarm status.
State change (Unconfirmed)	The Correlator service received an alarm event from an agent whose alarm status was unknown. The Correlator service assumed the status of PFM - Agent or PFM - RM based on the content of the received alarm event.

The following table describes the triggers that prompt PFM - Manager to issue agent events containing the messages described in the above table.

Status of the Correlator quick start function	Trigger for the Correlator service to check alarm status	Success or failure of alarm status checking and message to be included in agent events	
		Success	Failure
Disabled (when the Retry Getting Alarm Status label is enabled in the startup information file (jpccomm.ini))	When PFM - Manager starts	State information	State information (Unconfirmed)
	When the Correlator service fails to check alarm status on an agent and receives the next alarm event from the agent	State information	State change (Unconfirmed)#
Enabled	When PFM - Manager starts and then the Correlator service receives the first alarm event from an agent	State information	State information (Unconfirmed)
	When the Correlator service fails to check alarm status on an agent and then receives the next alarm event from the agent	State information	State change (Unconfirmed)#

#

The message is output only when the status of PFM - Agent or PFM - RM that is assumed by PFM - Manager changes.

To enable or disable the Correlator quick start function:

1. Stop the Performance Management programs and services.

When the Performance Management programs and services are running on the PFM - Manager host, execute the `jpcspm stop` command to stop all of them. When Performance Management is running in a cluster system, use cluster software to stop all the Performance Management programs and services.

2. Use a text editor to open the `jpccomm.ini` file on the PFM - Manager host.

The `jpccomm.ini` file is stored in the following location:

For a physical host

- For Windows  
`installation-folder\`
- For UNIX  
`/opt/jp1pc/`

For a logical host

- For Windows  
`environment-directory\jp1pc\`
- For UNIX  
`environment-directory/jp1pc/`

3. Enable or disable the Correlator quick start function.

In the `jpccomm.ini` file, in the `Common Section` section, set a desired value for the following label.

- Enabling the function  
`Correlator Startup Mode=1`
- Disabling the function  
`Correlator Startup Mode=0`

4. Save and close the `jpccomm.ini` file.

5. Start the Performance Management programs and services.

## (7) The Agent Collector service or Remote Monitor Collector service does not start

Suppose the OS of a PFM - Agent host or a PFM - RM host is Windows, PFM - Agent or PFM - RM starts, and the Agent Collector service or the Remote Monitor Collector service fails to start. When that occurs and Windows restarts, the following message might be output to a Windows event log.

- `service-name service hung on starting.`

These messages appear when the Windows Service Control Manager times out. The Service Control Manager is likely to time out if the communication load on PFM - Manager is high and PFM - Manager takes a long time to issue a response. These messages are output if all of the following conditions are met:

- The communication load on PFM - Manager is high.  
For example, many instances of startup processing for PFM - Agent or PFM - RM are simultaneously executed.
- In **Services** in Windows, the startup type for the PFM - Agent or PFM - RM services is set to automatic.

- The OS is restarted.

To prevent the Service Control Manager from timing out, perform either of the following procedures:

- If you want to start the services when the OS restarts, use the `jpcspm start` command instead of the Windows Service Control Manager.
- Perform the following on PFM - Agent or PFM - RM hosts to reduce the startup time for PFM - Agent or PFM - RM.

The following procedure reduces the reconnection processing time when PFM - Agent or PFM - RM cannot connect to PFM - Manager when the PFM - Agent or PFM - RM services start. If that occurs, the PFM - Agent or PFM - RM services are highly likely to start in standalone mode.

To reduce the startup time for PFM - Agent or PFM - RM, in the startup information file (`jpccomm.ini`), in `Agent Collector x Section#` and `Agent Store x Section#`, change the value for the `NS Init Retry Count` label from `NS Init Retry Count = 2` to `NS Init Retry Count = 1`.

<sup>#</sup>  
`x` represents the product ID of PFM - Agent or PFM - RM. For details on product IDs, see the list of identifiers in the appendix in the applicable PFM - Agent or PFM - RM manual. When multiple instances of PFM - Agent or PFM - RM are installed on the same host, set the value for the `NS Init Retry Count` label for each product ID.

The startup information file (`jpccomm.ini`) is stored in the following location:

If a PFM - Agent or PFM - RM host is a physical host

`installation-folder\jpccomm.ini`

If a PFM - Agent or PFM - RM host is a logical host

`environment-directory#\jplpc\jpccomm.ini`

<sup>#</sup>  
 Indicates a directory on the shared disk that is specified when a logical host is created.

## **(8) Multiple agents that start simultaneously take a long time to recover from stand-alone mode**

A monitoring agent that enters stand-alone mode during startup automatically tries to reconnect to the monitoring manager. If it succeeds, the monitoring agent enters normal mode.

If you start multiple monitoring agents simultaneously, communication from each monitoring agent to the monitoring manager is concentrated and connection errors will occur, and multiple monitoring agents might enter stand-alone mode. At that time, if those monitoring agents try to reconnect to the monitoring manager repeatedly at the same time it will cause a concentration of communication and the monitoring agents might be delayed in entering normal mode.

When such an event occurs, change the value of the `Random Retry Mode` label (the dispersion of the reconnection) of the `Common Section` section of the startup information file (`jpccomm.ini`) to 1 (enabled).

This operation allows attempts to reconnect from monitoring agents in stand-alone mode to the monitoring manager to be made at random intervals rather than at regular intervals and can thus avoid communication concentration.

Note that these settings are applicable when the version of PFM - Manager or PFM - Base in the system is 10-10-20 or later and the version of PFM - Agent or PFM - RM is 10-00 or later.

For details on how to change the startup information file (`jpccomm.ini`), see the part that explains the startup information file (`jpccomm.ini`) in the appendixes of the manual *JPI/Performance Management Reference*.

## 17.2.2 Recovery method when the KAVE00493-E message is output and services cannot start

When a physical host name used as the monitoring host name of PFM - Manager, PFM - Agent, or PFM - RM is changed improperly, subsequent service startup is suppressed. In addition, the KAVE00493-E message is output to avoid data being corrupted. In such a situation, identify the current physical host name and then recover from the event by using the methods shown below according to the type of service to start.



### Note

If you cannot identify the current physical host name, execute the `jpccconf host hostmode -display` command to check the method of obtaining the monitoring host name. You can see the command for checking the physical host name from the method of obtaining the monitoring host name. For details, see the chapter that explains commands in the manual *JPI/Performance Management Reference*.

Recovery method when a PFM - Manager service cannot start

Recover from the event according to the contents of (1) and (2).

Recovery method when a PFM - Agent or PFM - RM service cannot start

You can recover from the event by correctly performing the procedure of changing the physical host name of the corresponding host again.

For details on how to change the physical host name, see the chapters on installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

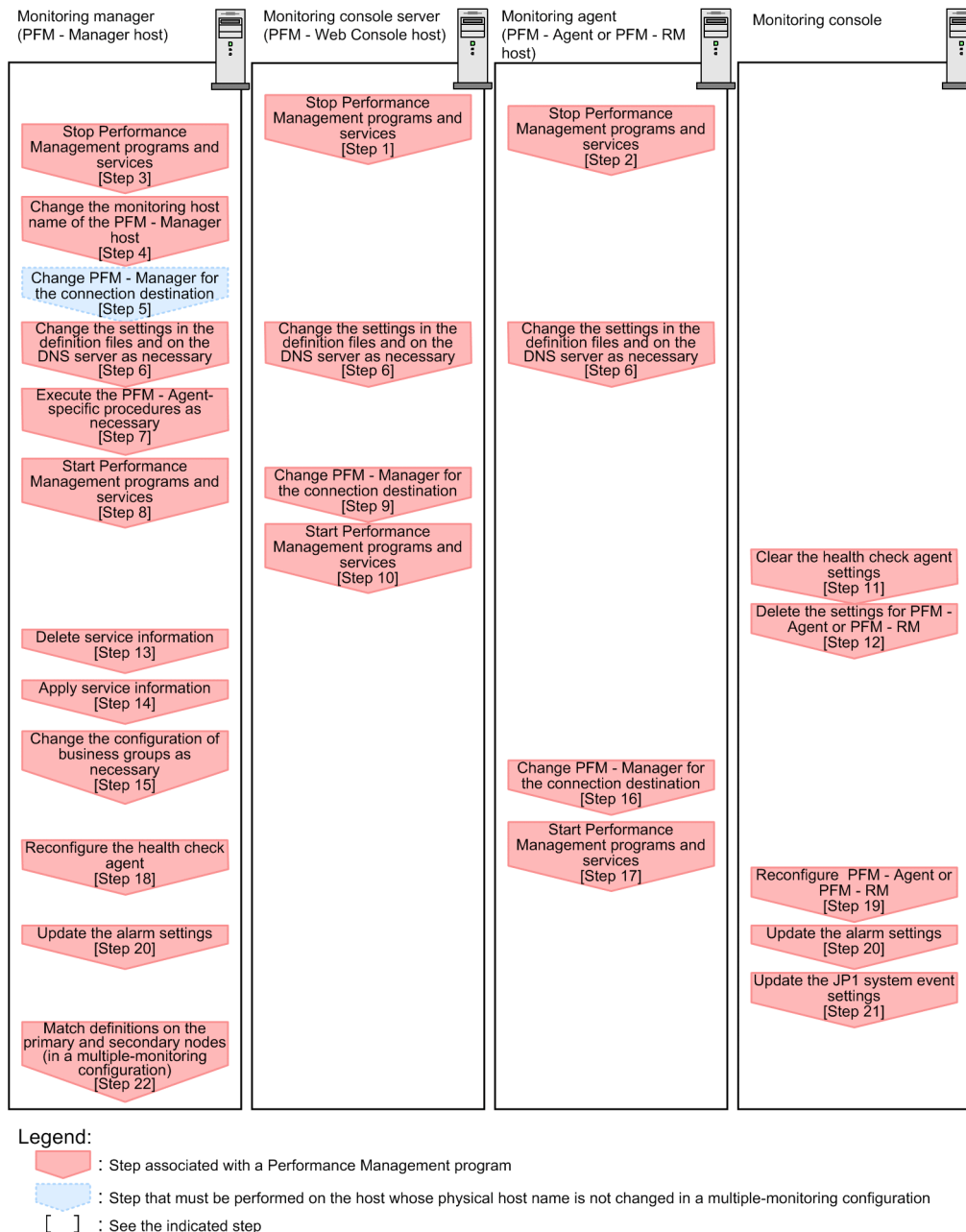
Note that the operation to change the physical host name itself is not needed because it has already been performed. Additionally, if the KAVE05217-E message is output during service stop and the service fails to stop, edit the `jpchosts` file so that the old host name can be resolved, and then re-execute the command. (If the service stops, restore the contents of the `jpchosts` file.)

### (1) Recovery procedure when the KAVE00493-E message is output and services cannot start (PFM - Manager)

To recover from this event, you need to perform the following operation on each host of the monitoring manager, monitoring console server, and monitoring agent, as well as on the monitoring console.

The following figure shows the procedure of the operation.

Figure 17–1: Recovery procedure when the KAVE00493-E message is output and services cannot start



## (2) Recovery procedure when the KAVE00493-E message is output and services cannot start

To recover from this event, you need to match the current physical host name with the monitoring host name to be used in the operation monitoring system, and delete the old information.

### Prerequisite conditions

- For details on commands to be used for operation, see the chapter that explains commands in the manual *JP1/Performance Management Reference*.
- If a host that you operate is running as a logical host, start or stop services by using the cluster software.



- There are commands that need a specific option (`-lhost logical-host-name`) when a host on which the commands are executed is running as a logical host. Check the details of a command and then execute the command (the example of command execution in the procedure below is for a host running as a physical host).

## Operation

1. Stop services on the PFM - Web Console host.

Stop all the Performance Management programs and services on the PFM - Web Console host connecting to PFM - Manager whose host name was changed. To do so, use the `jpcwstop` command.

In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

2. Stop services on the PFM - Agent or PFM - RM host.

Stop all the Performance Management programs and services on the PFM - Agent or PFM - RM host connecting to PFM - Manager whose host name was changed. To do so, use the `jpcspm stop` command.

3. Stop services on the PFM - Manager host.

Stop all the Performance Management programs and services on the PFM - Manager host whose host name was changed. To do so, use the `jpcspm stop` command.

In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

Note that if the KAVE05217-E message is output during command execution and the service fails to stop, edit the `jpchosts` file so that the old host name can be resolved, and then re-execute the command. (If the service can stop, restore the contents of the `jpchosts` file.)

4. Change the monitoring host name of the PFM - Manager host.

Change the monitoring host name by executing the `jpccconf host hostname` command on the PFM - Manager host whose host name was changed.

The following is an example of executing the command to change the physical host name to `hostB`:

In Windows:

```
jpccconf host hostname -newhost hostB -d d:\backup -dbconvert convert
```

In UNIX:

```
jpccconf host hostname -newhost hostB -d /var/tmp/backup -dbconvert convert
```

Note that when the `jpccconf host hostname` command is executed, information such as definition information or performance information before the change is all inherited.

5. Change the settings of the connection-target PFM - Manager (for multiple-monitoring configuration)

Change the settings of the connection-target PFM - Manager by executing the `jpccconf mgrhost define` command on the PFM - Manager host whose host name is not changed.

6. If necessary, change the `jpchosts` file, `hosts` file, and the DNS settings so that the new host name can be resolved in the Performance Management system.

If the machine needs to restart, change the settings so that the Performance Management programs and services do not start automatically after restart. After operation on the PFM - Manager host is complete, restore the settings so that the Performance Management programs and services start automatically.

7. If necessary, perform a procedure specific to PFM - Agent.

In a configuration in which PFM - Agent is installed on a PFM - Manager host whose host name was changed, you might have to perform a procedure specific to PFM - Agent.



Table 17–2: Necessity of PFM - Agent-specific procedure

Configuration		Necessity of procedures and reference
PFM - Agent 09-00 or later is installed on the PFM - Manager host.		The necessity of procedures specific to PFM - Agent differs by PFM - Agent. For details, see the chapter that describes installation and setup in each PFM - Agent manual.
The version of PFM - Agent installed on the PFM - Manager host is earlier than 09-00.	The following PFM - Agents: <ul style="list-style-type: none"> <li>• PFM - Agent for Cosminexus</li> <li>• PFM - Agent for Domino</li> <li>• PFM - Agent for Enterprise Applications</li> <li>• PFM - Agent for Microsoft SQL Server</li> </ul>	The PFM - Agent-specific procedure is necessary. For details, see the section that describes the optional PFM - Agent-specific procedure to be performed when the monitoring host name is changed in the <i>JPI/Performance Management Planning and Configuration Guide</i> .
	Other than the above	The PFM - Agent-specific procedure is not necessary.

If you need to perform a procedure specific to PFM - Agent, perform the procedure described in the reference shown in the table, and then go to the next step.

8. Start services on the PFM - Manager host.

Start the Performance Management programs and services on the PFM - Manager host. To do so, use the `jpcspm start` command.

In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

9. Change the settings of the connection-target PFM - Manager on the PFM - Web Console host.

Change the settings of the connection-target PFM - Manager on the PFM - Web Console host connecting to PFM - Manager whose host name was changed. To do so, change the initialization file (`config.xml`). For details, see the part that explains the initialization file (`config.xml`) in the appendix of the manual *JPI/Performance Management Reference*.

10. Start services on the PFM - Web Console host.

Start the Performance Management programs and services on the PFM - Web Console host connecting to PFM - Manager whose host name was changed. To do so, use the `jpcwstart` command.

11. Delete the health check agent settings.

If the health check function is used, delete the agent definition of a health check agent with service ID that contains the old host name from PFM - Web Console (delete from the management folder in the Agents tree and the association with alarm tables).

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on how to change the agent definition, see [3. Monitoring Agents](#) or [6. Monitoring Operations with Alarms](#).

12. Delete the PFM - Agent or PFM - RM settings.

From PFM - Web Console, delete the agent definition of the PFM - Agent or PFM - RM host with the service ID containing the old host name installed on the same host as the PFM - Manager whose host name was changed. Remove this agent definition from the management folder in the Agents tree.

In a multiple-monitoring configuration, perform this step on the primary system. For details on how to change the agent definition, see [3. Monitoring Agents](#) or [6. Monitoring Operations with Alarms](#).

For details about how to change the agent definition, see [3. Monitoring Agents](#).

### 13. Delete service information on the PFM - Manager host.

Even though the PFM - Manager host name is changed, the service information of the Performance Management programs with the old host name remains the same. Therefore, you need to delete unnecessary information. In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

The types of service information that you need to delete and the method of checking the service information are described as follows:

#### *Service information on the host with the old host name*

All the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id "*" -host old-host-name
```

#### *Service information whose service ID contains the old host name*

Items whose Service ID column contains the old host name of the items that are displayed by executing the following command must be deleted:

```
jpctool service list -id "*" -host old-host-name
```

Service information can be deleted by using the `jpctool service delete` command.

Delete service information on the host with the old host name by using the following command:

```
jpctool service delete -id "*" -host old-host-name
```

Additionally, delete service information whose service ID contains the old host name by using the following command:

```
jpctool service delete -id "???old-host-name" -host new-host-name
```

If the message KAVE05233-W is issued during command execution because of a service information deletion error, re-execute the command as follows:

```
jpctool service delete -id "*" -host old-host-name -force  
jpctool service delete -id "???old-host-name" -host new-host-name -force
```

#### *Note*

Even though you execute the `jpctool service list` command, old service information containing the old host name that remains in the database might not be displayed. Because such service information also needs to be deleted from the database, you must execute the `jpctool service delete` command shown above.

### 14. Apply the service information to PFM - Manager.

Synchronize the service information between PFM - Manager and PFM - Web Console so that the deletion of service information takes effect in PFM - Web Console. To do so, use the `jpctool service sync` command.

In a multiple-monitoring configuration, perform this step on both the primary and secondary managers.

The time when the service information synchronized by the `jpctool service sync` command takes effect depends on the version of PFM - Web Console.

### 15. Change the business group configuration if needed.

If the PFM - Manager host whose host name was changed is assigned to a business group, you need to change the configuration of the business group.

In a multiple-monitoring configuration, perform this step on the primary manager.

For details on the procedure, see [2.7 Setting and using business groups](#).

### 16. Change the settings for the connection-target PFM - Manager on the PFM - Agent or PFM - RM host.

Change the settings of the connection-target PFM - Manager on the PFM - Agent or PFM - RM host connecting to PFM - Manager whose host name was changed. To do so, use the `jpccconf mgrhost define` command. For example, if the host name of the connection-target PFM - Manager was changed to `hostB`, execute the following command:

```
jpccconf mgrhost define -host hostB
```

In this example, the `jpccconf mgrhost define` command is executed in interactive mode. However, the command can also be executed in non-interactive mode.

17. Start services on the PFM - Agent or PFM - RM host.

Start the Performance Management programs and services on the PFM - Agent or PFM - RM host connecting to PFM - Manager whose host name was changed. To do so, use `jpccspm start` command.

18. Reconfigure the definition of a health check agent.

If the health check function is used, reconfigure the definition (that was deleted in step 11) of a health check agent after changing the host name.

In a multiple-monitoring configuration, perform this step on the primary manager.

19. Reconfigure the definition of PFM - Agent or PFM - RM.

Reconfigure the definition (that was deleted in step 12) of PFM - Agent or PFM - RM which has been installed on the same host as PFM - Manager whose host name was changed.

In a multiple-monitoring configuration, perform this step on the primary manager.

20. Update the alarm settings.

In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

In a multiple-monitoring configuration, perform this step on the primary manager.

- The action handler of the PFM - Manager host is specified for the action handler that executes actions.  
Edit the alarm to set `PH1<new-PFM - Manager-host-name>` for the action handler that executes actions.
- JP1 events are issued by actions.  
Reconfigure the JP1 events of actions.

For details on how to edit alarms, see [6. Monitoring Operations with Alarms](#).

21. Update the JP1 system event settings.

If either of the conditions below is met, you need to update the JP1 system event settings from PFM - Web Console. In a multiple-monitoring configuration, perform this step on the primary manager.

- The old host name is specified as the name of the event server to which JP1/Base connects for JP1 system events.
- The old host name is specified as the name of the monitoring console host for JP1 system events.

For details on the JP1 system events, see [12. Linking with the Integrated Management Product JP1/IM for Operation Monitoring](#).

22. Match definition information between the primary and secondary managers (for multiple-monitoring configuration).

Export the definition information for multiple-monitoring from the primary manager, and then import it to the secondary manager to match the definition information between the primary and secondary managers.

For details on the procedure for matching definition information, see [11.5 Duplicating definition information](#).

23. Make a post-setting-change check.

After changing settings, perform the following checks:

- Collecting performance data  
Operate the system for more than twice the time specified for the collection interval of performance data, and confirm that performance data is properly collected.
- Executing the `jpchrpt` command  
Confirm that collected performance data is properly output.
- Checking the report definition and alarm definition  
Confirm that there is no problem with the report definition and alarm definition created in a Web browser.
- Checking action execution  
Confirm that a created alarm executes properly.

### 17.2.3 Troubleshooting problems related to connecting to agents

This subsection describes the possible causes and solutions for cases when PFM - Web Console displays error messages such as `Cannot connect to an agent` or `No agent is displayed`.

- The communication between PFM - Manager and PFM - Agent or PFM - RM is the cause of a problem.
- On the PFM - Manager host, execute `ping PFM - Agent-host-or-PFM - RM-host` and `ping IP-address-of-PFM - Agent-or-PFM - RM-host` to check the following:
  - Whether it is possible to communicate with the PFM - Agent host
  - If it is possible to communicate, whether the IP address matches that used by the PFM - Agent or PFM - RM host
  - If the `jpchosts` or `hosts` file is used, whether the IP address is correctly set in the file on PFM - Manager and PFM - Agent or PFM - RM hosts

Performance Management performs name resolution in the order of `jpchosts`, `hosts`, and DNS.

- On the PFM - Agent host or PFM - RM host, execute `ping PFM - Manager-host` and `ping IP-address-of-PFM - Manager-host` to check the following:
  - Whether it is possible to communicate with the PFM - Manager host
  - If it is possible to communicate, whether the IP address matches the address used by the PFM - Manager host
  - If the `jpchosts` or `hosts` file is used, whether the IP address is correctly set in the file on the PFM - Manager and PFM - Agent or PFM - RM hosts

Performance Management performs name resolution in the order of `jpchosts`, `hosts`, and DNS.



#### Tip

Ping traffic might be able to pass through firewalls depending on their settings. If communications via ping traffic are possible but the Performance Management system cannot perform communications, check the firewall routing.

- The firewall routing is the cause of a problem.  
If a firewall is configured between PFM - Manager and PFM - Agent or between PFM - Manager and PFM - RM, check whether fixed ports are assigned to PFM - Manager, PFM - Agent and PFM - RM, and whether traffic is allowed to pass through the firewalls.  
For details on firewall routing, see the manual *JP1/Performance Management Reference*.
- Non-existent PFM - Agent or PFM - RM in the system is selected.

When you execute `jpctool service list -id * -host *` on the PFM - Manager host, check whether the old host names are displayed.

If the old host names are displayed, on the PFM - Manager host, execute the `jpctool service delete` command to delete the service information of agents. Then execute the `jpctool service sync` command to synchronize the service information registered in PFM - Manager and PFM - Web Console.

For details on the commands, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

## 17.2.4 Troubleshooting problems related to logging on to PFM - Web Console

### (1) The specified Performance Management user name is not recognized during logon.

A specified Performance Management user account might not exist. Use the user name `ADMINISTRATOR` to log on to PFM - Web Console from the monitoring console, and then use the Users window to confirm whether a Performance Management user account has been created. If no Performance Management user account has been created, create one now.

If the user name that failed for logon was a business group user name, the business group might not be assigned to the user. Use the user name `ADMINISTRATOR` to log on to PFM - Web Console from the monitoring console, and then use the Users window to check whether the business group has been assigned to the user. If no business group has been assigned, assign one now.

For details on how to create Performance Management user accounts and assign business groups, see [2. Managing User Accounts and Business Groups](#).

### (2) A connection from PFM - Web Console to PFM - Manager (View Server service) cannot be established.

Possible causes and solutions:

- There is an error in the host name or port number specified in the Windows initialization file (`config.xml`). Confirm whether the host name and port number are correct. Correct any incorrect settings, restart PFM - Web Console, and then re-execute the operation.
- The View Server service has not been initialized.  
The services or processes required to start the View Server service might not have been started. Wait a moment and then re-execute the operation.
- The PFM - Manager host is using an IP address that does not enable a connection from the PFM - Web Console host.  
When multiple IP addresses are set for the PFM - Manager host or an IP address translation (such as NAT) is performed between PFM - Manager and PFM - Web Console, a connection might not be established. In this case, the host name must be for with PFM - Manager. For details on how to set host names, see the list of port numbers in an appendix of the manual *JPI/Performance Management Reference*.
- PFM - Web Console is connected to a PFM - Manager that has a function enabled on it that PFM - Web Console does not support.

If the version of the connected PFM - Manager is newer than that of PFM - Web Console, check that there are no functions enabled on the PFM - Manager that are not supported by PFM - Web Console.

If such a function is enabled, disable the function or consider upgrading the PFM - Web Console to a newer version.

The following table lists the corresponding functionality and PFM - Web Console versions that support the functionality.

Functionality	Supported in
Functionality for binding multiple alarm tables	PFM - Web Console 09-00 or later
Functionality for controlling access using business groups	PFM - Web Console 10-00 or later
Monitoring suspension function	PFM - Web Console 10-50 or later

### (3) The login window is not displayed in the web browser

Possible causes and solutions:

- The URL is invalid.  
If encrypted communication is enabled, specify a URL that begins with `https`.  
If encrypted communication is not enabled, specify a URL that begins with `http`.
- If encrypted communication is enabled, web browser settings are invalid.  
Enable TLS communication in the web browser settings.  
For details, see the description about how to configure a web browser to use the monitoring console in the *JPI/Performance Management Planning and Configuration Guide*.

### (4) A security warning window is displayed in the web browser

If encrypted communication is enabled, a security warning window is displayed according to the specified certificates.

The following are possible causes and examples of corrective actions and warning messages:

- The root certificate has not been imported into the web browser or the wrong root certificate has been imported.  
Import the root certificate issued by the certificate authority from which you acquired the server certificate.  
A warning message such as the following is displayed in the window:
  - Internet Explorer  
The security certificate on this Web site was not issued by a trusted certificate authority
  - Firefox  
The certificate is not trusted because no issuer chain was provided or The certificate does not come from a trusted source
- The server certificate stored in the folder for storing encrypted communication files on PFM - Web Console has expired.  
Renew the server certificate and update the settings. For details, see the section on changing the settings for encrypted communication between a web browser and the monitoring console server in the *JPI/Performance Management Planning and Configuration Guide*.  
A warning message such as the following is displayed in the window:
  - Internet Explorer  
The security certificate on this Web page has either expired or is invalid
  - Firefox



The certificate expired on (date)

- The host name (Common Name) specified in the server certificate does not match the host name of the URL in the login window.

Make sure that the host name (Common Name) specified in the server certificate matches the host name of the URL in the login window. If a host name in FQDN format is specified in Common Name, the URL in the login window must also be in the format *host-name + domain-name*.

You can use the `jpctool https output certtext` command to check the host name (Common Name) specified in the server certificate. For details about the command, see the section that describes the command in the manual *JPI/Performance Management Reference*.

A warning message such as the following is displayed in the window:

- Internet Explorer

The security certificate on this Web site was issued for the address of another Web site.

- Firefox

This certificate is valid only for the host name (Common Name) that is configured in the server certificate.

## 17.2.5 Troubleshooting problems related to executing commands

### (1) When the `jpctool service list` command is executed, the names of services that are not operating are output

Possible causes and solutions:

- A Performance Management program was uninstalled without its service information being deleted.  
Service information for a Performance Management program remains in the database even after the program is uninstalled. Execute the `jpctool service delete` command to delete the service information. For details on the `jpctool service delete` command, see the chapter that describe commands in the manual *JPI/Performance Management Reference*.
- The host name was changed without deleting the service information for a Performance Management program.  
If the host name is changed without deleting the service information for a Performance Management program, the service information for the service ID with the previous host name added remains in the database managed by the Master Manager service. Execute the `jpctool service delete` command to delete the service information. For details on the `jpctool service delete` command, see the chapter that describe commands in the manual *JPI/Performance Management Reference*. For details on how to change the host name, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

### (2) When the `jpctool db dump` command is executed, the output data does not match the data in the specified Store database

Specifying the same export file name for the same Store service in multiple executions of the `jpctool db dump` command causes the initial output results to be overwritten with the subsequent output results. Each time you execute the `jpctool db dump` command for the same Store service, specify a different export file name. For details on the `jpctool db dump` command, see the chapter that describe commands in the manual *JPI/Performance Management Reference*.

### (3) Deleted agents are displayed

Before executing the `jpctool service delete` command, you must unbind alarms. If you do not unbind alarms, deleted agents might be displayed for the alarm tables bound to the agents. This phenomenon occurs when you do the following:

- Select the **Show Bound Agents** method in the Alarms window of PFM - Web Console.
- Execute the `jpctool alarm list` command.

In this case, resolve the problem as follows:

1. Make a copy of the corresponding alarm table. Give the copy a new name.  
Example: Alarm table name: AAA -> AAA2
2. Delete the corresponding alarm table.  
Example: Delete alarm table AAA.
3. Copy back the alarm table copied in step 1, giving it the original name.  
Example: Alarm table name: AAA2 -> AAA
4. Delete the alarm table copy made in step 1.  
Example: Delete the alarm table AAA2.
5. Rebind the alarm table to the agent to which the corresponding alarm table was bound.

## 17.2.6 Troubleshooting problems related to agent management

### (1) No agent is displayed in the Agents window of PFM - Web Console

Agents to be monitored might not be defined. Use PFM - Web Console to define the agents to be monitored. For details on defining agents, see [3. Monitoring Agents](#).

### (2) The operating status of a server or agent is Unconfirmed or Not Supported

If the operating status of a server or an agent displayed in the System Operational Status Summary window of PFM - Web Console becomes `Unconfirmed` or `Not Supported`, perform the following procedure.

Before taking the action, check the operating status of each agent displayed in the navigation frame of the Agents window to identify which agent has an operating status of `Unconfirmed` or `Not Supported`.

The following table lists the locations to check for taking actions for each operation status.

Table 17–3: Locations to check for each operating status

Agent type	Operating status	Window area	
		Server Operational Status	Agent Operational Status
PFM - Agent or Remote Monitor Collector service	Unconfirmed	N/A	See (a).
	Not Supported	N/A	See (b).



Agent type	Operating status	Window area	
		Server Operational Status	Agent Operational Status
Remote agent	Unconfirmed	See (c).	
	Not Supported	See (d).	

Legend:

N/A: Not applicable

**(a) If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as "Unconfirmed"**

If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as `Unconfirmed` in the Agent Operational Status area, the Status Server service is not running on the host that is running the identified agent. Start the Status Server service.

**(b) If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as "Not Supported"**

If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as `Not Supported` in the Agent Operational Status area, the identified agent does not support the status management function. Consider upgrading the agent to a newer version that supports the status management function.

**(c) If there is a remote agent whose operating status is shown as "Unconfirmed"**

If there is a remote agent whose operating status is shown as `Unconfirmed` in the Server Operational Status area or the Agent Operational Status area, follow the procedure below.

1. Identify the Remote Monitor Collector service that corresponds to the identified remote agent.
2. Check whether the identified Remote Monitor Collector service is running.  
 If the Remote Monitor Collector service is not running, start the service.  
 For details about how to check the service status, see *1.6 Checking the status of services*. For details on how to start the services, see *1.2.1 Starting services on monitoring managers and monitoring agents*.  
 If the service is running or if the operating status of the remote agent is still shown as `Unconfirmed`, it is likely that the Remote Monitor Collector cannot communicate with the monitored host. Proceed to step 3.  
 If the operating status changes to `Not Supported` after starting the Remote Monitor Collector service, proceed to *17.2.6(2)(d) If there is a remote agent whose operating status is shown as "Not Supported"*.
3. Check the communication settings for the Remote Monitor Collector service and the monitored host.  
 A Remote Monitor Collector service polls its monitored host to check the operating status. If the system is configured to communicate from behind a firewall, check the firewall configuration. For details on the configuration required to allow polling communication, see the applicable appendix in the appropriate PFM - RM manual.  
 Check the settings for host name resolution.

**(d) If there is a remote agent whose operating status is shown as "Not Supported"**

If there is a remote agent whose operating status is shown as `Not Supported` in the Server Operational Status area or the Agent Operational Status area, follow the procedure below.

1. Identify the Remote Monitor Collector service corresponding to the identified remote agent.

2. Select the identified Remote Monitor Collector service in the navigation frame of the Services window.
3. Click **Properties** in the method frame and select **Health Check Configurations** from the tree area of the Service Properties window.
4. Change the value for **Health Check for Target Hosts** to **Yes**, and click the **Finish** or **Apply** button.
5. Wait until polling is performed again.  
The default polling interval is five minutes.  
If the operating status changes to `Unconfirmed` after the time indicated by the polling interval is reached, proceed to *17.2.6(2)(c) If there is a remote agent whose operating status is shown as "Unconfirmed"*.

## 17.2.7 Troubleshooting problems related to report definition

### (1) There is a time period not indicated on the history report

If the current time of the machine where PFM - Agent or PFM - RM is installed is changed to a time in the future, the history information from before the change to after the change is not saved.

### (2) The View Server service can run out of memory when a large number of reports are displayed simultaneously

#### (a) Windows

If you use PFM - Web Console to collect a large amount of report data, a memory shortage can occur with the View Server service. If this occurs, the `KAVJS5001-I` message is output.

By default, the View Server service runs with a fixed maximum memory size of 256 MB. For this reason, a memory shortage can occur with the service according to the amount of data to be processed, regardless of how much memory is available in the system. (If this error occurs, the View Server service might output a `KAVE00104-E` message.)

You can prevent this problem by using the report cache filing function to reduce the size of memory to be used. To enable the report cache filing function, in the initialization file (`config.xml`), under the `<reportCacheFileMode>` tag under the `<vsa>` tag, specify `true` for `useReportCacheFile`. For details on the initialization file (`config.xml`), see the appendix that describes the initialization file (`config.xml`) in the manual *JP1/Performance Management Reference*.

For the following case, increase the upper limit for the memory used by the View Server service:

- The report cache filing function cannot be used, for example, when PFM - Web Console 09-00 or earlier is used.

By increasing the upper limit for the memory used by the View Server service, more report data can be handled.

To increase the upper limit for the memory used by the View Server service:

1. Stop PFM - Manager.
2. Create an empty file as the name of `jvmopt.ini` in `installation-directory\mgr\viewsvr`.
3. Use a text editor to add the following two lines in `jvmopt.ini`:

```
-Xmxmaximum-memory-size-to-be-used-by-the-View-Server-service  
-Djava.rmi.dgc.leaseValue=172800000
```

4. Save and update `jvmopt.ini`.

5. Restart PFM - Manager.

### Example

The following example increases the maximum size of the memory that can be used by the View Server service to 354 MB:

```
-Xmx384M  
-Djava.rmi.dgc.leaseValue=172800000
```

### Note 1

The value specified with the `-Xmx` option indicates the maximum size of the memory that can be used by the View Server service.

### Note 2

The `-Xmx` option indicates only the maximum size of the memory that can be used by the View Server service. This amount of memory is not always used by the service.

### Note 3

You cannot specify a value greater than 385 MB as the maximum size of the memory that can be used by the View Server service.

### Note 4

If PFM - Manager is running in a logical host environment, change the `jvmopt.ini` file in the installation directory of both the executing node and the standby node.

## (b) In UNIX:

If you use PFM - Web Console to collect a large amount of report data, a memory shortage can occur with the View Server service. If this occurs, the `KAVJS5001-I` message is output.

By default, the View Server service runs with a fixed maximum memory size of 256 MB. For this reason, a memory shortage can occur with the service according to the amount of data to be processed, regardless of how much memory is available in the system. (If this error occurs, the View Server service might output a `KAVE00104-E` message.)

You can prevent this problem by using the report cache filing function to cut down the size of memory to be used. To enable the report cache filing function, in the initialization file (`config.xml`), under the `<reportCacheFileMode>` tag under the `<vsa>` tag, specify `true` for `useReportCacheFile`. For details on the initialization file (`config.xml`), see the appendix that describes the initialization file (`config.xml`) in the manual *JP1/Performance Management Reference*.

For the following case, increase the upper limit for the memory used by the View Server service:

- The report cache filing function cannot be used, for example, when PFM - Web Console 09-00 or earlier is used.

By increasing the upper limit for the memory used by the View Server service, more report data can be handled.

To increase the upper limit for the memory used by the View Server service:

1. Stop PFM - Manager.
2. Use a text editor to search the following line in `/opt/jp1pc/mgr/viewsvr/jpcvsvr:`

```
-Xmxmaximum-memory-size-to-be-used-by-the-View-Server-service\
```

3. Save and update `/opt/jplpc/mgr/viewsvr/jpcvsvr`.

4. Restart PFM - Manager.

### Example

The following example increases the maximum size of the memory that can be used by the View Server service to 354 MB:

```
-Xmx384m \
```

### Note 1

The value specified with the `-Xmx` option indicates the maximum size of the memory that can be used by the View Server service.

### Note 2

The `-Xmx` option indicates only the maximum size of the memory that can be used by the View Server service. This amount of memory is not always used by the service.

### Note 3

When you perform an installation, the `/opt/jplpc/mgr/viewsvr/jpcvsvr` file is overwritten. If you increase the maximum size of the memory that can be used by the View Server service, back up the above file before overwriting the installation, and then overwrite the file with the backup.

### Note 4

You cannot specify a value greater than 385 MB as the maximum size of the memory that can be used by the View Server service.

### Note 5

If PFM - Manager is used in a logical host environment, edit `/opt/jplpc/mgr/viewsvr/jpcvsvr` for both the active and standby servers.

## 17.2.8 Troubleshooting problems related to alarm definition

### (1) The program defined to be executed as an action does not work properly

Possible causes and solutions:

- The machine's login environment does not match the execution environment for the program defined to be executed as an action.

If the login environment does not match the execution environment for the program defined to be executed as an action, execution of the program might not be possible. Determine whether the defined program can be executed as a Performance Management action. The following table lists the execution environment for a program defined to be executed as a Performance Management action.

Table 17–4: Execution environment when a program is executed as a Performance Management action

Execution environment	Windows	UNIX
Account	System account	root user permission

Execution environment	Windows	UNIX
Environment variables	System environment variables when a Performance Management program service starts	root user environment variables when Performance Management starts
Current directory	Folder of the Action Handler service	Directory of the Action Handler service
Shell at startup	(Not applicable)	Login shell with root user permission

- You do not have permissions to execute the defined program.

When the following programs are defined as Performance Management actions, execution of the program might not be possible depending on the restrictions of the execution permissions:

- Programs in an NFS mount directory
- Programs for viewing or updating files in an NFS mount directory

Confirm whether the defined program can be executed as a Performance Management action. For details on the execution environment when a program is executed as a Performance Management action, see [Table 17-4 Execution environment when a program is executed as a Performance Management action](#).

- PFM - Manager or the Action Handler service of PFM - Agent or PFM - RM of the destination host for performing the action has not started.

If the PFM - Manager or the Action Handler service of PFM - Agent or PFM - RM of the destination host for performing the action is stopped, the action cannot be performed. To perform the action, start PFM - Manager and the Action Handler service of PFM - Agent or PFM - RM of the destination host for performing the action.

## (2) No alarm event is displayed

Possible causes and solutions:

- PFM - Manager has not started.

When PFM - Manager is stopped, alarm events from PFM - Agent or PFM - RM might not be issued correctly. To monitor alarm events, start PFM - Manager.

## (3) Although the threshold value for an alarm is exceeded, the color of the alarm icon remains green in the Alarm Status window in the Agents tree

Possible causes and solutions:

- An alarm table that uses multi-byte characters is bound in an environment where the character encodings of the LANG environment variable for the PFM - Manager host, PFM - Agent host, and PFM - RM host do not match.

In such cases, an alarm that uses multi-byte characters is not evaluated normally. Match the character encoding of the LANG environment variable for the PFM - Manager host, PFM - Agent host, and PFM - RM host before operation. For LANG environment variable settings, check the common message logs and check which character encoding is output for the most recent service activation message.

Note that when the PFM - Manager host is using an English environment and when the character encoding is changed while the current settings apply, the characters in the existing alarm definition are garbled and cannot be deleted. Therefore, perform the following:

1. If alarm tables that use multi-byte characters in the alarm definition are necessary, export all the alarm tables from PFM - Web Console.

Note that you cannot use the `jpctool alarm export` command to export alarm tables.

2. Delete all alarm tables that use multi-byte characters in the alarm definition.

3. Stop PFM - Manager.
4. Change the character encoding of the LANG environment variable for the PFM - Manager host.
5. Start PFM - Manager.
6. If you exported alarm tables in step 1, use PFM - Web Console or the `jpctool alarm import` command to import alarm tables.

For notes on environments that have several character encodings, see the chapter describing Performance Management functionality in the *JPI/Performance Management Planning and Configuration Guide*.

## (4) Many alarms are generated when an alarm table is deleted

If you delete an alarm table that is bound to an agent, the alarm status always changes to normal. The following table describes the relationship between alarm status changes and whether alarm events are issued.

#	Alarm status		Whether an event is issued
	Before an alarm table is deleted	After an alarm table is deleted	
1	Abnormal	Normal	An alarm event is issued.
2	Warning	Normal	An alarm event is issued.
3	Normal	Normal	An alarm event is not issued.

When you delete an alarm table, if the status of any of the alarms contained in the alarm table is abnormal or warning, the alarm status of the agent changes from abnormal or warning to normal. When that occurs, an alarm event is issued.

If you delete an alarm table that is bound to multiple agents, many alarm events are generated, possibly exceeding the peak capability temporarily.

You can check whether the peak capability is exceeded by checking whether the following message is output to the common log.

```
KAVE00422-W The number of events waiting to be processed reached the limit.
```

If the KAVE00429-E or KAVE00345-E message is output to the common log in addition to the above message, the Action Handler service has failed to delete action definitions. However, in this case, the alarms that trigger actions are already deleted and any action that has failed to be deleted will not be executed. The action information held by the Action Handler service is restored when the Action Handler service restarts.

## (5) After changing the port number of PFM - Manager during operation, no alarm events are displayed

With PFM - Manager version 11-50 or later, if, after you change the port number setting specified for the Master Manager or Correlator for which the port number has been fixed, you do not restart the PFM services running on the agent host on which PFM - Base version 11-50 or later is installed, alarm events are not displayed. In this case, you need to restart the PFM services on which PFM - Base version 11-50 or later is installed.

For details about how to change the port number setting, see the section describing how to change the port number setting in the *JPI/Performance Management Planning and Configuration Guide*.

## 17.2.9 Troubleshooting problems related to collecting and managing performance data

### (1) Even if the data storage time is set for a shorter period, the size of the Store database for Agent Store does not become smaller

If the file capacity of the Store database is already at its limit in Store version 1.0, the file size will not become smaller even if a shorter data retention period is set. In this case, set a shorter retention period, back up the Store database, and then restore it.

For details on how to set the data retention period, see *4.1.2 Modifying the retention conditions for performance data (in Store 2.0)* or *4.1.3 Modifying the retention conditions for performance data (in Store 1.0)*. For details on how to back up and restore the Agent Store and Remote Monitor Store databases, see *9.3.3 Backing up and restoring the performance data*.

### (2) The KAVE00128-E, KAVE00163-E, or KAV00103-E message is output to the common message log and startup of the Store service fails

Inconsistent data might have been stored in the Store database when a PFM service was unexpectedly stopped or was forcibly stopped due to the machine powering off. To recover from this error:

- If the Store database has been backed up, restore it.
- If the Store database has not been backed up, stop the PFM service containing the Store service that cannot be started (Master Store service, Agent Store service, or Remote Monitor Store service), initialize the Store database, and then start the deactivated PFM service.

After you initialize the Store database, delete all the files in the installation directories of the Store database:

When the Store database version is 1.0

- Files with the extension `.DB`
- Files with the extension `.IDX`

When the Store database version is 2.0

- Files with the extension `.DB`
- Files with the extension `.IDX`

Delete the files in the STPI, STPD, and STPL directories.

(Do not delete the STPI, STPD, and STPL directories themselves.)

The following shows the default installation directories of the Store database.

Store database installation directory for performance data:

For details, see the appropriate PFM - Agent or PFM - RM manual.

Store database installation directory for event data:

When PFM - Manager is in a non-cluster environment

- In Windows:  
`installation-folder\mgr\store\`
- In UNIX:  
`/opt/jplpc/mgr/store/`



When PFM - Manager is in a cluster environment

- In Windows:  
`environment-directory\jplpc\mgr\store\`
- In UNIX:  
`environment-directory/jplpc/mgr/store/`

### (3) Collection of performance data is skipped and the KAVE00213-W message is output

Collection of performance data by the Agent Collector service and Remote Monitor Collector service is scheduled for each record. If the previous collection for the same record or the collection for another record is not completed, the current collection is skipped.

There are two methods for avoiding this event:

- Adjusting the value of the `Collection Offset` property  
This method is effective when the time of collection of historical data overlaps with another one and the collection is skipped.  
In the properties of the Agent Collector service or Remote Monitor Collector service, adjust the value of the `Collection Offset` property for records for which collection is skipped.  
For details on how to change the value of the `Collection Offset` property, see [4.1.1 Modifying the recording options for performance data](#).
- Giving a higher priority to the collection of historical data than to the display processing of real-time reports  
This method is effective when the time of collection of historical data overlaps with that of the collection processing for real-time report display and the collection is skipped. This method is available when the version of PFM - Manager, PFM - Base, and PFM - Web Console in the system is 10-10-20 or later. This method is also available when the version of PFM - Agent or PFM - RM which displays real-time reports is 10-00 or later.  
Change the value of the `Historical Data Collection Priority Mode` label (the history collection priority function) of the startup information file (`jpccomm.ini`) for the monitoring agent to 1 (enabled).  
For details on how to change the startup information file (`jpccomm.ini`), see the part that explains the startup information file (`jpccomm.ini`) in the appendixes of the manual *JPI/Performance Management Reference*.



#### Note

The `Historical Data Collection Priority Mode` label exists in the common section and each Agent Collector section of the `jpccomm.ini` file. If you want to specify the settings collectively for all the Agent Collector services and Remote Monitor Collector services on the host, change the value of the item in the common section. If you want to specify the settings independently for a specific Agent Collector service or Remote Monitor Collector service, change the value of the item in the corresponding Agent Collector section.

Note that both the methods described above are based on the assumption that processing is executed as scheduled. Therefore, in some cases, such as when processing takes longer than planned due to the reduction of response from the monitored target, you might not be able to avoid skipping collection.



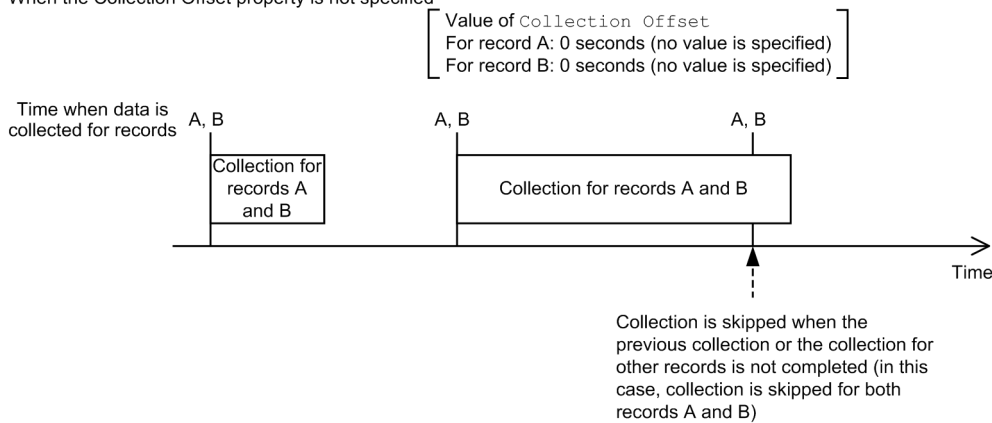
## (a) Difference in how performance data is collected depending on whether the Collection Offset property is specified

If the `Collection Offset` property is specified for a record, the collection for the target record is delayed for the specified value.

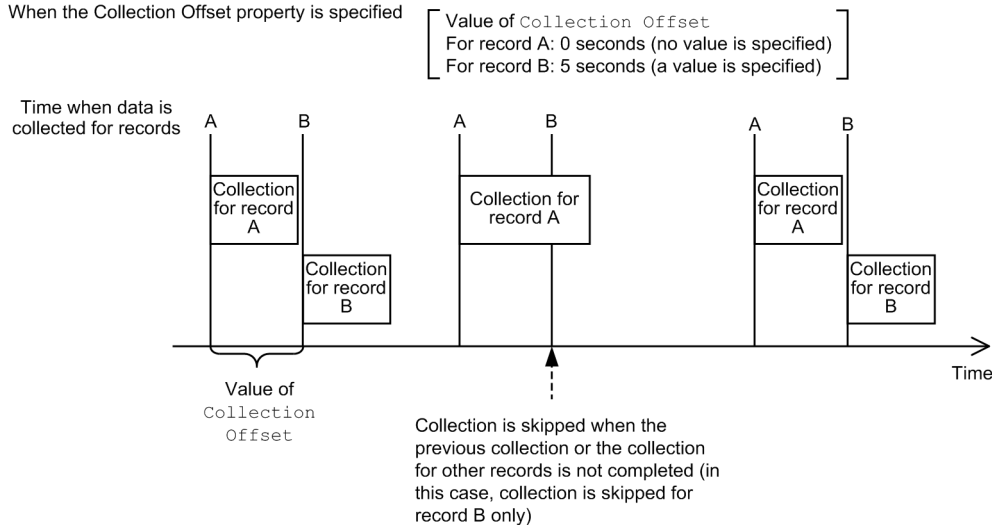
The following figure describes how performance data is collected depending on whether the `Collection Offset` property is specified.

Figure 17–2: Difference in how performance data is collected depending on whether the `Collection Offset` property is specified

- When the `Collection Offset` property is not specified



- When the `Collection Offset` property is specified



## (b) Display processing of real-time reports when a higher priority is given to the collection of historical data

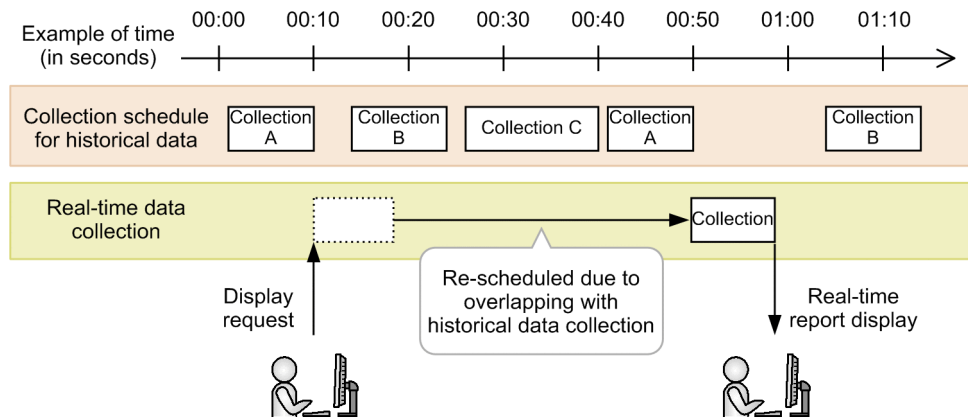
If the value of the `Historical Data Collection Priority Mode` in the startup information file (`jpccomm.ini`) for the monitoring agent is changed to 1, display of real-time reports changes from normal mode to *re-schedule* mode or *temporary log* mode. This prevents the time of collection of historical data from overlapping with that of collection for real-time report display

- *Re-schedule mode*

When a request to display a real-time report is issued, the subsequent collection schedule for historical data is automatically checked and if an overlap might occur, the display processing for the real-time report is re-scheduled.

Note that this mode cannot be used for records that take a long time to be collected or for group agents.

Figure 17–3: Overview of re-schedule mode



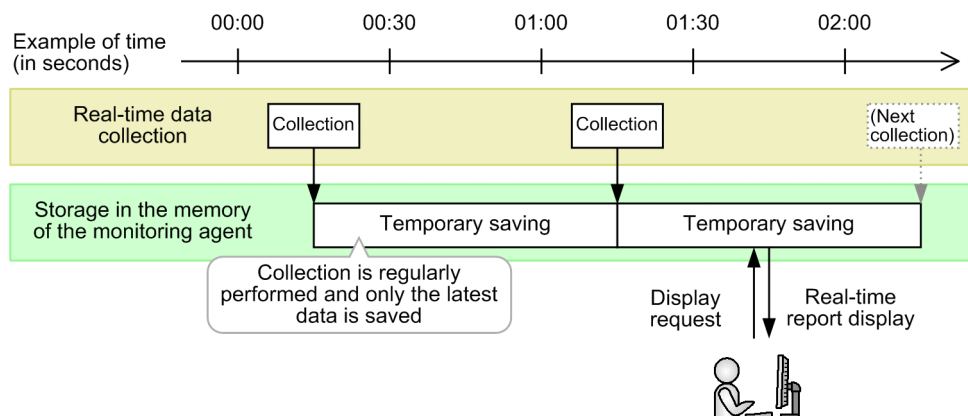
For details, see *17.2.9(3)(d) Operation when real-time reports are displayed in re-schedule mode.*

- *Temporary log mode*

Data required for real-time report display is automatically collected at regular intervals and only the latest data is temporarily stored in the memory. When a request to display a real-time report is issued, it is displayed with the temporarily stored data.

This mode is available for all records regardless of time required for collection.

Figure 17–4: Overview of temporary log mode



For details, see *17.2.9(3)(e) Operation when real-time reports are displayed in temporary log mode.*

When you first enable the `Historical Data Collection Priority Mode` label in the `jpccomm.ini` file, re-schedule mode is enabled.

### (c) Changing the operation mode for real-time reports

You can change the operation mode (re-schedule mode or temporary log mode) for real-time reports when the `Historical Data Collection Priority Mode` value is 1 (enabled) in the startup information file (`jpccomm.ini`) of a monitoring agent by a command.

#### Changing the operation mode in the Service Properties window

Change the value of the `Realtime Report Data Collection Mode` property for each record to be used for real-time reports in the service properties of the Agent Collector service or remote agent of the target monitoring agent.

## Changing the operation mode by using a command

1. Use the `jpcasrec output` command to output the contents of the current definition to a file in XML format.
2. Change and save the value of the `<realtime-report-data-collection-mode>` tag.
3. Use the `jpcasrec update` command to update the contents of the definition.

## Specified value (common to the methods of using the window and command)

The value to be specified for the `Realtime Report Data Collection Mode` property and the `<realtime-report-data-collection-mode>` tag is common. Specify either of the following values:

- `Reschedule` (re-schedule mode)
- `Temporary Log` (temporary log mode)

For details on the `Realtime Report Data Collection Mode` property (in the service properties of the Agent Collector service or remote agent), see the appendixes of the appropriate agent manual. For additional details about the commands, see the chapter that explains commands in the manual *JPI/Performance Management Reference*.

## (d) Operation when real-time reports are displayed in re-schedule mode

If you display a real-time report in re-schedule mode, the display processing differs from the normal display processing of real-time reports as follows.

- If collection of historical data is scheduled within 10 seconds from a display request, the display of a real-time report is re-scheduled. In this case, the real-time report is displayed when the collection schedule of historical data has at least 10 seconds of spare time.
  - After a display request is issued, a real-time report is displayed when at least 10 seconds of spare time is available. *Re-schedule mode* is displayed at the top of the reports window and when you use the `jpcrpt` command, a message indicating the specified mode is output to confirm that re-scheduling is set to be performed.
  - For records that require at least 10 seconds to collect data, an error message is displayed in the window and a real-time report cannot be displayed.

For those records, consider displaying real-time reports in temporary log mode.

For records that might take at least 10 seconds to collect data, the value of the `Over 10 Sec Collection Time` property<sup>#</sup> is set to `Yes`. All records for group agents correspond to such records. Note that records other than such records might also take at least 10 seconds to collect data and real-time reports might not be able to be displayed depending on the environment.

<sup>#</sup>: This property is only displayed when the value of the `Historical Data Collection Priority Mode` label of the startup information file (`jpccomm.ini`) for an agent is set to 1 (enabled).
- Checking and re-scheduling the collection schedule of historical data are also executed during automatic updating of real-time reports.
- If a real-time report cannot be displayed within 50 seconds from a display request, the re-scheduling processing results in timeout because the schedule is too tight.
  - If an event in which a real-time report is not displayed continues, retry a while later. If a real-time report is still not displayed, adjust the collection interval of records or consider using historical reports.
  - Adjust the timeout time of the report display processing, which is set in the `reportFirstDataTimeout` parameter of the initialization file (`config.xml`), in coordination with the timeout time of the re-scheduling processing. If the report display timeout time is set to less than 60 seconds, a timeout is more likely to occur during re-scheduling (default value: 600 seconds). Change the value of the `reportFirstDataTimeout` parameter or adjust the collection schedule of historical data so that re-scheduling becomes less frequent.

## (e) Operation when real-time reports are displayed in temporary log mode

If you display a real-time report in temporary log mode, the display processing differs from the normal display processing of real-time reports as follows.

- Data that is temporarily saved by using a mechanism for displaying historical data is used for real-time report display.
  - Although the contents are displayed as a real-time report, they are the contents the last time data is collected rather than when a display request is issued. *Temporary log mode* is displayed at the top of the window in which a report is displayed and when you use the `jpccrpt` command, a message indicating the specified mode is output during command execution so that you can see that temporary log data is set to be displayed.

Note that while monitoring is suspended, the collection of display data for real-time reports continues to be performed.

- Because the collected latest data is stored in the memory, the memory usage of a monitoring agent that displays real-time reports increases.

The memory usage is the sum of the used memory amount for each target record.

The used memory amount for each target record can be calculated by the following estimation formula:

$$(fixed\ portion\ in\ record\ size^{#1} + variable\ portion\ in\ record\ size^{#1} + 20,000) \times number\ of\ record\ instances^{#2}$$

#1: For details, see the manual of each agent.

#2: For details on how to check this, see the *Release Notes* of each agent.

- Although collection processing in temporary log mode is performed regardless of the settings of the `Log` property for a target record (whether to collect historical data), the settings of the `Collection Interval` and `Collection Offset` properties are applied. If the collection interval for a target record is set to 0, data is not collected and a real-time report cannot be displayed.
- The following setting items for report display are disabled:
  - Whether to display data with delta values  
Fields for which delta values are collected (fields whose the `Delta` column is `Yes`) are always displayed by the amount of change in performance data from the previous collection.
  - Refresh interval  
Updating is performed according to the setting value of the `Collection Interval` property (collection interval) for a target record regardless of the report display settings. A symbol – is displayed in place of the refresh interval in the report display window.
- Temporarily saved data for real-time reports is deleted when the service stops and the value of the `Realtime Report Data Collection Mode` property is changed.
  - Immediately after a service starts or the value of the `Realtime Report Data Collection Mode` property for a record is changed, a real-time report might not be able to be displayed. In this case, wait until the collection processing is performed and then make a retry.

## 17.2.10 Troubleshooting problems related to the monitoring suspension function

### (1) The KAVJS6570-I message is output to the Monitoring Suspension Settings window

The KAVJS6570-I message is output when monitoring is suspended or resumed and whether the monitoring status is changed in the monitoring agent is unknown. The method for handling this error differs depending on the status of the monitoring agent. Check the status of the monitoring agent and if necessary, reconfigure the settings of monitoring suspension or resumption.

To handle this error:

1. Make sure that the monitoring status of the monitoring agent is changed.

Make sure that there is a monitoring agent whose **Monitoring status** or **Settings** contains ? in the Monitoring Suspension Settings window.

- When ? does not exist

There is no problem because the monitoring status of the monitoring agent is changed.

- When ? exists

Perform step 2 and subsequent steps.

2. Check the status of the monitoring agent service in which ? is found in step 1.

Execute the `jpctool service list` command in PFM - Manager and check `Status` in the output result.

- When `Status` is `Inactive` or `Stopping`

The monitoring status is changed when the monitoring agent starts. Because monitoring is not performed while the monitoring agent stops, if you want to resume monitoring immediately, start the monitoring agent.

- When `Status` is `S Active` or `S Busy`

The monitoring status is changed when the stand-alone mode is released. Because alarm monitoring is not performed in stand-alone mode, if you want to resume monitoring immediately, release the stand-alone mode.

- When `Status` is `Starting` or `Busy`

Wait until the start processing is completed or the request processing is completed, click the **Refresh** button in the Monitoring Suspension Settings window, and then perform step 1 again.

- When `Status` is `Active`

The monitoring status is not changed because an error occurred in communication between the monitoring manager and monitoring agent. Reconfigure the settings of monitoring suspension or resumption in the Monitoring Suspension Settings window.



#### Note

If you want to check the current monitoring status of a monitoring agent which is marked with ?, you can check it by executing the `jpctool monitor status` command on each host.

### (2) The KAVE06189-W message is output during command execution

The KAVE06189-W message is output when monitoring is suspended or resumed and whether the monitoring status is changed in the monitoring agent is unknown. The method for handling this error differs depending on the status of the

monitoring agent. Check the status of the monitoring agent and if necessary, reconfigure the settings of monitoring suspension or resumption.

To handle this error:

1. Make sure that the monitoring status of the monitoring agent is changed.

Execute the `jpctool monitor list` command in PFM - Manager to check whether there is a monitoring agent whose `Status` or `Setting` contains `*` in the output result.

- When `*` does not exist

There is no problem because the monitoring status of the monitoring agent is changed.

- When `*` exists

Perform step 2 and subsequent steps.

2. Check the status of the monitoring agent service in which `*` is found in step 1.

Execute the `jpctool service list` command in PFM - Manager and check `Status` in the output result.

- When `Status` is `Inactive` or `Stopping`

The monitoring status is changed when the monitoring agent starts. Because monitoring is not performed while the monitoring agent stops, if you want to resume monitoring immediately, start the monitoring agent.

- When `Status` is `S Active` or `S Busy`

The monitoring status is changed when the stand-alone mode is released. Because alarm monitoring is not performed in stand-alone mode, if you want to resume monitoring immediately, release the stand-alone mode.

- When `Status` is `Starting` or `Busy`

Wait until the start processing is completed or the request processing is completed and then perform step 1 again.

- When `Status` is `Active`

The monitoring status is not changed because an error occurred in communication between the monitoring manager and monitoring agent. Execute the `jpctool monitor suspend` or `jpctool monitor resume` command to reconfigure the settings.



#### Note

If you want to check the current monitoring status of a monitoring agent that is marked with `*`, you can check it by executing the `jpctool monitor status` command on each host.

## 17.2.11 Troubleshooting problems related to linking with other programs

### (1) JP1 events are not reported when linking with JP1/IM

Possible causes and solutions:

- There is an error in the settings for enabling JP1 events to be issued.

Confirm whether the settings for issuing JP1 events are correct with PFM - Web Console.

- There is an error in the alarm setting.

Confirm whether the alarm setting is correct with PFM - Web Console.

- JP1/Base is not installed or set up.

Confirm whether JP1/Base is installed and set up.

- There is an error in a command definition of an alarm definition.

Confirm whether JP1/Base is installed and set up.

When you set `-r logical-host-name` as an argument for issuing JP1 events in a command definition of an alarm definition, do not include unnecessary line feeds. If you do so, JP1 events will fail to be sent. The following is an example of definition with error:

```
[[Action Definition Command]]
Command Name=../../tools/jpcimevt
Action Handler=PH1hostA
[[[Message Text]]]
<omitted>""JPC_REPORTID=aaaaaaaa:7518b0c:128fd04b38c:-7a16" -r hostA
Δ
[Alarm Data]
:
```

Legend:

Δ: Unnecessary line feed

## (2) Monitored PFM - Agent or PFM - RM is not displayed in the monitoring tree window when linking with a monitored object function of JP1/IM

Possible causes and solutions:

- The monitored PFM - Agent or PFM - RM has never been started.  
If PFM - Agent or PFM - RM has never been started, it is not displayed in the monitoring tree. Start PFM - Agent or PFM - RM and then redisplay the monitoring tree.
- PFM - Agent and PFM - Manager are not connected, or PFM - RM and PFM - Manager are not connected.  
If PFM - Agent and PFM - Manager, or PFM - RM and PFM - Manager are not connected, establish a connection.
- The monitored object linkage function of JP1/IM is not set up.  
If the monitored object linkage function of JP1/IM is not set up, set it up.

## (3) The display color of the monitored object does not change when linking with a monitored object function of JP1/IM

Possible causes and solutions:

- A JP1 event has not been issued.  
Use the Event Monitor window to make sure that a JP1 event has been issued. If a JP1 event has not been issued, make sure that the alarm definition is correct.
- There is an error in the JP1/Base settings.  
Confirm that there are no errors in the JP1/Base settings. When the issuing of a JP1 event from the PFM - Agent or PFM - RM host is specified, confirm whether the transmission of a JP1 event from the PFM - Agent or PFM - RM host to the PFM - Manager host is set.

## (4) Startup of the JP1 system event monitor fails

If the `[Monitoring Console Https]` setting does not match the current encrypted communication setting when a JP1 system event is issued, startup of the JP1 system event monitor will fail. If this occurs, you must change temporarily the encrypted communication setting to match the `[Monitoring Console Https]` setting when JP1 system events



are issued. To determine the [Monitoring Console Https] setting when a JP1 system event is issued, check the URL in the web browser at the time of monitor startup.

Table 17–5: Combinations of settings that allow monitor startup from JP1 system events

[Monitoring Console Https] setting when a JP1 system event is issued	URL in the web browser at monitor startup	Encrypted communication setting
Yes	Begins with https	Enabled
No	Begins with http	Disabled

For details about the encrypted communication settings, see the section on changing the settings for encrypted communication between a web browser and the monitoring console server in the *JP1/Performance Management Planning and Configuration Guide*.

## (5) Performance Management reports cannot be displayed from the console of JP1/IM or JP1/AJS3

The cause of the problem and action to be taken differ depending on the message displayed under Connecting to the PFM - Web Console host (*PFM - Web Console host name*) . . . The following table describes the cause and action to be taken for each message.

Table 17–6: Cause and action to be taken for each message

Message	Cause	Action
<ul style="list-style-type: none"> <li>Internet Explorer: Internet Explorer cannot display the webpage</li> <li>Firefox: Unable to connect</li> </ul>	The PFM - Web Console service is not running on the PFM - Web Console host specified in the <search-WebConsole> tag in config.xml.	Make sure that the PFM - Web Console service is running on the host indicated by <i>host-name</i> . If the service has stopped, start it.
<ul style="list-style-type: none"> <li>Internet Explorer: Internet Explorer cannot display the webpage</li> <li>Firefox: Server Not Found</li> </ul>	The host parameter is specified incorrectly for PFM - Web Console specified in the <search-WebConsole> tag in config.xml.	The value specified for the host parameter must be a host name that can be resolved from the host running the browser. Change the settings so that name resolution is possible, or specify a host name that can be resolved to an IP address.
<ul style="list-style-type: none"> <li>Internet Explorer: Internet Explorer cannot display the webpage</li> <li>Firefox: Secure Connection Failed or The connection was reset</li> </ul>	The https parameter is specified incorrectly for PFM - Web Console specified in the <search-WebConsole> tag in config.xml.	Change the value of the https parameter as follows according to the encrypted communication setting of PFM - Web Console installed on the host indicated by <i>host-name</i> : <ul style="list-style-type: none"> <li>If encrypted communication is enabled: on</li> <li>If encrypted communication is disabled: off</li> </ul>
Internet Explorer cannot display the webpage	Encrypted communication is enabled for PFM - Web Console specified in the <search-WebConsole> tag in config.xml, but the Web browser (Internet Explorer) is not configured to use TLS.	Enable TLS communication in the Web browser settings. For details, see the section explaining how to configure a Web browser to use the monitoring console in the <i>JP1/Performance Management Planning and Configuration Guide</i> .



Message	Cause	Action
500 Internal Server Error	The version of PFM - Web Console specified in the <code>&lt;search-WebConsole&gt;</code> tag in <code>config.xml</code> is earlier than 11-10.	Check the version of PFM - Web Console installed on the host indicated by <i>host-name</i> .
Security warning message shown below# <ul style="list-style-type: none"> <li>Internet Explorer: Content was blocked because it was not signed by a valid security certificate.</li> <li>Firefox: Your connection is not secure</li> </ul>	For PFM - Web Console running on the host indicated by <i>host-name</i> , the host name (Common Name) specified in the server certificate does not match the host name specified for the <code>host</code> parameter in the <code>&lt;search-WebConsole&gt;</code> tag in <code>config.xml</code> .	Make sure that the host name (Common Name) specified in the server certificate matches the host name specified for the <code>host</code> parameter in the <code>config.xml</code> . If a host name in FQDN format is specified in Common Name, you need to specify the value in the format <i>host-name + domain-name</i> for the <code>host</code> parameter in <code>config.xml</code> . You can use the <code>jjpcwtool https output certtext</code> command to check the value specified for Common Name. For details about this command, see the chapter that describes the command in the manual <i>JPI/Performance Management Reference</i> .

#

From a browser, access the PFM - Web Console instance that is displayed as the host name.

When you access PFM - Web Console, the following security message appears:

- Internet Explorer:

The security certificate on this Web site was issued for the address of another Web site.

- Firefox:

This certificate is valid only for the host name (Common Name) that is configured in the server certificate.

For details about the actions to be taken if any other security warning message appears, see [17.2.4\(4\) A security warning window is displayed in the web browser](#).

## 17.2.12 Troubleshooting other problems

Check the existing circumstances when errors occur. If a message is output, read its contents. For details on the log information output by Performance Management, see [17.4 Log information to be output when Performance Management is used](#).

If you cannot resolve an error by taking any of the steps described from [17.2.1 Troubleshooting problems related to setup and service startup](#) to [17.2.11 Troubleshooting problems related to linking with other programs](#), or if an error occurs not described in these sections, collect the data needed to investigate the error, and then contact the system administrator.

For details on the data you need to collect and how to collect it, see [17.5 Data to be collected in the event of trouble](#) and [17.6 Procedures for collecting data in the event of trouble](#).

## 17.3 Troubleshooting for multiple monitoring

---

This section explains how to handle problems that might occur while you are using multiple monitoring.

### 17.3.1 When the `jpctool config mgrimport` command is executed, an error is output

If the KAVE06142-E message is output to the standard error output and common message log, the import has failed because duplicated definition information is inconsistent. In that case, do the following in PFM - Manager on the secondary Manager.

1. Check the definition information name shown in KAVE06142-E.
2. Reference the description of how to verify definition information in the manual *JPI/Performance Management Reference*. Determine the definition information (file name, section name/label name, or property name) which is inconsistent from the definition information name.
3. After you have determined the inconsistent definition information, change the corresponding definition information on the secondary Manager so that it matches with that on the primary Manager and then perform an import.  
After you change definition information on the primary Manager, you must export the definition information from the primary Manager, copy it to the secondary Manager, and then import it. For details, see *11.5.1 Procedure for duplicating definition information*.

### 17.3.2 The host name is not distributed to agents when the `jpccconf primmgr notify` command is executed

#### (1) When batch switching the primary Manager and the secondary Manager

If you batch switch the primary Manager and the secondary Manager and the host name fails to be distributed, the host name is output to the standard error output. In that case, do the following in PFM - Manager on the secondary Manager.

1. Confirm that the Status Server service is running on the host whose host name failed to be distributed.
2. Reconfigure.  
For details, see *11.7.2 Batch switching the primary Manager and the secondary Manager*.
3. Check the result of distribution.

If the command execution succeeded, the host name of the new primary Manager is distributed as a batch to hosts on which the Status Server service is running. The host name is not distributed to hosts on which the Status Server service is not running. The distribution result indicating whether distribution to each host succeeded is output to a CSV file.

If the distribution result is `Success`, the host name was distributed normally.

If the distribution result is `Failure`, reconfigure the host name of the new primary Manager for hosts to which the host name failed to be distributed. Start the Status Server service on hosts to which the host name failed to be distributed and then perform a batch switch operation again.

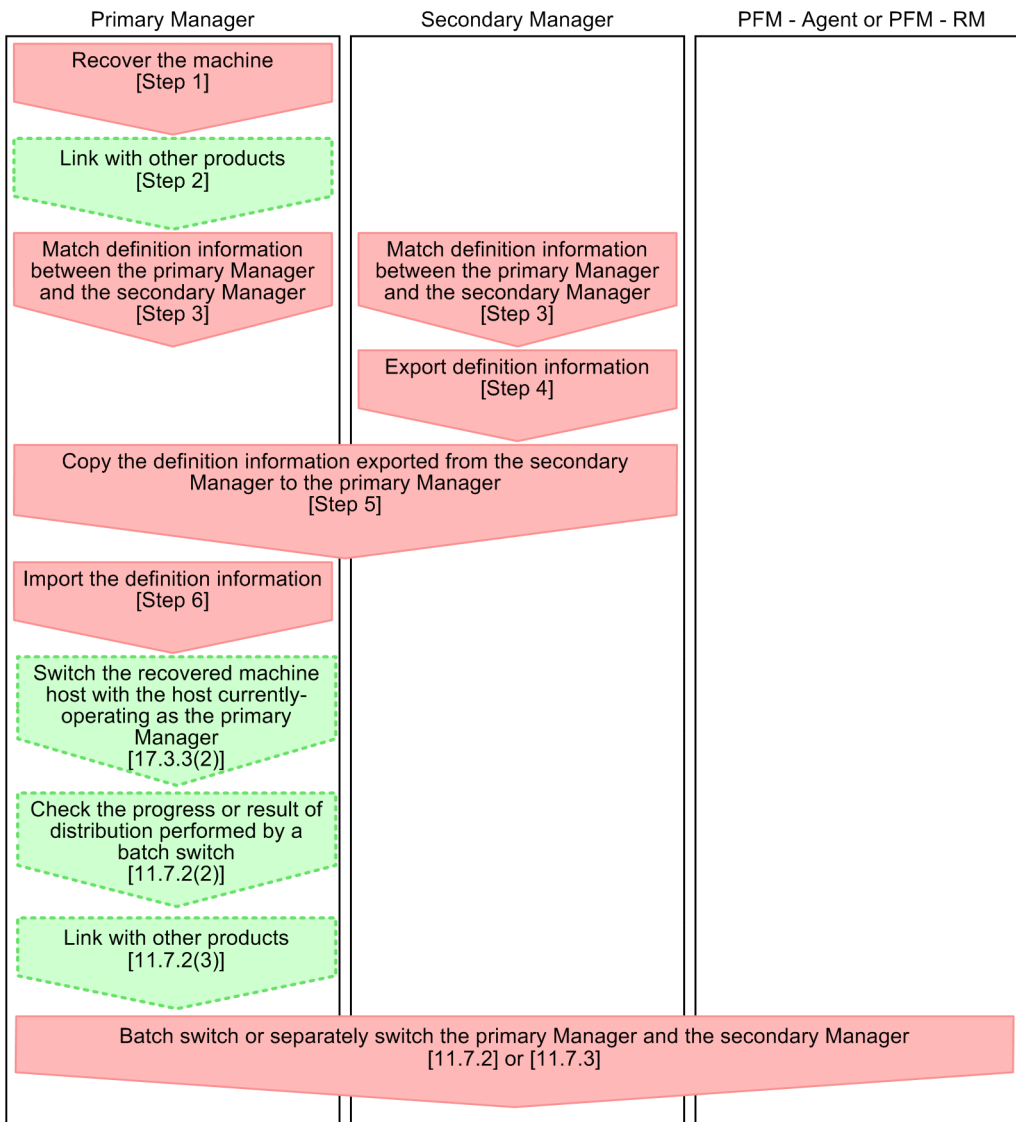
## **(2) When switching the primary Manager and the secondary Manager separately**

Execute the `jpccconf mgrhost define` command to perform reconfiguration on the host running PFM - Agent or PFM - RM to which the host name failed to be distributed. If you perform reconfiguration separately, the Status Server service does not need to be running. If a physical host and logical host exist on a machine, you must perform reconfiguration in both the physical host and the logical host. For details, see [11.7.3 Switching the primary Manager and the secondary Manager separately](#).

### **17.3.3 The host name is not distributed to the primary Manager when the `jpccconf primmgr notify` command is executed**

A possible cause of the problem is that the PFM - Manager service stopped for some reason (perhaps the host went down), and distribution to PFM - Manager on the primary Manager failed. The following figure shows the procedure for recovering the machine that is down and then switching the primary Manager and the secondary Manager.

Figure 17–5: Procedure for recovering the machine that is down and reconfiguring it as the primary Manager



Legend:

 : Required setup items

 : Optional setup items

[ ] : Reference

## (1) Recovering the machine

To recover the machine of the primary Manager that is down and match the definition information with that of the secondary Manager:

### 1. Recover the machine.

Recover or reconfigure the machine that is down so that it can operate. Do this in PFM - Manager and PFM - Web Console.

### 2. Link with other products.

For details, see [11.3.3 Link with other systems in a multiple-monitoring environment](#).

### 3. Match the definition information of the primary Manager and the secondary Manager.

In a multiple-monitoring environment, you must match the definition information of the primary Manager and the secondary Manager. For details about items that need to be matched, see [11.1.3 Definition information for multiple monitoring](#).

4. Export the definition information.

Do this in PFM - Manager and PFM - Web Console on the secondary Manager. For details, see [11.5.2 Exporting definition information](#).

5. Copy the definition information exported from the secondary Manager to the primary Manager.

Do this in PFM - Manager and PFM - Web Console.

Copy each output-destination folder or directory. Do not change the file configuration.

6. Import the definition information.

Do this in PFM - Manager and PFM - Web Console on the primary Manager. For details, see [11.5.3 Importing definition information](#).

## (2) Switching the recovered machine host with the host currently-operating as the primary Manager

To reconfigure the recovered machine host as the primary Manager, switch the primary Manager and the secondary Manager. For details, see [11.7.1 Procedure for switching the primary Manager and the secondary Manager](#). Note that in this case, you need to read *the secondary Manager as the recovered machine*.

### 17.3.4 A connection from PFM - Web Console to PFM - Manager cannot be established

A possible cause of this problem is that the PFM - Web Console does not support multiple monitoring for PFM - Manager. PFM - Web Console versions 10-10 or later support multiple monitoring. For details, see [11.2.2 Prerequisite product version](#).

### 17.3.5 No agent is displayed on the secondary Manager

Possible causes and solutions:

- The host name of the secondary Manager is not registered in the setting of PFM - Manager for the connection destination for agents.

Make sure that the host name of the secondary Manager is registered as PFM - Manager for the connection destination of the corresponding agents. For details about the settings of hosts for configuring a multiple-monitoring environment, see [11.3 Setting up multiple monitoring](#).

- There is an error in the setting of PFM - Manager for the connection destination for agents.

Make sure that there are no spelling errors, host specification errors, or other errors in the host name set as PFM - Manager for the connection destination of the agents. For details about the settings of hosts when configuring a multiple-monitoring environment, see [11.3 Setting up multiple monitoring](#).

## 17.3.6 Troubleshooting related to events

### (1) Multiple actions are executed in one event

A possible cause of the problem is that the remote action control function of the agent that reported the event is in all execution mode.

If the remote action control function is in all execution mode, remote actions will be executed twice. Change the execution mode to fit operational needs. For details about the remote action control function, see [11.3.5 Controlling remote actions](#).

### (2) No events are sent to the secondary Manager

Possible causes and solutions:

- The secondary Manager is not registered in the setting of PFM - Manager for the connection destination.  
Make sure that the host name of the secondary Manager is set as PFM - Manager for the connection destination. If the host name has not been set, set it. For details about setting up the primary Manager and the secondary Manager, see [11.3 Setting up multiple monitoring](#).
- There is an error in the setting of PFM - Manager for the connection destination.  
Make sure that there are no spelling errors, host specification errors, or other errors in the host name set as PFM - Manager for the connection destination. For details about setting up the primary Manager and the secondary Manager, see [11.3 Setting up multiple monitoring](#).

### (3) Events are sent to the secondary Manager but actions are not executed

A possible cause of the problem is that the remote action control function of the agent that reported the event is in one-side execution mode or primary execution mode.

If the remote action control function is in primary execution mode, only remote actions of events reported to the primary Manager are executed. If the remote action control function is in one-side execution mode, only remote actions of the event that is first reported successfully are executed. Change the execution mode according to the operation. For details about the remote action control function, see [11.3.5 Controlling remote actions](#).

### (4) Events are sent to both the primary Manager and the secondary Manager but actions are executed only on the primary Manager

A possible cause of the problem is that the remote action control function of the agent that reported the event is in one-side execution mode or primary execution mode.

If the remote action control function is in primary execution mode, only remote actions of events reported to the primary Manager are executed. If the remote action control function is in one-side execution mode, only remote actions of the event that is first reported successfully are executed. Change the execution mode to fit operational needs. For details about the remote action control function, see [11.3.5 Controlling remote actions](#).

### (5) When the primary Manager is down, no action is executed from event notification

Possible causes and solutions:

- The remote action control function of the agent that reported the event is in primary execution mode.

If the remote action control function is in primary execution mode, only remote actions of events reported to the primary Manager are executed. Therefore, while the primary Manager is not running, no remote actions will be executed.

Change the execution mode of the remote action control function to all execution mode or one-side execution mode according to the operation, or switch the primary Manager and the secondary Manager.

For details about the remote action control function, see [11.3.5 Controlling remote actions](#).

For details about the procedure for switching the primary Manager and the secondary Manager, see [11.7 Switching the primary Manager and the secondary Manager](#).

- There is an error which set alarm actions in the action handler.

If `<host-name-of-primary-manager><Action Handler>` is set as the action handler in which alarm actions are set, actions of events reported to the secondary Manager are also executed on the primary Manager. Therefore, while the primary Manager is not running, no remote actions will be executed.

When you set `Manager` for the action handler, actions are executed by the action handler of PFM - Manager receiving events.

You can set `Manager` for the action handler from PFM - Web Console or by executing the `jpctool alarm import` command.

For details, see [6.4 Setting alarms using the Web browser \(Alarms tree\)](#) or the chapter that describes the `jpctool alarm import` command in the manual *JP1/Performance Management Reference*.

## 17.3.7 A connection from the time the JP1/IM's Event Console starts monitoring to PFM - Web Console cannot be established

### (1) When issuing a JP1 system event to link to JP1/IM

A possible cause of the problem is that PFM - Manager and PFM - Web Console linked with the JP1 system event are not running.

Check whether PFM - Manager and PFM - Web Console are running. If they are not running, start them. If you cannot start PFM - Manager and PFM - Web Console due to a failure or other reasons, select running instances of PFM - Manager and PFM - Web Console from the Tool Launcher window of JP1/IM and connect them to PFM - Web Console.

For details, see [12.3.2 Setup for linking with JP1/IM](#).

### (2) When issuing a JP1 user event to link to JP1/IM

A possible cause of the problem is that PFM - Manager and PFM - Web Console linked with the JP1 user event are not running.

Check whether PFM - Manager and PFM - Web Console are running. If they are not running, start them. If you cannot start PFM - Manager and PFM - Web Console due to a failure or other reasons, do either of the following operations and connect to PFM - Web Console.

- Select running instances PFM - Manager and PFM - Web Console from the Tool Launcher window of JP1/IM and connect them to PFM - Web Console.
- Open the definition file for opening monitor windows and change the PFM - Web Console address set for `PATH` to the address of PFM - Web Console that is running. Save the file and restart JP1/IM. For details, see [12.3.2 Setup for linking with JP1/IM](#).

### 17.3.8 PFM-related settings cannot be specified from JP1/SLM

A possible cause of the problem is that PFM - Manager for the connection destination and PFM - Web Console on the primary Manager are not running.

Check whether PFM - Manager and PFM - Web Console are running. If they are not running, start them. If you cannot start PFM - Manager and PFM - Web Console due to a failure or other reasons, change the connection target to PFM - Manager and PFM - Web Console running on the secondary Manager. For details, see [13.3.1 Setup for JP1/SLM linkage](#).



## 17.4 Log information to be output when Performance Management is used

When an error occurs with Performance Management, check the log information and investigate the problem.

### 17.4.1 Type of log information

#### (1) System log

The system log contains log information that reports the system status and errors that occurred. This log information is output to the following log file:

- In Windows  
Event log file
- In UNIX  
syslog file

For details on the output format, see the chapter explaining the log information in the manual *JPI/Performance Management Reference*.

Notes on logical host use:

To check the control of Performance Management by cluster software, the cluster software log is required in addition to the Performance Management system log.

#### (2) Common message logs

The common message logs contain log information that reports the system status and errors that have occurred. The information output to these logs is more detailed than the system log information. For details on the output destination file name and file size for common message logs, see [17.4.2 Details on log information](#). For details on the output format, see the chapter describing the log information in the manual *JPI/Performance Management Reference*.

Note:

The language of the common message log information is determined by the `LANG` environment variable set when a service is started or a command is executed, therefore, the common message log might contain character strings with different language codes.

Notes on logical host use:

The common message logs are output to the shared disk when Performance Management is used on a logical host. The common message log information before and after a failover is recorded in the same log file, because the log file on the shared disk is inherited together with the system when a failover takes place.

#### (3) Operation status logs

The operation status logs contain the log information output by PFM - Web Console.

For details on the output destination file name and file size for operation status logs, see [17.4.2 Details on log information](#). For details on the output format, see the chapter describing the log information in the manual *JPI/Performance Management Reference*.

## (4) Trace logs

The trace logs contain log information needed, when an error occurs, to investigate the cause of the error or to determine the processing time required by each process.

The trace log information is output to a log file for each Performance Management service.

Notes on logical host use:

The trace logs are output to the shared disk when Performance Management is used on a logical host. The trace log information before and after a failover is recorded in the same log file, because the log file on the shared disk is inherited together with the system when a failover takes place.

## 17.4.2 Details on log information

This section describes the log information output from Performance Management.

### (1) Common message logs and operation status logs

The following tables list (by OS) the services or controls that are the output sources, the log file names, and the amount of disk space used for common message logs and operation status logs. The wrap-around file method is used to write data to the operation status log.

Table 17–7: File names of common message logs (in Windows)

Type of log information	Output source	File name	Disk space used <sup>#1</sup> (KB)
Common message log	Performance Management	<i>installation-folder</i> \log\jpclog{01 02} <sup>#2</sup>	8,192 (× 2) (default)
		<i>installation-folder</i> \log\jpclogw{01 02} <sup>#2</sup>	8,192 (× 2) (default)
Common message log (for logical host use)	Performance Management for logical host use	<i>environment-directory</i> <sup>#3</sup> \jpclog\log\jpclog{01 02} <sup>#2</sup>	8,192 (× 2) (default)
		<i>environment-directory</i> <sup>#3</sup> \jpclog\log\jpclogw{01 02} <sup>#2</sup>	8,192 (× 2) (default)

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 256 (× 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

The value 01 or 02 is appended to the file name of the common message log.

For the sequential file method (jpclog)

This method always writes the newest log information to the jpclog01 file (whose name ends with 01).

When the log file size reaches the specified value, the method renames the file from jpclog01 to jpclog02 and saves the file. Then the method creates another file named jpclog01 and writes the newest log information to it.

For the wrap-around file method (jpclogw)

When the log file size reaches the set value, the next log file contents are cleared, and the newest log information is written in the next log file. The file to be written to changes in the following manner: the file after jpclogw01 is jpclogw02 and the file after jpclogw02 is jpclogw01.

#3

The environment directory is a folder on the shared disk specified at the time the logical host is created.

Table 17–8: File names of operation status logs (in Windows)

Type of log information	Output source	File name	Disk space used <sup>#1</sup> (KB)
Operation status log	PFM - Web Console	<i>installation-folder\log\jpcwtracelog-file-number<sup>#2</sup>.log</i>	4,096 (× 10)
		For the <i>jpcrpt</i> command (one-execution-per-log recording method) <sup>#3</sup> <i>installation-folder\log\jpcrpt_process-ID-of-executed-command_log-file-number<sup>#2</sup>.log</i>	4,096 (× 10 × 13 (number of PFM - Web Console commands)) + 8192
		For the <i>jpcrpt</i> command (multiple-executions-per-log recording method) <sup>#3</sup> <i>installation-folder\log\jpcrpt_loglog-file-number<sup>#2</sup>.log</i>	
		For the <i>jpcrdef</i> , <i>jpcasrec</i> , <i>jpcaspsv</i> or <i>jpcprocdef</i> command <i>installation-folder\log\command-name_sub-command-name_log-file-number<sup>#2</sup>.log</i>	
		For the <i>jpcmkkey</i> command <i>installation-folder\log\jpcmkkey_log-file-number<sup>#2</sup>.log</i>	
		For all other commands <i>installation-folder\log\command-name_log-file-number<sup>#2</sup>.log</i>	

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 256 (× 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

The log file number is the number of output log files, starting from 1.

Operation status log output

The output size of the operation status log (excluding the log for the *jpcrpt* command) can be set by using `logFileSize × logFileNumber` in the initialization file (`config.xml`).

#3

For details about the log output format of the *jpcrpt* command, see [17.4.2\(1\)\(a\) Log output format of the \*jpcrpt\* command](#).

Table 17–9: File names of common message logs (in UNIX)

Type of log information	Output source	File name	Disk space used <sup>#1</sup> (KB)
Common message log	Performance Management	<i>/opt/jp1pc/log/jpclog{01 02}<sup>#2</sup></i>	8,192 (× 2) (default)
		<i>/opt/jp1pc/log/jpclogw{01 02}<sup>#2</sup></i>	8,192 (× 2) (default)

Type of log information	Output source	File name	Disk space used <sup>#1</sup> (KB)
Common message log (for logical host use)	Performance Management for logical host use	<i>environment-directory</i> <sup>#3</sup> /jplpc/log/jpclog{01 02} <sup>#2</sup>	8,192 (× 2) (default)
		<i>environment-directory</i> <sup>#3</sup> /jplpc/log/jpclogw{01 02} <sup>#2</sup>	8,192 (× 2) (default)

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 256 (× 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

The value 01 or 02 is appended to the file name of the common message log.

For the sequential file method (jpclog)

This method always writes the newest log information to the jpclog01 file (whose name ends with 01).

When the log file size reaches the set value, the file is renamed from jpclog01 to jpclog02 and then saved. Another file named jpclog01 is created and the newest log information is written to this file.

For the wrap-around file method (jpclogw)

When the log file size reaches the set value, the next log file contents are cleared, and the newest log information is written in the next log file. The file to be written to changes in the following manner: the file after jpclogw01 is jpclogw02 and the file after jpclogw02 is jpclogw01.

#3

The environment directory is a directory on the shared disk specified at the time the logical host is created.

Table 17–10: File names of operation status logs (in UNIX)

Type of log information	Output source	File name	Disk space used <sup>#1</sup> (KB)
Operation status log	PFM - Web Console	/opt/jplpcwebcon/log/jpcwtracelog-file-number <sup>#2</sup> .log	4,096 (× 10)
		For the jpcrpt command (one-execution-per-log recording method) <sup>#3</sup> /opt/jplpcwebcon/log/jpcrpt_process-ID-of-executed-command_log-file-number <sup>#2</sup> .log	4,096 (× 10 × 13 (number of PFM - Web Console commands)) + 8192
		For the jpcrpt command (multiple-executions-per-log recording method) <sup>#3</sup> /opt/jplpcwebcon/log/jpcrpt_loglog-file-number <sup>#2</sup> .log	
		For the jpcrdef, jpcasrec, jpcaspsv or jpcprocdef command /opt/jplpcwebcon/log/command-name_sub-command-name_log-file-number <sup>#2</sup> .log	
		For the jpcmkey command /opt/jplpcwebcon/log/jpcmkey_log-file-number <sup>#2</sup> .log	
		For all other commands /opt/jplpcwebcon/log/command-name_log-file-number <sup>#2</sup> .log	

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 256 (× 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

The log file number is the number of output log files, starting from 1.

Operation status log output

The output size of the operation status log (excluding the log for the `jpcrpt` command) can be set by using `logFileSize × logFileNumber` in the initialization file (`config.xml`).

#3

For details about the log output format of the `jpcrpt` command, see [17.4.2\(1\)\(a\) Log output format of the `jpcrpt` command](#).

## (a) Log output format of the `jpcrpt` command

As the log recording method for the `jpcrpt` command, you can choose either of the following:

- One-execution-per-log recording method
- Multiple-executions-per-log recording method

To change the log recording method, use `outputMultiProcessForJpcrpt` in the initialization file (`config.xml`).

When you change the log recording method, previous log information is not automatically deleted.

If you want to delete previous log information, do so manually.

The details on each log recording method are described below.

### ■ One-execution-per-log recording method

Each execution of the `jpcrpt` command is logged in one log file.

HNTRLib's trace function for single executions is used to log the executions of the `jpcrpt` command.

When you execute the `jpcrpt` command at least 1,500 times per month (average of 50 times per day) and you use this method to log the executions of the command, you need to specify a short retention period for log files to keep the size of used disk space within the limit as described in the above table.

The following shows an example setting:

- If the command is executed 3,000 times per month (or on average 100 times per day)  
Limit the retention period of the log files to a maximum of 15 days.
- If the command is executed 6,000 times per month (or on average 200 times per day)  
Limit the retention period of the log files to a maximum of seven days.

Note that the examples are only a guideline because the retention period for log files for the `jpcrpt` command that is logged using the one-execution-per-log recording method must satisfy the following condition.

If the total file size for the log files exceeds the value of `logFileNumber × logFileSize` specified in the initialization file (`config.xml`), the `jpcrpt` command deletes log files until the total file size is below the specified value.

In this case, only the files updated earlier than the number of days specified by `logFileRetention` in the initialization file (`config.xml`) are deleted.

Below are examples of how to calculate the retention period.

*Example 1:*

This example assumes that `logFileRetention` is set to 3 days (= 72 hours) and the following 6 files remain.

```
jpcrpt_3509_log1.log    9 MB  100 hours before
jpcrpt_3510_log1.log    9 MB   80 hours before
-----<Reference time (= 72 hours before)>-----
jpcrpt_3511_log1.log    9 MB   60 hours before
jpcrpt_3512_log1.log    9 MB   40 hours before
jpcrpt_3513_log1.log    9 MB   20 hours before
jpcrpt_3514_log1.log    9 MB    Several minutes before
```

When the `jpcrpt` command is executed in this situation, the files updated earlier than the reference time are deleted in chronological order until the total size of the log files is below 40 MB. This is because the current total size for the 6 log files is 54 MB, which is greater than 40 MB.

In this example, `jpcrpt_3509_log1.log` and `jpcrpt_3510_log1.log` would be deleted. The total file size becomes 36 MB and 4 files remain.

*Example 2:*

This example assumes that `logFileRetention` is set to 3 days (= 72 hours) and the following 6 files remain.

```
jpcrpt_3509_log1.log    7 MB  100 hours before
jpcrpt_3510_log1.log    7 MB   80 hours before
-----<Reference time (= 72 hours before)>-----
jpcrpt_3511_log1.log    7 MB   60 hours before
jpcrpt_3512_log1.log    7 MB   40 hours before
jpcrpt_3513_log1.log    7 MB   20 hours before
jpcrpt_3514_log1.log    7 MB    Several minutes before
```

When the `jpcrpt` command is executed in this situation, the files updated earlier than the reference time are deleted in chronological order until the total size of the log files is below 40 MB. This is because the current total size for the 6 log files is 42 MB, which is greater than 40 MB.

In this example, `jpcrpt_3509_log1.log` would be deleted. The total file size becomes 35 MB and 5 files remain including `jpcrpt_3510_log1.log`, which is updated earlier than the reference time.

*Example 3:*

This example assumes that `logFileRetention` is set to 3 days (= 72 hours) and the following 6 files remain.

```
jpcrpt_3509_log1.log    1 MB  100 hours before
jpcrpt_3510_log1.log    1 MB   80 hours before
-----<Reference time (= 72 hours before)>-----
jpcrpt_3511_log1.log    1 MB   60 hours before
jpcrpt_3512_log1.log    1 MB   40 hours before
jpcrpt_3513_log1.log    1 MB   20 hours before
jpcrpt_3514_log1.log    1 MB    Several minutes before
```

Even if the `jpcrpt` command is executed in this situation, none of the files are deleted, including those updated earlier than the reference time, because the total log file size is 6 MB, which is smaller than 40 MB.

*Example 4:*

This example assumes that `logFileRetention` is set to 30 days (= 720 hours) and the following 6 files remain.

```

-----<Reference time (= 720 hours before)>-----
jpcrpt_3509_log1.log  9 MB  100 hours before
jpcrpt_3510_log1.log  9 MB   80 hours before
jpcrpt_3511_log1.log  9 MB   60 hours before
jpcrpt_3512_log1.log  9 MB   40 hours before
jpcrpt_3513_log1.log  9 MB   20 hours before
jpcrpt_3514_log1.log  9 MB      Several minutes before

```

When the `jpcrpt` command is executed in this situation, the current total size for the 6 files would be 54 MB, which is greater than 40 MB. However, because none of the retention times for the files exceeds 30 days (= 72 hours) from the time they were saved, as set in `logFileRetention`, none of the files would be deleted.

## ■ Multiple-executions-per-log recording method

Multiple executions of the `jpcrpt` command are logged in a log file.

HNTRLib's trace function for multiple executions is used to log the executions of the `jpcrpt` command.

The number of log files and the maximum size of a log file can be specified separately from the settings for operation status logs (`logFileSize`, `logFileNumber`).

With the multiple-executions-per-log recording method, log information is written in wrap-around format. If the specified file size is exceeded, old data is overwritten automatically.

For this reason, you do not need to specify a short retention period for log files to keep the used disk space within the specified limits like you do for the one-execution-per-log recording method.

Also note that log files are not deleted when the multiple-executions-per-log recording method is used because the `logFileRetention` setting has no influence.

Note the following when you log the executions of the `jpcrpt` command using this method.

- The executions of the `jpcrpt` command are not logged when locks are not obtained.
- The size of the log files is fixed. The log data of one execution of the `jpcrpt` command ends with an EOF character.
- In addition to the log files, a management file is created.
- The executions of the `jpcrpt` command are logged in multiple log files in wrap-around fashion. This means that when all the log files become full, the first log file starts to be overwritten. Older executions of the `jpcrpt` command exist after each EOF character.

The following example describes how to calculate the approximate number of executions of the `jpcrpt` command each log file can contain when the multiple-executions-per-log recording method is used.

Example:

Number of executions of the `jpcrpt` command that can be recorded in a log file when the `jpcrpt` command outputs messages of the `WARN` log level to a report file

When the `jpcrpt` command outputs messages of the `WARN` log level to a report file, approximately 50 kilobytes of log data is recorded in a log file for each execution of the `jpcrpt` command.

Use the following formula to calculate the approximate number of executions of the `jpcrpt` command that can be recorded in a log file:

$$(\logFileNumberMulti \times \logFileSizeMulti \times 1,024 \text{ kilobytes}) / 50 \text{ kilobytes}$$

As a result, a log file can record 819 executions of the `jpcrpt` command ( $10 \times 4 \times 1,024 \div 50 = 819$ ) with default settings when the multiple-executions-per-log recording method is used.



## (2) Trace log

The following tables list (by OS) the services or controls that are the output sources and the installation directories for trace logs.

Table 17–11: Installation folder names of trace logs (in Windows)

Type of log information	Output source	Folder name
Trace log	Action Handler	<i>installation-folder\bin\action\log\</i>
	Agent Collector and Remote Monitor Collector	<i>installation-folder\xxx<sup>#1</sup>\agent\instance-name<sup>#2</sup>\log\</i>
	Agent Store and Remote Monitor Store	<i>installation-folder\xxx<sup>#1</sup>\store\instance-name<sup>#2</sup>\log\</i>
	Correlator	<i>installation-folder\mgr\clator\log\</i>
	Agent Collector (health check agent)	<i>installation-folder\agt0\agent\log\</i>
	Agent Store (health check agent)	<i>installation-folder\agt0\store\log\</i>
	Master Store	<i>installation-folder\mgr\store\log\</i>
	Master Manager	<i>installation-folder\mgr\manager\log\</i>
	Name Server	<i>installation-folder\mgr\namesvr\log\</i>
	Performance Management command	<i>installation-folder\tools\log\</i>
	Status Server	<i>installation-folder\bin\statsvr\log\</i>
	Trap Generator	<i>installation-folder\mgr\trapgen\log\</i>
	View Server	<i>installation-folder\mgr\viewsvr\log\</i>
Trace log (for logical host use)	Action Handler	<i>environment-directory<sup>#3</sup>\jp1pc\bin\action\log\</i>
	Agent Collector and Remote Monitor Collector	<i>environment-directory<sup>#3</sup>\jp1pc\xxx<sup>#1</sup>\agent\instance-name<sup>#2</sup>\log\</i>
	Agent Store and Remote Monitor Store	<i>environment-directory<sup>#3</sup>\jp1pc\xxx<sup>#1</sup>\store\instance-name<sup>#2</sup>\log\</i>
	Correlator	<i>environment-directory<sup>#3</sup>\jp1pc\mgr\clator\log\</i>
	Agent Collector (health check agent)	<i>environment-directory<sup>#3</sup>\jp1pc\agt0\agent\log\</i>
	Agent Store (health check agent)	<i>environment-directory<sup>#3</sup>\jp1pc\agt0\store\log\</i>
	Master Store	<i>environment-directory<sup>#3</sup>\jp1pc\mgr\store\log\</i>
	Master Manager	<i>environment-directory<sup>#3</sup>\jp1pc\mgr\manager\log\</i>
	Name Server	<i>environment-directory<sup>#3</sup>\jp1pc\mgr\namesvr\log\</i>
	Performance Management command	<i>environment-directory<sup>#3</sup>\jp1pc\tools\log\</i>
	Trap Generator	<i>environment-directory<sup>#3</sup>\jp1pc\mgr\trapgen\log\</i>



Type of log information	Output source	Folder name
Trace log (for logical host use)	View Server	<i>environment-directory</i> <sup>#3</sup> \jplpc\mgr\viewsvr\log\

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a folder for each instance.

#3

The environment directory is a folder on the shared disk specified at the time the logical host is created.

**Table 17–12: Installation directory names of trace logs (in UNIX)**

Type of log information	Output source	Directory name
Trace log	Action Handler	/opt/jplpc/bin/action/log/
	Agent Collector and Remote Monitor Collector	/opt/jplpc/xxx <sup>#1</sup> /agent/instance-name <sup>#2</sup> /log/
	Agent Store and Remote Monitor Store	/opt/jplpc/xxx <sup>#1</sup> /store/instance-name <sup>#2</sup> /log/
	Correlator	/opt/jplpc/mgr/clator/log/
	Agent Collector (health check agent)	/opt/jplpc/agt0/agent/log/
	Agent Store (health check agent)	/opt/jplpc/agt0/store/log/
	Master Store	/opt/jplpc/mgr/store/log/
	Master Manager	/opt/jplpc/mgr/manager/log/
	Name Server	/opt/jplpc/mgr/namesvr/log/
	Performance Management command	/opt/jplpc/tools/log/
	Status Server	/opt/jplpc/bin/statsvr/log/
	Trap Generator	/opt/jplpc/mgr/trapgen/log/
	View Server	/opt/jplpc/mgr/viewsvr/log/
Trace log (for logical host use)	Action Handler	<i>environment-directory</i> <sup>#3</sup> /jplpc/bin/action/log/
	Agent Collector and Remote Monitor Collector	<i>environment-directory</i> <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /agent/instance name <sup>#2</sup> /log/
	Agent Store and Remote Monitor Store	<i>environment-directory</i> <sup>#3</sup> /jplpc/xxx <sup>#1</sup> /store/instance name <sup>#2</sup> /log/
	Correlator	<i>environment-directory</i> <sup>#3</sup> /jplpc/mgr/clator/log/
	Agent Collector (health check agent)	<i>environment-directory</i> <sup>#3</sup> /jplpc/agt0/agent/log/

Type of log information	Output source	Directory name
Trace log (for logical host use)	Agent Store (health check agent)	<i>environment-directory</i> <sup>#3</sup> /jplpc/agt0/store/log/
	Master Store	<i>environment-directory</i> <sup>#3</sup> /jplpc/mgr/store/log/
	Master Manager	<i>environment-directory</i> <sup>#3</sup> /jplpc/mgr/manager/log/
	Name Server	<i>environment-directory</i> <sup>#3</sup> /jplpc/mgr/namesvr/log/
	Performance Management command	<i>environment-directory</i> <sup>#3</sup> /jplpc/tools/log/
	Trap Generator	<i>environment-directory</i> <sup>#3</sup> /jplpc/mgr/trapgen/log/
	View Server	<i>environment-directory</i> <sup>#3</sup> /jplpc/mgr/viewsvr/log/

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#2

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a directory for each instance.

#3

The environment directory is a directory on the shared disk specified at the time the logical host is created.

## 17.5 Data to be collected in the event of trouble

If the actions described in *17.2 Troubleshooting* are not successful in correcting the error, collect the necessary data, and then contact the system administrator to determine the cause of the error. This subsection describes the data that you need to collect in the event of an error.

Performance Management provides commands for collecting the needed data in one operation. To collect PFM - Manager, PFM - Agent, and PFM - RM data, use the `jpcras` command. To collect PFM - Web Console data, use the `jpcwras` command. The following tables indicate the data that can be collected by the `jpcras` or `jpcwras` command.

Note:

The data collected by the `jpcras` or `jpcwras` command depends on the options you specify when you execute the command. For details on the options specified in the command and the data that can be collected, see the chapter explaining the commands in the manual *JP1/Performance Management Reference*.

Notes on logical host use:

Note the following when using a logical host.

- The logs for Performance Management for logical host use are stored on the shared disk. When the shared disk is online (in Windows) or mounted (in UNIX), the `jpcras` command can be used to collect all logs on the shared disk at once.
- To determine the cause of any problems at the time of a failover, the data before and after the failover is required. Therefore, the data of both the executing and standby nodes is required.
- To investigate Performance Management for logical host use, the cluster software data is required. Because the starting and stopping of Performance Management for logical host use are controlled by the cluster software, investigate Performance Management by comparing the operations of the cluster software and Performance Management.

### 17.5.1 Data to be collected in the event of trouble (in Windows)

#### (1) Log information about the OS

The following table lists the log information about the OS to be collected.

Type of information	Outline	Default file name	Collected by the <code>jpcras</code> command	Collected by the <code>jpcwras</code> command
System log	Windows event log	N/A	Y	Y
Process information	List of processes	N/A	Y	Y
System file	hosts file	<code>system-folder\system32\drivers\etc\hosts</code>	Y	Y
	services file	<code>system-folder\system32\drivers\etc\service</code>	Y	Y
OS information	System information	N/A	Y	Y
	Network status	N/A	Y	Y
	Host name	N/A	Y	Y

Type of information	Outline	Default file name	Collected by the jpcras command	Collected by the jpcwras command
OS information	Firewall information	N/A	Y	N
Dump information	Log files regarding problem reports and solutions	<i>output-destination-folder-for-user-mode-process-dump\program-name .process-ID .dmp</i> Example: <i>jpcagtt.exe.2420.dmp</i>	N	N

**Legend:**

- Y: Can be collected
- N: Cannot be collected
- N/A: Not applicable

#

If your setup provides for output of log files to a different folder, be sure that you collect the data from the correct folder.

## (2) Performance Management information

You need to collect the information about Performance Management listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The Performance Management information required to be collected is shown below.

Type of information	Outline	Default file name	Collected by the jpcras command
Common message log	Message log output from Performance Management (sequential file method)	<i>installation-folder\log\jpclog{01 02}#1</i>	Y
	Message log output from Performance Management (wrap-around file method)	<i>installation-folder\log\jpclogw{01 02}#1</i>	Y
Common message log (logical host use)	Message log output from Performance Management (sequential file method)	<i>environment-directory\jplpc\log\jpclog{01 02}#1</i>	Y
	Message log output from Performance Management (wrap-around file method)	<i>environment-directory\jplpc\log\jpclogw{01 02}#1</i>	Y
Configuration information	Each configuration information file	<ul style="list-style-type: none"> <li>• Files under the installation folder</li> <li>• Files under <i>installation-folder\sys</i></li> <li>• Files under <i>environment-directory\jplpc</i></li> <li>• Files under <i>environment-directory\jplpc\sys</i></li> <li>• Files under <i>environment-directory</i></li> </ul>	Y
Database information	Name Server	<ul style="list-style-type: none"> <li>• <i>installation-folder\mgr\namesvr\*.DB</i></li> <li>• <i>installation-folder\mgr\namesvr\*.IDX</i></li> </ul>	Y
	Master Manager	<ul style="list-style-type: none"> <li>• <i>installation-folder\mgr\manager\*.DB</i></li> </ul>	Y

Type of information	Outline	Default file name	Collected by the jpcras command
Database information	Master Manager	<ul style="list-style-type: none"> <li><i>installation-folder</i>\mgr\manager\*.IDX</li> </ul>	Y
	Master Store	<ul style="list-style-type: none"> <li><i>installation-folder</i>\mgr\store\*.DB</li> <li><i>installation-folder</i>\mgr\store\*.IDX</li> </ul>	Y
	View Server	<ul style="list-style-type: none"> <li><i>installation-folder</i>\mgr\viewsvr\data\*</li> <li><i>installation-folder</i>\mgr\viewsvr\Reports\*</li> </ul>	Y#7
	Agent Store and Remote Monitor Store	<p>Store database 1.0:</p> <ul style="list-style-type: none"> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\*.DB</li> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\*.IDX</li> </ul> <p>Store database 2.0:</p> <ul style="list-style-type: none"> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\*.DB</li> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\*.IDX</li> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\STPD\*</li> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\STPI\*</li> <li><i>installation-folder</i>\xxx#2\store\instance-name#3\STPL\*</li> </ul>	Y#7
	Agent Store (health check agent)	<p>Store database 1.0:</p> <ul style="list-style-type: none"> <li><i>installation-folder</i>\agt0\store\*.DB</li> <li><i>installation-folder</i>\agt0\store\*.IDX</li> </ul> <p>Store database 2.0:</p> <ul style="list-style-type: none"> <li><i>installation-folder</i>\agt0\store\*.DB</li> <li><i>installation-folder</i>\agt0\store\*.IDX</li> <li><i>installation-folder</i>\agt0\store\STPD\*</li> <li><i>installation-folder</i>\agt0\store\STPI\*</li> <li><i>installation-folder</i>\agt0\store\STPL\*</li> </ul>	Y#7

Type of information	Outline	Default file name	Collected by the jpcras command
Database information (logical host use)	Name Server	<ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\mgr\namesvr\*.DB</li> <li><i>environment-directory</i>\jp1pc\mgr\namesvr\*.IDX</li> </ul>	Y
	Master Manager	<ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\mgr\manager\*.DB</li> <li><i>environment-directory</i>\jp1pc\mgr\manager\*.IDX</li> </ul>	Y
	Master Store	<ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\mgr\store\*.DB</li> <li><i>environment-directory</i>\jp1pc\mgr\store\*.IDX</li> </ul>	Y
	View Server	<ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\mgr\viewsvr\data\*</li> <li><i>environment-directory</i>\jp1pc\mgr\viewsvr\Reports\*</li> </ul>	Y#7
	Agent Store and Remote Monitor Store	<p>Store database 1.0:</p> <ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\*.DB</li> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\*.IDX</li> </ul> <p>Store database 2.0:</p> <ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\*.DB</li> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\*.IDX</li> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\STPD\*</li> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\STPI\*</li> <li><i>environment-directory</i>\jp1pc\xxx#2\store\instance-name#3\STPL\*</li> </ul>	Y#7
	Agent Store (health check agent)	<p>Store database 1.0:</p> <ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\agt0\store\*.DB</li> <li><i>environment-directory</i>\jp1pc\agt0\store\*.IDX</li> </ul> <p>Store database 2.0:</p> <ul style="list-style-type: none"> <li><i>environment-directory</i>\jp1pc\agt0\store\*.DB</li> <li><i>environment-directory</i>\jp1pc\agt0\store\*.IDX</li> </ul>	Y#7

Type of information	Outline	Default file name	Collected by the jpcras command
Database information (logical host use)	Agent Store (health check agent)	<ul style="list-style-type: none"> <li>• <i>environment-directory</i> \agt0\store\STPD\*</li> <li>• <i>environment-directory</i> \agt0\store\STPI\*</li> <li>• <i>environment-directory</i> \agt0\store\STPL\*</li> </ul>	Y <sup>#7</sup>
Trace log	Trace information of each service in the Performance Management program	N/A <sup>#4</sup>	Y
Other files	Other information files	<ul style="list-style-type: none"> <li>• Files under the installation folder</li> <li>• Files under <i>environment-directory</i> \jplpc</li> </ul>	Y
Install log <sup>#5</sup>	Message log at the time of installation	<ul style="list-style-type: none"> <li>• <i>system-folder</i>\TEMP\HCDINST \*.LOG</li> <li>• <i>system-folder</i>\TEMP\HCDINST \*.LOG</li> <li>• Following files under <i>installation-folder</i>\PSB:<sup>#6</sup> <ul style="list-style-type: none"> <li>• install.log</li> <li>• SPKMANAGE.LOG</li> <li>• insresult.dat</li> </ul> </li> </ul>	N
		%SystemDrive%\Windows\Temp \pfm_reg_history.log	Y

Legend:

- Y: Can be collected
- N: Cannot be collected
- N/A: Not applicable

#1

For details on the output format of the log files, see *16.5 Detecting problems by linking with the integrated system monitoring product*.

#2

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *JPI/Performance Management Planning and Configuration Guide*.

#3

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a folder for each instance.

#4

For details on the trace log storage destination, see *17.4.2 Details on log information*.

#5

Collect this information if the installation fails.

#6

Collect these files when installation has failed but the file exists.

#7

Collected only when a directory name, a service key, or the `all` or `data` option is specified. If the option is omitted, the file is not collected.

### (3) PFM - Web Console information

You need to collect the information about PFM - Web Console listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The PFM - Web Console information required to be collected is shown below.

Type of information	Outline	Default file name	Collected by the <code>jpcwras</code> command
Web server information	Server log of Web server or Web container	N/A	Y
Registry information	Product registry information	N/A	Y
Operation status log <sup>#1</sup>	Message log output from PFM - Web Console	<i>installation-folder</i> \log <i>\jpcwtracelog-file-number</i> <sup>#2</sup> .log	Y
	Message log output from a PFM - Web Console command	For the <code>jpcrpt</code> command (one-execution-per-log recording method) <sup>#3</sup> <i>installation-folder</i> \log <i>\jpcrpt_process-ID-of-executed-command_log-file-number</i> <sup>#2</sup> .log  For the <code>jpcrpt</code> command (multiple-executions-per-log recording method) <sup>#3</sup> <i>installation-folder</i> \log <i>\jpcrpt_loglog-file-number</i> <sup>#2</sup> .log  For the <code>jpcrdef</code> , <code>jpcasrec</code> , <code>jpcaspsv</code> or <code>jpcprocdef</code> command <i>installation-folder</i> \log\ <i>command-name_sub-command-name_log-file-number</i> <sup>#2</sup> .log  For the <code>jpcmkkey</code> command <i>installation-folder</i> \log <i>\jpcmkkey_log-file-number</i> <sup>#2</sup> .log  For all other commands <i>installation-folder</i> \log\ <i>command-name_log-file-number</i> <sup>#2</sup> .log	Y
File information	List of PFM - Web Console installation files	N/A	Y
Configuration Info	PFM - Web Console configuration information	<i>installation-folder</i> \config\*.* <i>installation-folder</i> \sample\config\*.*	Y
PFM - Web Console log information	(Un)installer log file	<i>system-folder</i> \TEMP\HCDINST \*.*.LOG	N

Legend:

Y: Can be collected



N: Cannot be collected

N/A: Not applicable

#1

For details on the output format of the operation status log, see the chapter explaining the log information in the manual *JPI/Performance Management Reference*.

#2

The log file number is the number of output log files, starting from 1.

Operation status log output

The output size of the operation status log (excluding the log for the `jpcrpt` command) can be set by using `logFileSize × logFileNumber` in the initialization file (`config.xml`).

#3

For details about the log output format of the `jpcrpt` command, see *17.4.2(1)(a) Log output format of the jpcrpt command*.

## (4) Operation information

You need to collect the following information about the operation being performed when an error occurs:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon
- Arguments specified in a command if a problem occurred while the command was executed

## (5) Error information on window displays

Obtain printouts of the following:

- The Web browser
- The window operation when the application error occurred
- The error message dialog box (including the contents displayed if there is a **Details** button)
- Command Prompt or the Administrator Console window if a problem occurred while a command was executed

## (6) User mode process dump

Collect a user mode process dump if a Performance Management process stopped due to an application error.

## (7) Problem reports

Collect problem reports if a Performance Management process stopped due to an application error.

## (8) Docker environment information

If you are using Performance Management in a Docker environment, you have to collect the following Docker environment information:

Type of information	Outline	Collected by the <code>jpcras</code> command
Docker environment information	Docker version	Y
	Docker container list	Y
	Process within the Docker container	Y
	Docker container information	Y

Legend:

Y: Can be collected

## (9) Other information

You also need to collect the following information:

- The contents of **System Information**, which is displayed by choosing **Accessories** and then **System Tools**
- Java VM thread dump  
When collecting PFM - Web Console information, collect the Java VM thread dump.

To collect the Java VM thread dump:

1. Execute the following command ten times at three-second intervals.

```
# installation-directory/CPSB/CC/web/bin/cjdumpweb PFMWebConsole
```

2. Execute the `jpcwras` command.

Note:

Because the operation of Java VM becomes unstable when collecting a thread dump, restart the PFM - Web Console service.

## 17.5.2 Data to be collected in the event of trouble (in UNIX)

### (1) Log information about the OS

The following table lists the log information about the OS to be collected.

Type of information	Outline	Default file name	Collected by the <code>jpcras</code> command	Collected by the <code>jpcwras</code> command
System log	syslog	<ul style="list-style-type: none"> <li>• In HP-UX /var/adm/syslog/syslog.log</li> <li>• In Solaris /var/adm/messages*</li> <li>• In AIX /var/adm/syslog*</li> <li>• In Linux /var/log/messages*</li> </ul>	Y#1	Y#1
Process information	List of processes	N/A	Y	Y

Type of information	Outline	Default file name	Collected by the <code>jpcras</code> command	Collected by the <code>jpcwras</code> command
System file	hosts file	<code>/etc/hosts</code>	Y	Y
		<code>/etc/inet/ipnodes</code> <sup>#2</sup>	Y <sup>#3</sup>	N
	services file	<code>/etc/services</code>	Y	Y
OS information	System information	--	Y	Y
	Patch information	--	Y	Y
	Kernel information	--	Y	Y
	Version information	--	Y	Y
	Network status	--	Y	Y
	Environment variables	--	Y	Y
	Host name	--	Y	Y
	Firewall information(Linux)	--	Y	N
Dump information	core file <sup>#4</sup>	--	Y	N

**Legend:**

- Y: Can be collected
- N: Cannot be collected
- : There is no default file.

**#1**

This cannot be collected in a system where output is not set to the default path or file name. In this case, use a different method to collect this information.

**#2**

The `/etc/inet/ipnodes` file is available only under Solaris. Collect it together with the `/etc/hosts` file.

**#3**

This file can only be collected with the `jpcras` command included in PFM - Manager 09-00 or PFM - Base 09-00 or later.

**#4**

Under HP-UX 11i V3 (IPF), you can use the `coreadm` command to rename the core file. If the core file is renamed to a file name that does not start with `core`, the `jpcras` command cannot collect it. In this case, collect the file manually.

## (2) Performance Management information

You need to collect the information about Performance Management listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The Performance Management information required to be collected is shown below.

Type of information	Outline	Default file name	Collected by the jpcras command
Common message log	Message log output from Performance Management (sequential file method)	/opt/jp1pc/log/jpclog{01 02}#1	Y
	Message log output from Performance Management (wraparound file method)	/opt/jp1pc/log/jpclogw{01 02}#1	Y
Common message log (logical host use)	Message log output from Performance Management (sequential file method)	<i>environment-directory</i> /jp1pc/log/jpclog{01 02}#1	Y
	Message log output from Performance Management (wrap-around file method)	<i>environment-directory</i> /jp1pc/log/jpclogw{01 02}#1	Y
Configuration information	Each configuration information file	<ul style="list-style-type: none"> <li>Files under /opt/jp1pc</li> <li>Files under /opt/jp1pc/sys</li> <li>Files under <i>environment-directory</i>/jp1pc</li> <li>Files under <i>environment-directory</i>/jp1pc/sys</li> <li>Files under <i>environment-directory</i></li> </ul>	Y
Database information	Name Server	<ul style="list-style-type: none"> <li><i>environment-directory</i>/jp1pc/mgr/namesvr/*.DB</li> <li><i>environment-directory</i>/jp1pc/mgr/namesvr/*.IDX</li> </ul>	Y
	Master Manager	<ul style="list-style-type: none"> <li>/opt/jp1pc/mgr/manager/*.DB</li> <li>/opt/jp1pc/mgr/manager/*.IDX</li> </ul>	Y
	Master Store	<ul style="list-style-type: none"> <li>/opt/jp1pc/mgr/store/*.DB</li> <li>/opt/jp1pc/mgr/store/*.IDX</li> </ul>	Y
	View Server	<ul style="list-style-type: none"> <li>/opt/jp1pc/mgr/viewsvr/data/*</li> <li>/opt/jp1pc/mgr/viewsvr/Reports/*</li> </ul>	Y#7
	Agent Store and Remote Monitor Store	<p>Store database 1.0:</p> <ul style="list-style-type: none"> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/*.DB</li> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/*.IDX</li> </ul> <p>Store database 2.0:</p> <ul style="list-style-type: none"> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/*.DB</li> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/*.IDX</li> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/STPD\*</li> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/STPI\*</li> <li>/opt/jp1pc/xxx#2/store/<i>instance-name</i>#3/STPL\*</li> </ul>	Y#7

Type of information	Outline	Default file name	Collected by the jpcras command
Database information	Agent Store (health check agent)	Store database 1.0: <ul style="list-style-type: none"> <li>• /opt/jp1pc/agt0/store/*.DB</li> <li>• /opt/jp1pc/agt0/store/*.IDX</li> </ul> Store database 2.0: <ul style="list-style-type: none"> <li>• /opt/jp1pc/agt0/store/*.DB</li> <li>• /opt/jp1pc/agt0/store/*.IDX</li> <li>• /opt/jp1pc/agt0/store/STPD \*</li> <li>• /opt/jp1pc/agt0/store/STPI \*</li> <li>• /opt/jp1pc/agt0/store/STPL \*</li> </ul>	Y#7
Database information (logical host use)	Name Server	<ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/mgr/namesvr/*.DB</li> <li>• <i>environment-directory</i>/jp1pc/mgr/namesvr/*.IDX</li> </ul>	Y
	Master Manager	<ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/mgr/manager/*.DB</li> <li>• <i>environment-directory</i>/jp1pc/mgr/manager/*.IDX</li> </ul>	Y
	Master Store	<ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/mgr/store/*.DB</li> <li>• <i>environment-directory</i>/jp1pc/mgr/store/*.IDX</li> </ul>	Y
	View Server	<ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/mgr/viewsvr/data/*</li> <li>• <i>environment-directory</i>/jp1pc/mgr/viewsvr/Reports/*</li> </ul>	Y#7
	Agent Store and Remote Monitor Store	Store database 1.0:Store database 1.0: <ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/*.DB</li> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/*.IDX</li> </ul> Store database 2.0: <ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/*.DB</li> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/*.IDX</li> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/STPD/*</li> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/STPI/*</li> <li>• <i>environment-directory</i>/jp1pc/xxx#2/store/instance-name#3/STPL/*</li> </ul>	Y#7
	Agent Store (health check agent)	Store database 1.0: <ul style="list-style-type: none"> <li>• <i>environment-directory</i>/jp1pc/agt0/store/*.DB</li> </ul>	Y#7

Type of information	Outline	Default file name	Collected by the jpcras command
Database information (logical host use)	Agent Store (health check agent)	<ul style="list-style-type: none"> <li><i>environment-directory</i>/jp1pc/agt0/store/*.IDX</li> </ul> Store database 2.0: <ul style="list-style-type: none"> <li><i>environment-directory</i>/jp1pc/agt0/store/*.DB</li> <li><i>environment-directory</i>/jp1pc/agt0/store/*.IDX</li> <li><i>environment-directory</i>/agt0/store/STPD/*</li> <li><i>environment-directory</i>/agt0/store/STPI/*</li> <li><i>environment-directory</i>/agt0/store/STPL/*</li> </ul>	Y <sup>#7</sup>
Trace log	Trace information of each service in the Performance Management program	N/A <sup>#4</sup>	Y
Install log <sup>#5</sup>	Standard log of Hitachi Program Product Installer	<ul style="list-style-type: none"> <li>/etc/.hitachi/.hitachi.log</li> <li>/etc/.hitachi/.hitachi.log{01 02 03 04 05}</li> <li>/etc/.hitachi/.install.log</li> <li>/etc/.hitachi/.install.log{01 02 03 04 05}</li> <li>/opt/jp1pc/PSB/etc/.hitachi/.hitachi.log<sup>#6</sup></li> <li>/opt/jp1pc/PSB/etc/.hitachi/.install.log<sup>#6</sup></li> </ul>	N

Legend:

Y: Can be collected

N: Cannot be collected

N/A: There is no default file.

#1

For details on the output format of the log files, see *16.5 Detecting problems by linking with the integrated system monitoring product*.

#2

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on the service keys of each PFM - Agent or PFM - RM, see the naming rules in an appendix of the *JP1/Performance Management Planning and Configuration Guide*.

#3

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a directory for each instance.

#4

For details on the trace log destination directory, see *17.4.2 Details on log information*.

#5

Collect this information if the installation fails.

#6

Collect this file when installation has failed but the file exists.

#7

Collected only when a directory name, a service key, or the `all` or `data` option is specified. If the option is omitted, the file is not collected.

### (3) PFM - Web Console information

You need to collect the information about PFM - Web Console listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The PFM - Web Console information that needs to be collected is shown below.

Type of information	Outline	Default file name	Collected by the <code>jpcwras</code> command
Web server information	Server log of Web server or Web container	N/A	Y
Operation status log <sup>#1</sup>	Message log output from PFM - Web Console	<code>/opt/jp1pcwebcon/log/jpcwtrace<sup>log-file-number</sup>#2.log</code>	Y
	Message logs output from PFM - Web Console commands	For the <code>jpcrpt</code> command (one-execution-per-log recording method) <sup>#3</sup> <code>/opt/jp1pcwebcon/log/jpcrpt_<sup>process-ID-of-executed-command_log-file-number</sup>#2.log</code>  For the <code>jpcrpt</code> command (multiple-executions-per-log recording method) <sup>#3</sup> <code>/opt/jp1pcwebcon/log/jpcrpt_log<sup>log-file-number</sup>#2.log</code>  For the <code>jpcrdef</code> , <code>jpcasrec</code> , <code>jpcaspsv</code> or <code>jpcprocdef</code> command <code>/opt/jp1pcwebcon/log/<sup>command-name_sub-command-name_log-file-number</sup>#2.log</code>  For the <code>jpcmkey</code> command <code>/opt/jp1pcwebcon/log/jpcmkey_<sup>log-file-number</sup>#2.log</code>  For all other commands <code>/opt/jp1pcwebcon/log/<sup>command-name_log-file-number</sup>#2.log</code>	Y
File information	List of PFM - Web Console installation files	N/A	Y
Configuration Info	PFM - Web Console configuration information	<code>/opt/jp1pcwebcon/conf/*.*</code> <code>/opt/jp1pcwebcon/sample/conf/*.*</code>	Y

Legend:

Y: Can be collected

--: There is no default file.

#1

For details on the output format of the operation status log, see the chapter describing the log information in the manual *JP1/Performance Management Reference*.

#2

The log file number is the number of output log files, starting from 1.

Operation status log output

The output size of the operation status log (excluding the log for the `jpcrpt` command) can be set by using `logFileSize × logFileNumber` in the initialization file (`config.xml`).

#3

For details about the log output format of the `jpcrpt` command, see [17.4.2\(1\)\(a\) Log output format of the `jpcrpt` command](#).

## (4) Operation information

You need to collect the following information about the operation being performed when an error occurs:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon
- Arguments specified in a command if a problem occurred while the command was executed

## (5) Error information

You need to obtain the following error information:

- Messages output to the console, if the error occurred during command execution

## (6) Docker environment information (Linux)

If you are using Performance Management in a Linux Docker environment, you have to collect the following Docker environment information:

Type of information	Outline	Collected by the <code>jpcras</code> command
Docker environment information	Docker version	Y
	Docker container list	Y
	Process within the Docker container	Y
	Docker container information	Y

Legend:

Y: Can be collected



## 17.6 Procedures for collecting data in the event of trouble

---

This subsection describes how to collect data in the event of an error.

### 17.6.1 Collecting data if a problem occurs in Windows (except for PFM - Web Console)

#### (1) Collecting dump information

The following describes how to collect dump information.

1. Open Task Manager.
2. Select the **Processes** tab.
3. Right-click the name of the process for which you want to collect dump information and select **Create Dump File**.  
Dump files are stored in the following folder:

```
system-drive\Users\user-name\AppData\Local\Temp\
```

4. Collect the dump files from the folder given in step 3.  
If the setting of an environment variable was changed so that the dump files are directed to a folder other than that given in step 3, collect the dump files from the new folder.

#### (2) Executing the data collection command

Use the `jpccras` or `jpccwras` command to collect the data needed to determine the cause of an error. Note that the user who executes the procedures described below must have Administrators permissions.

To execute the data collection command:

1. Log on to the host where the service subject to this data collection is installed.
2. At the command prompt, execute the following command to enable the extended command facility of the command interpreter:

```
cmd /E:ON
```

3. Specify in the `jpccras` or `jpccwras` command the data to be collected and the storage folder for the data, and then execute the command.

The following shows an example of specifying the command when all information that can be obtained by the `jpccras` command is to be stored in the `c:\tmp\jp1pcc\mgr` folder:

```
jpccras c:\tmp\jp1pcc\mgr all all
```

When the `jpccras` command is executed, the `jpctool service list -id * -host *` command is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take some time to complete the `jpctool service list -id * -host *` command. In such a case, by setting the value of the

JPC\_COLCTRLNOHOST environment variable to 1, you can suppress the `jpctool service list -id * -host *` command, to reduce the time required to complete the command.

For details on the `jpccras` command, see the chapter explaining the command in the manual *JP1/Performance Management Reference*.

Note:

If the user account control function (UAC) of the OS is enabled, a dialog box for user account control may appear during command execution. If this occurs, click the **Continue** button to proceed with data collection. Clicking the **Cancel** button stops data collection.

### (3) Executing the data collection command (for logical host use)

The data of Performance Management for logical host use exists on the shared disk, and this data must be collected from both the executing node and standby node.

Use the `jpccras` or `jpccwras` command to collect the data needed to determine the cause of an error. The following describes the procedure for executing the data collection command. Note that the user who executes the procedure described below must have Administrators permissions.

To execute the data collection command for logical host use:

1. Make the shared disk available online.

The data of the logical host is stored on the shared disk. For the executing node, make sure that the shared disk is online and then collect the data.

2. For both the executing and standby nodes, specify in the `jpccras` or `jpccwras` command the data to be collected and the storage folder for the data, and then execute the command.

The following shows an example of specifying the command when all information that can be obtained by the `jpccras` command is to be stored in the `c:\tmp\jplpc\mgr` folder:

```
jpccras c:\tmp\jplpc\mgr all all
```

Point:

To determine the cause of an error in the logical host environment, you need to obtain the data about Performance Management on both physical and logical hosts. Execute the `jpccras` command without the `lhost` argument on a node connected to the shared disk. You can collect all the data about Performance Management on both physical and logical hosts for that node. For this reason, do not specify the `lhost` argument in the `jpccras` command when Performance Management exists in the logical host environment.

If Performance Management exists in the logical host environment, the log files on the shared disk are acquired. In addition, when the `jpccras` command is executed on a node in which the shared disk is offline, files on the shared disk cannot be acquired, but the command ends normally without an error.

Note:

Execute the command to collect the data on both the executing node and standby node. To investigate the conditions before and after a failover, the data of both the executing node and standby node is required.

3. Collect the cluster software data.

This data is required to investigate whether an error occurred in either the cluster software or Performance Management. Collect the data to enable an investigation of the control request, such as a start or stop request from the cluster software to Performance Management, and the results.

When the `jpccras` command is executed, the `jpctool service list -id * -host *` command is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take a long time to complete the `jpctool service list -id * -host *` command. In such a case, by setting the value of the `JPC_COLCTRLNOHOST` environment variable to 1, you can suppress the `jpctool service list -id * -host *` command, to reduce the time required to complete the command.

For details on the `jpccras` command, see the chapter explaining the command in the manual *JP1/Performance Management Reference*.

## (4) Collecting Windows event logs

In Windows Event Viewer, collect the contents of the **System** and **Application** panes.

## (5) Checking information about the operation

Check the information about the operation when an error occurs and record the information. You also need to check the following information:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon
- Arguments specified in a command if a problem occurred while the command was executed

## (6) Collecting error information on window displays

Obtain printouts of the following:

- The Web browser
- The window operation, if an application error occurred
- The error message dialog box  
Also print a copy of any detailed information.
- Command Prompt or the Administrator Console window if a problem occurred while a command was executed  
Before you obtain the printouts of Command Prompt or the Administrator Console window, perform the following in the Command Prompt Properties window.
  - **Edit Options** on the **Options** tab  
Select the **Quick Edit mode** checkbox.
  - The **Layout** tab  
Under **Screen buffer size**, set **Height** to 500.

## (7) Collecting other information

You also need to collect the following information:

- The contents of **System Information**, which is displayed by choosing **Accessories** and then **System Tools**

## 17.6.2 Collecting data if a problem occurs in UNIX (except for PFM - Web Console)

### (1) Executing the data collection command

Use the `jpccras` command to collect the data needed to determine the cause of an error. Note that the user who executes the procedures described below must be a root user.

To execute the data collection command:

1. Log on to the host where the service subject to this data collection is installed.
2. Specify in the `jpccras` command the data to be collected and the storage directory for the data, and then execute the command.

The following shows an example of specifying the command when all information that can be obtained by the `jpccras` command is to be stored in the `/tmp/jp1pc/mgr` directory:

```
jpccras /tmp/jp1pc/mgr all all
```

The data collected by the data collection command is compressed by the `tar` command and the `compress` command or the `gzip` command, and then stored in the specified directory. Example of the file name:

Data collected by the `jpccras` command: `jpccrasYYMMDD.tar.Z`

`YYMMDD` represents the year, month, and date.

When the `jpccras` command is executed, the `jpctool service list -id "*" -host "*" command` is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take an extended period to complete the `jpctool service list -id "*" -host "*" command`. In such a case, by setting the value of the `JPC_COLCTRLNOHOST` environment variable to 1, you can suppress the `jpctool service list -id "*" -host "*" command`, to reduce the time required to complete the command.

For details on the `jpccras` command, see the chapter explaining the commands in the manual *JP1/Performance Management Reference*.

### (2) Executing the data collection command (for logical host use)

The data of Performance Management for logical host use exists on the shared disk, and this data must be collected from both the executing node and standby node.

Use the `jpccras` command to collect the data needed to determine the cause of an error. The following describes the procedure for executing the data collection command. Note that the user who executes the procedure described below must be a root user.

To execute the data collection command for logical host use:

1. Mount the shared disk.  
The data of the logical host is stored on the shared disk. For the executing node, make sure that the shared disk is mounted and then collect the data.
2. For both the executing and standby nodes, specify in the `jpccras` command the data to be collected and the storage directory for the data, and then execute the command.

The following shows an example of specifying the command when all information that can be obtained by the `jpccras` command is to be stored in the `/tmp/jp1pc/mgr` directory:

```
jpcras /tmp/jplpc/mgr all all
```

The data collected by the data collection command is compressed by the `tar` command and the `compress` command or the `gzip` command, and then stored in the specified directory. Example of the file name:

Data collected by the `jpcras` command: `jpcrasYYMMDD.tar.Z`

`YYMMDD` represents the year, month, and date.

Point:

To determine the cause of an error in the logical host environment, you need to obtain the data about Performance Management on both physical and logical hosts. Execute the `jpcras` command without the `lhost` argument on a node connected to the shared disk. You can collect all the data about Performance Management on both physical and logical hosts for that node. For this reason, do not specify the `lhost` argument in the `jpcras` command when Performance Management exists in the logical host environment.

If the `jpcras` command is executed on a node in which the shared disk is not mounted, files on the shared disk cannot be acquired, but the command ends normally without an error.

Note:

Execute the command to collect the data on both the executing node and standby node. To investigate the conditions before and after a failover, the data of both the executing node and standby node is required.

### 3. Collect the cluster software data.

This data is required to investigate whether an error occurred in either the cluster software or Performance Management. Collect the data to enable an investigation of the control request, such as a start or stop request from the cluster software to Performance Management, and the results.

When the `jpcras` command is executed, the `jpctool service list -id "*" -host "*" command` is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take an extended period to complete the `jpctool service list -id "*" -host "*" command`. In such a case, by setting the value of the `JPC_COLCTRLNOHOST` environment variable to 1, you can suppress the `jpctool service list -id "*" -host "*" command`, to reduce the time required to complete the command.

For details on the `jpcras` command, see the chapter explaining the commands in the manual *JP1/Performance Management Reference*.

## (3) Checking information about the operation

Check the information about the operation when an error occurs and record the information. You also need to check the following information:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon

## (4) Collecting error information

You need to obtain the following error information:

- Messages output to the console, if the error occurred during command execution

## (5) Collecting other information

You also need to collect the following information:

- The command arguments that were specified, if the error occurred during command execution

### 17.6.3 Collecting data if a problem occurs (in PFM - Web Console)

#### (1) Executing the data collection command

Use the `jpcwras` command to collect the data needed to determine the cause of an error. Note that the user who executes the procedures described below must be a root user.

To execute the data collection command:

1. Log on to the host where the service whose data you want to collect is installed.
2. Execute the `jpcwras` command, specifying the data to be collected and the storage directory for the data.

The following shows an example of specifying the command when all information that can be obtained by the `jpcwras` command is to be stored in the `/tmp/jp1pcwebcon` directory:

```
jpcwras /tmp/jp1pcwebcon
```

To gather together the data collected by the data collection command, you can use an archiving tool (such as the `tar` command) and compression tool (such as `gzip` or `compress`) available on the host where the data is collected to archive or compress the specified directory in its entirety.

For details on the `jpcwras` command, see the chapter explaining the commands in the manual *JP1/Performance Management Reference*.

#### (2) Collecting error information on the screen

When using a Web browser with PFM - Web Console, collect hard copies of the following:

- The content of the Web browser window
- Windows on the screen when the application error occurred
- The error dialog boxes  
Also copy the detailed information if the dialog box contains a **Details** button.
- The command line of the terminal when an error occurs during command execution.

## 17.7 Restoring the Performance Management system

---

This subsection describes the procedure for using the backup file to restore Performance Management to its normal status when an error occurs in the Performance Management server.

Note:

When restoring from a backup file, make sure that you use the same version of the product.

You can use the following procedure to restore Performance Management to its status before an error occurred.

- For a serious error such as disk failure

This procedure is used when there is a possibility of wide-ranging damage to the Performance Management files due to a physical disk failure, or when the procedure for an error related to changes in the configuration fails to restore the Performance Management system.

Reinstall or set up Performance Management again.

Next, restore the system by restoring, from the backup file, all definition information, performance data, and event data for Performance Management.

Point:

When changing the system configuration or updating the Performance Management version, it is recommended that a backup of the various definition information be obtained. Because performance data and event data are constantly updated, we recommend that you make regular backups in case of a disk failure. Performance Management provides commands for backing up performance data and event data.

For details on obtaining backups, see [9. Backing Up and Restoring Data](#).

### 17.7.1 Procedures for recovering from serious failures such as disk failures

Use the following procedure to restore Performance Management when there is a serious error related to a disk failure.

#### (1) Uninstallation

Uninstall the Performance Management program.

For details on how to uninstall the Performance Management program, see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

#### (2) Reinstallation

Reinstall the Performance Management program.

For details on how to reinstall the Performance Management program, see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

#### (3) Setup

Set up the Performance Management program again. During setup, use the instance name and physical host name used in the environment before the error occurred.



For details on how to set up the Performance Management program, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

## (4) Restoring definition information

Restore the backed-up service definition information.

For details on the service definition information to be restored, see *9.2 Backing up and restoring definition information*.

## (5) Restoring performance data and event data

Restore the backed-up Store database that contains performance data and event data.

For details on restoring the Store database, see *9.3 Backing up and restoring operation monitoring data*.

## (6) Starting services

Start the Performance Management program services and confirm that the services start normally.

For details on starting the services, see *1.2 Starting services*. Use the `jpctool service list` command to check the service status. For details about checking the service status, see *1.6 Checking the status of services*.

## (7) Restoring the report and alarm table definition information

Restore the backed-up report and alarm table definition information.

For details about restoring the report definition information, see *9.2.8 Backing up and restoring a report definition*. For details about restoring the alarm definition information, see *9.2.9 Backing up and restoring an alarm definition*.

## (8) Checking operations

Lastly, make sure that the trouble has been resolved. Check whether the following items are normal:

- Check whether performance data can be collected  
Run Performance Management for more than twice the length of the collection interval for performance data to confirm that performance data can be collected without a problem.  
For details on the collection interval of performance data, see *4.1.1 Modifying the recording options for performance data*.
- Check whether there is a problem with the data in the Store database  
Export the data of the Store database to a text file and check whether there is a problem with the data. Use the `jpctool db dump` command to export the data in the Store database to a text file.  
For details on the `jpctool db dump` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.
- Check the report and alarm definitions  
Check whether there is a problem with the report and alarm definitions. Use PFM - Web Console to check the report and alarm definitions.  
For details on the report definition, see *5. Creation of Reports for Operation Analysis*. For details about the alarm definition, see *6. Monitoring Operations with Alarms*.
- Check the binding of the alarm table  
Check the binding of the alarm table and bind it as necessary.



For details on binding the alarm table, see [6.6.1 Changing the association between an alarm table and a monitoring agent](#).



# Appendixes

## A. Version Changes

---

This appendix explains the changes made to the manual in each version.

### A.1 Changes in 11-50

- Added the auto alarm bind function.
- A folder having the name of the host can now be automatically created as the folder to which to add agents.
- Modified the description regarding the partial backup of performance data with Store version 2.0.
- Added a monitoring process that is linked with the IT service management product (JP1/SS).
- Added a troubleshooting guide to be followed when no alarm event is displayed after the port number of the PFM - Manager is changed during operation.
- Added a description regarding the materials that must be collected when an issue occurs with Performance Management used in a Docker environment.

### A.2 Changes in 11-10

- The following OSs are now supported:
  - AIX V7.2
  - Microsoft(R) Windows Server(R) 2016
- From the event console window of JP1/IM, you can now display Performance Management reports about an event source host even if the reports have not been associated with alarms.
- By linking Performance Management with JP1/AJS3, from the Dashboard window you can now display Performance Management reports about a job execution host.
- The description of the setup procedure for linking with JP1/IM was changed.

### A.3 Changes in 11-01

- Restart of the Performance Management services is now unnecessary if the information about the local host is not changed after editing the `jpchosts` file.
- Firewall information (Linux) was added as the OS information that must be collected when a problem occurs.

### A.4 Changes in 11-00

#### (1) Changes from manual 3021-3-042-30(E) to manual 3021-3-A38(E)

- The following operating systems are no longer supported:  
PFM - Manager and PFM - Web Console
  - Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2003 (include R2)

- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2008 (other than R2)
- AIX 6 (32-bit)
- AIX 7 (32-bit)
- HP-UX 11i V3 (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (32-bit x86)
- Solaris 10

#### PFM - Base

- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2003 (include R2)
- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2008 (other than R2)
- AIX 6 (32-bit)
- AIX 7 (32-bit)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (32-bit x86)
- The following operating systems are now supported:
  - CentOS 6.1 (x64) or later
  - CentOS 7.1 or later
  - Red Hat Enterprise Linux<sup>(R)</sup> Server 7.1 and later
  - Oracle Linux<sup>(R)</sup> Operating System 6.1 (x64) and later
  - Oracle Linux<sup>(R)</sup> Operating System 7.1 and later
  - SUSE Linux<sup>(R)</sup> Enterprise Server 12
- A product name was changed from JP1/ITSLM to JP1/SLM.
- Linkage with network management products (NNM) was deprecated.
- ODBC-compliant application programs were deprecated.
- Encrypted communication was supported to connect from web browsers to monitoring console servers.
- The following languages were supported by Performance Management:
  - Korean
  - Spanish
  - Chinese (simplified)
  - German
  - French
  - Russian

- Checking of alarm application status and application of alarm information were supported.

## **(2) Changes from manual 3021-3-348-20(E) to manual 3021-3-A38(E)**

- The following operating systems are no longer supported:

PFM - Manager and PFM - Web Console

- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2003 (include R2)
- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2008 (other than R2)
- AIX 6 (32-bit)
- AIX 7 (32-bit)
- HP-UX 11i V3 (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (32-bit x86)
- Solaris 10

PFM - Base

- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2003 (include R2)
- Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2008 (other than R2)
- AIX 6 (32-bit)
- AIX 7 (32-bit)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (32-bit x86)
- The following operating systems are now supported:
  - CentOS 6.1 (x64) and later
  - CentOS 7.1 or later
  - Red Hat Enterprise Linux<sup>(R)</sup> Server 7.1 and later
  - Oracle Linux<sup>(R)</sup> Operating System 6.1 (x64) and later
  - Oracle Linux<sup>(R)</sup> Operating System 7.1 and later
  - SUSE Linux<sup>(R)</sup> Enterprise Server 12
- The following monitoring agent products were added:
  - PFM - Agent for Cosminexus
  - PFM - Agent for DB2
  - PFM - Agent for Domino
  - PFM - Agent for Exchange Server

- PFM - Agent for HiRDB
- PFM - Agent for IIS
- PFM - Agent for OpenTP1
- PFM - Agent for WebLogic Server
- PFM - Agent for WebSphere Application Server
- A product name was changed from JP1/ITSLM to JP1/SLM.
- Linkage with network management products (NNM) was deprecated.
- ODBC-compliant application programs were deprecated.
- Encrypted communication was supported to connect from web browsers to monitoring console servers.
- Checking of alarm application status and application of alarm information were supported.

## A.5 Changes in 10-50

### (1) Changes in manual 3021-3-042-30(E)

Note: The changes include the functions that were added between version 10-10 and version 10-50.

- The following operating systems are now supported:
  - Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2012 R2 Datacenter
  - Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2012 R2 Standard
- The monitoring suspension function was supported.
- The [Action Handler Section] section was added to the startup information file (`jpccomm.ini`) (synchronous execution controller for actions).
- The Random Retry Mode label was added to the [Common Section] section in the startup information file (`jpccomm.ini`) (dispersion of reconnection).
- A modification was made so that service startup is suspended when a physical host name used as the monitoring host name of PFM - Manager, PFM - Agent, or PFM - RM is changed in an undesigned method.
- The function that prioritizes collection of historical data over display of real-time reports (history collection priority function) is now supported.

### (2) Changes in manual 3021-3-348-20(E)

Note: The changes include the functions that were added between version 10-10 and version 10-50.

- The following operating systems are now supported:
  - Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2012 R2 Datacenter
  - Microsoft<sup>(R)</sup> Windows Server<sup>(R)</sup> 2012 R2 Standard
- The monitoring suspension function is now supported.
- The Action Handler Section section was added to the startup initialization file (`jpccomm.ini`) (the synchronous execution controller for actions).
- The Random Retry Mode label was added to the Common Section section of the `jpccomm.ini` file (the dispersion of the reconnection).

- A modification was made so that service startup is suspended when a physical host name used as the monitoring host name of PFM - Manager, PFM - Agent, or PFM - RM is changed in an undesigned method.
- The function that prioritizes the collection of historical data over the display of real-time reports (history collection priority function) is now supported.

## A.6 Changes in 10-10

### (1) Changes in manual 3021-3-042-20(E)

- The following operating systems are now supported:
  - Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
  - Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- A modification was made so that status changes of each record instance can be monitored by a single alarm definition.
- The manual configuration was modified as follows:
  - The contents from subsections 6.9.3(3) to (5) were moved to subsections 6.2.2(1) to (3).
- A command for synchronizing the configuration information of PFM - Manager and PFM - Agent (or PFM - RM) is now supported. This eliminates the need to restart PFM - Agent (or PFM - RM) after configuration information is restored in PFM - Manager.
- The multiple monitoring function is now supported.

### (2) Changes in manual 3021-3-348-10(E)

- The following OSs are now supported:
  - Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
  - Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- A modification was made so that status changes of each record instance can be monitored by a single alarm definition.
- The manual configuration was modified as follows:
  - The contents from subsections 6.9.3(3) to 6.9.3(5) were moved to subsections 6.2.2(1) to (3).
- A command for synchronizing the configuration information of PFM - Manager and PFM - Agent (or PFM - RM) is now supported. This eliminates the need for restart of PFM - Agent (or PFM - RM) after configuration information is restored in PFM - Manager.
- The multiple monitoring function is now supported.

## A.7 Changes in 10-00

### (1) Changes in manual 3021-3-042-10(E)

- The following operating systems are no longer supported:
  - HP-UX 11i V2 (IPF)
  - Solaris 9 (SPARC)
  - Solaris 10 (x64)

- Solaris 10 (x86)
- AIX 5L V5.3
- Red Hat Enterprise Linux<sup>(R)</sup> AS 4 (AMD64 & Intel EM64T)
- Red Hat Enterprise Linux<sup>(R)</sup> AS 4 (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> AS 4 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> ES 4 (AMD64 & Intel EM64T)
- Red Hat Enterprise Linux<sup>(R)</sup> ES 4 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (x86)
- The following operating systems are now supported:
  - Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (64-bit x86\_64)
  - Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (32-bit x86)
  - Microsoft<sup>(R)</sup> Windows Server 2012 Datacenter
  - Microsoft<sup>(R)</sup> Windows Server 2012 Standard
- JP1 Performance Management can now link with JP1/IT Service Level Management.
- Performance data can now be collected in IPv6 environments.
- Limits were added to the filter text boxes.
- A note regarding the Agents window was added.
- Filter conditions can now be specified when searching from a window.
- Data group buttons were added for navigating to a report's previous or next time band.
- The descriptions of backup and restoration were revised.
- Information about backup and restoration of the information set in definition templates for process monitoring was added.
- Information about migrating definition information and operation monitoring data was added.
- JP1 event settings were added to the health check agent properties.
- Information about the output format of troubleshooting logs was added.
- The start time and end time can now be hidden when a report is displayed.

## **(2) Changes in manual 3021-3-348(E)**

- The following operating systems are no longer supported:
  - HP-UX 11i V2 (IPF)
  - Solaris 9 (SPARC)



- Solaris 10 (x64)
- Solaris 10 (x86)
- AIX 5L V5.3
- Red Hat Enterprise Linux<sup>(R)</sup> AS 4 (AMD64 & Intel EM64T)
- Red Hat Enterprise Linux<sup>(R)</sup> AS 4 (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> AS 4 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> ES 4 (AMD64 & Intel EM64T)
- Red Hat Enterprise Linux<sup>(R)</sup> ES 4 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 (x86)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (AMD/Intel 64)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (IPF)
- Red Hat Enterprise Linux<sup>(R)</sup> 5 Advanced Platform (x86)
- The following operating systems are now supported:
  - Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (64-bit x86\_64)
  - Red Hat Enterprise Linux<sup>(R)</sup> Server 6 (32-bit x86)
  - Microsoft<sup>(R)</sup> Windows Server 2012 Datacenter
  - Microsoft<sup>(R)</sup> Windows Server 2012 Standard
- JP1 Performance Management can now link with Job Management Partner 1/IT Service Level Management Description, User's Guide, Reference and Operator's Guide.
- Performance data can now be collected in IPv6 environments.
- Limits now apply to the process that refines on-screen information based on keywords.
- A point regarding the Agents window has been added.
- You can now specify filter conditions when searching from a window.
- Data group buttons have been added that you can use to navigate to the previous or next time band of a report.
- The description of backup and restoration has been revised.
- Information about the backup and restoration of the information set in definition templates for process monitoring has been added.
- Information about migrating definition information and operation monitoring data has been added.
- JP1 event settings have been added to the health check agent properties.
- Information about the output format of troubleshooting logs has been added.
- The start time and end time can now be hidden when displaying a report.

## A.8 Changes in 09-50

### (1) Changes in manual 3020-3-R32-31(E)

- An access control feature based on business groups has been added, allowing you to set the range of information individual users can monitor.
- Business group ordinary user has been added as a user permission for Performance Management.
- You can now use the following commands to create and edit business groups:
  - `jpccconf bgdef check`  
Verifies the contents of a business group definition file.
  - `jpccconf bgdef delete`  
Deletes definition information for a business group.
  - `jpccconf bgdef display`  
Displays definition information for a business group.
  - `jpccconf bgdef export`  
Exports definition information for a business group to a file.
  - `jpccconf bgdef import`  
Imports definition information for a business group from a file.
  - `jpccconf bgdef list`  
Displays a list of business group names.
- In the Edit Agents > New Agents window, you can now use keywords to refine the list of agents.
- The `jpctool service sync` command can now be used to synchronize the service information registered in PFM - Manager and PFM - Web Console.
- The autolabel feature can now display tooltips that show data values plotted on a graph.
- The default color for graph series has been changed. You can also now change the color used to display series in a graph.
- A cautionary note about pie graphs has been added.
- Information about how to plan report definitions to avoid a memory shortage when displaying reports that use graphs has been added.
- A cautionary note describing what to do when a report takes a long time to display has been added.
- Information about the temporary files created when a graph image is displayed or output has been added.
- The **Show Grid** graph option now only applies to the graph in the foreground.
- When a series group contains 3D clustered column/3D stacked column graphs or line graphs, any group can now be displayed in the foreground regardless of the order of the series groups.
- The sequence in which the Y axis scales are displayed in combination reports now conforms to the order in which the graphs are drawn.
- The following conditions regarding combination reports have been added or changed:
  - The conditions under which some or all of a graph or legend is invisible and the legend breaks over two or more lines
  - The conditions under which part of the legend is invisible due to an excessive number of characters
  - The conditions under which the series group name overlaps the legend

- The conditions under which a line break appears in the graph title
- The user-created alarm table can now be displayed as a separate tree from the table of alarms defined by monitoring templates.
- The maximum number of alarms you can define in one alarm table has been increased from 50 to 250. Accordingly, the maximum number of alarms you can define in one alarm definition file has been increased from 50 to 250.
- The circumstances that cause an alarm event with the message text `Alarm Cleared` to be generated have been changed. Accordingly, a description of alarm evaluation when PFM - Agent or PFM - RM stops has been added.
- The following message text can now be output in an agent event relating to the operation status of a monitored system:
  - `Monitored System Available`
  - `Monitored System Unavailable`
- Depending on the confirmation status of an agent alarm, the following message text can now be output in an agent event:
  - `State change(Unconfirmed)`
  - `State information`
  - `State information(Unconfirmed)`
- The `jpccprocdef` command has been added.
- A cautionary note about the health check function has been added.
- Troubleshooting procedures have been added for the following circumstances:
  - When the Correlator service takes a long time to start after PFM - Manager restarts
  - When the Agent Collector service or Remote Monitor Collector service fails to start
- Windows firewall information is now part of the troubleshooting information collected when a problem occurs in a Windows environment.
- A list of command locations has been added.

## A.9 Changes in 09-10

### (1) Changes in manual 3020-3-R32-21(E)

- Information about the settings of the health check function when PFM - Manager version 09-00 or later is installed has been added.
- You can now limit the information available to users with general user permission in the **Agents** tree.
- Process monitoring in PFM - Agent for Platform and PFM - RM for Platform can now be configured in the **Agents** tree.
- Information about the number of user accounts has been added.
- The following commands can now be used to create and edit the Agents tree.
  - `jpccconf agttree export`  
Exports an Agents tree definition file.
  - `jpccconf agttree import`  
Imports an Agents tree definition file.

- Information about how to handle a situation in which performance data collection is skipped has been added.
- The **OK** button has been removed from the Service Properties window, and **Close** and **Apply** buttons have been added.
- Information about the retention period for records in the Store database has been added.
- Reports can now be displayed over several pages when there are too many graph legends.
- The information cached to memory when displaying reports can now be output to a file.
- The maximum number of lines of table data displayed in the Print window and in HTML reports can now be restricted.
- The maximum number of drilldown data items in a graph can now be restricted.
- When monitoring alarms using multi instance records, users can now be notified when the value of a field returns to a normal range.
- An example of alarm evaluation when a monitoring time range and damping condition are specified has been added.
- An example of specifying an abnormal condition and warning condition in an alarm condition has been added.
- The message sent when a JP1 event is issued can now be defined within a range from 0 to 1,023 bytes.
- Information about the limits that apply to the number of alarm tables you can define in one Agent product has been added.
- Information about the character encodings used during alarm evaluation has been added.
- The setup command can now be executed in non-interactive mode.
- Information about making changes to a logical host environment after starting operation has been added.
- You can now choose how the system determines which Action Handler service is selected by default in the New Alarm > Action Definition window and Edit > Action Definitions window of PFM -Web Console when issuing a JP1 event.

## A.10 Changes in 09-00

### (1) Changes in manual 3020-3-R32(E)

- PFM - RM has been added to the Performance Management product to support remote monitoring.
- Events that occur in a Performance Management service can now be reported as JP1 system events or agent events.
- The product name display function has been added. Service keys and IDs can now be displayed and specified in a new format.
- A new command syntax compatible with pre-08-11 commands has been added. A unified option specification format has been introduced.
- Summaries of the entire system status and the latest operating status of services can now be checked in the Summary View.
- The tiling display function has been added. Multiple historical report graphs can now be displayed as thumbnails.
- The search fields function has been added. Information on an item to be monitored can now be found by searching for a keyword when setting an alarm or report.
- The Quick Guide function has been added. Reports can now be displayed without performing a conventional report definition procedure. The alarm definition procedure has been simplified.
- A definition for displaying a report can now be edited from the View Report window.

- The procedure for changing the name of a host running a Performance Management product has been simplified.
- PFM - Manager, PFM - Base, and PFM - Web Console services can now be started and stopped in a synchronized manner.
- Internet Explorer 7.0 and Firefox 3 have been added as monitoring console Web browsers.
- Mozilla has been removed as a monitoring console Web browser.
- An agent for monitoring a virtual environment has been added.
- Remote monitors for Windows, UNIX, Oracle, and Microsoft SQL Server have been added.
- The name *solution set* has been changed to *monitoring template*.
- The alarm table version in the monitoring template for the health check agent has been changed from 8.11 to 8.50 and 09.00.
- The alarm table in the monitoring template for the health check agent has been renamed to the following:  
PFM Health Check Template Alarms
- For JP1 Version 9 JP1/Performance Management, the manual contents of the old edition *JP1 Version 8 JP1/Performance Management System Configuration and User's Guide* (3020-3-K61-40(E)) have now been divided into the following two manuals.
  - *JP1 Version 9 JP1/Performance Management Planning and Configuration Guide* (3020-3-R31(E))
  - *JP1 Version 9 JP1/Performance Management User's Guide* (3020-3-R32(E))

The following table describes the correspondence between the *JP1 Version 8 JP1/Performance Management System Configuration and User's Guide* (3020-3-K61-40(E)) and the *JP1 Version 9 JP1/Performance Management User's Guide* (3020-3-R32(E)):

<i>JP1 Version 8 JP1/Performance Management System Configuration and User's Guide</i> (3020-3-K61-40(E))	<i>JP1 Version 9 JP1/Performance Management User's Guide</i> (3020-3-R32(E))
PART 1: Overview	Moved to the <i>JP1 Version 9 JP1/Performance Management Planning and Configuration Guide</i> (3020-3-R31(E)).
1. Overview of Performance Management	
2. Using Performance Management	
PART 2: Design	
3. Design of Operation Monitoring Systems that Use Performance Management	
4. Performance Management Functions	
PART 3: Configuration	
5. Installation and Setup (in Windows)	
6. Installation and Setup (in UNIX)	
PART 4: Operation	PART 1: Operation
7. Starting and Stopping Performance Management	1. Starting and Stopping Performance Management
8. Managing User Accounts	2. Managing User Accounts
9. Monitoring Agents	3. Monitoring Agents
10. Managing Operation Monitoring Data	4. Managing Operation Monitoring Data
11. Creation of Reports for Operation Analysis	5. Creation of Reports for Operation Analysis
12. Operation Monitoring with Alarms	6. Operation Monitoring with Alarms

<i>JP1 Version 8 JP1/Performance Management System Configuration and User's Guide (3020-3-K61-40(E))</i>	<i>JP1 Version 9 JP1/Performance Management User's Guide (3020-3-R32(E))</i>
13. Displaying Events	7. Displaying Events
14. Backing Up and Restoring Data	8. Backing Up and Restoring Data
PART 5: System Linkage	PART 2: System Linkage
15. Construction and Operation with a Cluster System	9. Construction and Operation with a Cluster System
16. Operation Monitoring Linked with the Integrated Management Product JP1/IM	10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring
17. Linking with Network Node Manager (NNM) for Operation Monitoring	11. Linking with Network Node Manager (NNM) for Operation Monitoring
18. Linking with ODBC-Compliant Application Programs for Operation Analysis	12. Linking with ODBC-Compliant Application Programs for Operation Analysis
PART 6: Troubleshooting	PART 3: Troubleshooting
19. Detecting Problems within Performance Management	13. Detecting Problems within Performance Management
20. Error Handling Procedures	14. Error Handling Procedures
Appendix A. Limits	Moved to the <i>JP1 Version 9 JP1/Performance Management Planning and Configuration Guide (3020-3-R31(E))</i> .
Appendix B. Naming Rules	
Appendix C. System Estimates	
Appendix D. Kernel Parameter List	
Appendix E. Migration Steps and Notes on Migration	
Appendix F. Version Compatibility	
Appendix G. Outputting Action Log Data	
Appendix H. Health Check Agent	
Appendix I. Version Changes	
Appendix J. Glossary	Appendix B. Glossary

- Windows Server 2008 is now supported.
- A report graph can now be displayed with time adjustment.
- A PFM service that has stopped abnormally can now be restarted automatically.
- More than one alarm table can now be bound to a monitoring agent.
- Performance Management can now be used in an environment where there are multiple hosts with the same name.
- The Performance Management setup procedure has been simplified.
- PFM - Web Console can now be used in a UNIX environment.
- A description required for installing a Solaris patch for version 09-00 has been added.
- The number 4.0 has been added to the data model version of the health check agent. Accordingly, the `PI_HAVL`, `PD_HOST`, and `PI_SYS` records have been added.
- The number 8.50 has been added as the alarm table version in the monitoring template of the health check agent. Accordingly, the `Host Status Change` and `Host Not Available` alarms have been added.

- Host Availability (4.0), Hosts Availability (4.0), Hosts Status (Real-Time) (4.0), and System Summary (4.0) have been added as reports in the monitoring templates of the health check agent.

## **B. Reference Material for This Manual**

---

The reference material for readers of this manual is described in the *JP1/Performance Management Planning and Configuration Guide*.



## C. Glossary

---

Terminology used in this manual

See the glossary in the appendixes of the *JPI/Performance Management Planning and Configuration Guide*.

# Index

## A

- abnormal status 108
  - Action Handler label 294, 295
  - actions 242
    - notes on executing 268
    - possible when alarm status changes 266
    - setting 266
  - administrator user permission 64
  - agent event 330
  - agent for PFM - Agent 97
  - agents
    - Agent for PFM - Agent 97
    - associating with alarm 304
    - changing association with alarm table 279
    - checking agent status 106
    - checking connection to alarm table 309
    - displaying properties 116
    - displaying those bound to alarm table 281
    - distributing properties in batch 117
    - editing properties 117
    - integrated management 516
    - monitoring 95
    - PFM - RM group agent 97
    - PFM - RM remote agent 97
    - types 97
    - types supporting summary display 110
    - unbinding alarm tables 306
    - usable types 97
  - Agents tree 96
    - creating using commands 104
    - editing using commands 104
  - alarm application status, checking 283
  - alarm conditions
    - differences among alarm 244
  - alarm created by using Quick Guide
    - default values 277
  - alarm damping 248
  - alarm definition
    - checking file 298
    - creating file 287
    - modifying 298
  - Alarm Definition File Code label 289
  - Alarm Definition File Version label 288
  - alarms 242
  - Alarm Name label 290
  - Alarm Table Name label 289
  - associating with report 270
  - character encoding during evaluation 326
  - checking status 107
  - condition 263
  - copying 271
  - creating 261
  - creating using Quick Guide 276
  - deleting 272, 302
  - displaying associated reports 331
  - displaying properties (definition) 285
  - editing 272
  - events 242, 330
  - message 262
  - message text 255
  - name 262
  - notes on creating 315
  - notes on evaluating 325
  - operating 243
  - properties 331
  - setting in Web browser (Alarms tree) 261
  - setting in Web browser (Quick Guide) 276
  - setting up 243
  - starting monitoring by using 311
  - status 108
  - table 242
  - table name 261
  - using to start monitoring 282
  - using to stop monitoring 282, 310
- alarm tables
    - associating with monitoring agent 304
    - changing association with monitoring agent 279
    - checking connection to monitoring agent 309
    - checking properties 312
    - copying 271, 300
    - deleting 272, 301
    - displaying bound monitoring agents 281
    - exporting 273
    - importing 274
    - unbinding with monitoring agent 306
  - all business groups 80
  - all execution mode 541
  - assigned business groups 80
  - assignment of business groups 80

- associating
  - alarm table with monitoring agent 304
- associating report with alarm 270
- authentication mode
  - user account 78
- Autolabel
  - checking data values 207
- Automatically binding alarms to monitoring agents 274
- automatic bind 244
- automatic refresh interval 53
- automatic restart functionality 670
  - configuring 671
  - service startup units 671
  - using 674
- available functions
  - business group users 71
  - system users 66

## B

- backing up 349
  - cluster system 518
  - event data 392
  - performance data 394
  - performance data, partial (Store 2.0) 397
- backup data
  - converting data model (Store 2.0) 152
  - importing (Store 2.0) 151
- baseline 166
  - registering in combination bookmark 215
- batch distribution of properties 117
- batch switching
  - primary Manager 560
  - secondary Manager 560
- binding 242, 279
- bookmark folder
  - deleting 194
  - renaming 193
- bookmark properties
  - checking 195
- bookmarks
  - adding folder 192
  - creating 190
  - deleting 194
  - renaming 193
- building
  - system linked with JP1/AJS3 620
  - system linked with JP1/SS 629

- business group definition file 86
- Business Group Definition File Code label 87
- Business Group Definition File Version label 87
- Business Group Name label 88
- business group ordinary user 65
- business group user 64
- business group users
  - available functions 71

## C

- cautionary notes
  - relationship between alarm damping and issuing events 316
  - report series paging 224
  - starting and stopping 54
- changing
  - business group assignments 82
  - password 81
  - permissions of user account 82
- changing configuration after JP1/SLM linkage 610
  - applying changes in Performance Management 612
  - host name 610
  - PFM - Manager logical host 611
- character set
  - changing 315
- checking
  - agent status 106
  - alarm status 107
  - alarm table properties 312
  - bookmark properties 195
  - operation monitoring data (event data) 558
  - operation monitoring data (performance data) 558
  - operation monitoring data matches 558
  - service status, from web browser 51
- checking duplication
  - definition information (alarm information of alarm definition and action definition) 553
  - definition information (binding information) 553
  - definition information (bookmark definition information) 556
  - definition information (business group information) 554
  - definition information (managed agents) 555
  - definition information (Performance Management user account information and agents tree (User Agents) information) 554
  - definition information (process monitoring template information) 556

- definition information (report definition) 553
- definition information (settings of auto alarm bind) 555
- definition information (settings of PFM - Manager for connection destination) 555
- PFM - Manager definition information 553
- PFM - Web Console definition information 556
- checking settings
  - PFM - Manager to which monitoring agent connects 557
- Check Value Exist label 290
- cluster configuration
  - designing 407
- cluster software 476
- cluster system 405
  - backing up and restoring 518
  - changing configuration (UNIX) 491
  - changing configuration (Windows) 443
  - collecting and managing operation monitoring data 517
  - configuration in UNIX 465
  - configuration in Windows 415
  - environment directory 413
  - executing node 405
  - failover 405, 519
  - failure recovery 522
  - integrated agent management 516
  - local disk 413
  - logical host 412, 413
  - logical host name 416, 465
  - logical IP address 416, 465
  - managing user accounts 516
  - note 523
  - operation 513
  - overview 405
  - PFM - Manager services to register (standalone mode) 426
  - PFM - Manager services to register (with PFM - Manager, PFM - RM for Platform, and PFM - Agent for Oracle) 427
  - physical host 413
  - planning data configuration 413
  - planning failover method 414
  - planning network configuration 412
  - planning operation 414
  - realtime monitoring by alarm 518
  - shared disk 413
  - standby node 405
  - starting and stopping Performance Management 513
  - status management 667
- collecting and managing
  - operation monitoring data 517
- Collection Interval property 128
- Collection Offset property 128
- combination bookmark
  - registering baseline in 215
- combination reports
  - displaying 212, 216
  - examples of real-world use 218
  - notes on 236
  - preparing to display 215
  - whether displayable 212
- Command label 292
- commands
  - jpcaspsv output 144
  - jpcaspsv update 144
  - jpcasrec output 129
  - jpcasrec update 130
  - jpccconf agtree export 105
  - jpccconf db display 152
  - jpctrdef create 188
  - jpctrdef delete 189
  - jpctrdef output 188
  - jpccspm start 30
  - jpccspm stop 40
  - jpctool alarm active 311
  - jpctool alarm bind 304
  - jpctool alarm check 298
  - jpctool alarm copy 300
  - jpctool alarm delete 301, 302
  - jpctool alarm export 287, 298, 313
  - jpctool alarm import 299
  - jpctool alarm inactive 310
  - jpctool alarm list 309
  - jpctool alarm unbind 306
  - jpctool db clear 151, 156
  - jpctool db dump 155
  - jpctool db import 151
  - jpctool service list 50
  - jpccwstart 35
  - jpccwstop 43
  - operating alarm by using 304
  - setting alarm by using 287
  - ulimit 158
- common message logs (troubleshooting) 725, 726

- component version [173](#)
- condition
  - alarms [263](#)
- Condition label [291](#)
- config.xml [230](#)
- configuration
  - cluster system in UNIX [465](#)
  - cluster system in Windows [415](#)
- configuration for issuing JP1 events [254](#)
- configuration for sending SNMP traps [254](#)
- configuring
  - health check function [640](#)
  - status management function [664](#)
- configuring email sender [252](#)
- control command
  - PFM - Manager [476](#)
  - PFM - Web Console registered in cluster software [482](#)
- controlling
  - execution of remote actions [541](#)
  - remote actions [541](#)
- conventions
  - diagrams [10](#)
  - fonts and symbols [11](#)
  - mathematical expressions [12](#)
  - version numbers [12](#)
- copying
  - alarm [271](#)
  - alarm table [271](#), [300](#)
  - reports [180](#)
- counting range for summary display [114](#)
- counting unit for summary display [114](#)
- creating
  - alarm definition file [287](#)
  - alarms [261](#)
  - alarms using Quick Guide [276](#)
  - alarm tables [261](#)
  - new report [170](#)
  - notes on creating reports [229](#)
  - report [517](#)
  - report by using command [188](#)
  - report by using existing report [170](#)
  - reports in Web browser (Quick Guide) [185](#)
  - reports in Web browser (Reports tree) [172](#)
- creating in Web browser
  - Agents tree [98](#)

- creating PFM - Manager logical host after JP1/SLM linkage [611](#)
- CSV format [225](#)
  - outputting event history [336](#)
- CSV output [223](#)

## D

- Damping setting
  - differences among alarm evaluations [247](#)
- data configuration
  - planning [413](#)
- data model
  - converting for backup data (Store 2.0) [152](#)
  - version [173](#)
- data to be collected in event of trouble [735](#)
- data to be collected in the event of trouble (in UNIX) [742](#)
- data to be collected in the event of trouble (in Windows) [735](#)
- default values
  - for reports with Quick Guide [186](#)
  - of alarm created by using Quick Guide [277](#)
- definition information
  - duplicated from primary Manager onto secondary Manager [529](#)
  - duplicating [548](#)
  - exporting [549](#)
  - importing [551](#)
  - matched in jpccomm.ini [531](#)
  - multiple monitoring [528](#)
  - same setting must be specified on primary Manager and secondary Manager [529](#)
- definition information (alarm information of alarm definition and action definition)
  - checking duplication [553](#)
- definition information (binding information)
  - checking duplication [553](#)
- definition information (bookmark definition information)
  - checking duplication [556](#)
- definition information (business group information)
  - checking duplication [554](#)
- definition information (managed agents)
  - checking duplication [555](#)
- definition information (Performance Management user account information and agents tree (User Agents) information)
  - checking duplication [554](#)
- definition information (process monitoring template information)

- checking duplication 556
- definition information (report definition)
  - checking duplication 553
- definition information (settings of automatic bind)
  - checking duplication 555
- definition information (settings of PFM - Manager for connection destination)
  - checking duplication 555
- deleting
  - alarm 273, 302
  - alarm tables 272, 301
  - bookmark 194
  - bookmark folder 194
  - folders, bookmarks, reports 194
  - report folder 183
  - report from bookmark 195
  - reports 183
  - unnecessary reports 189
  - user account 83
- deleting and setting
  - properties 127
- deleting PFM - Manager logical host after JP1/SLM linking 611
- Description property 127
- designing
  - cluster configuration 407
- Detail Records 127
- detecting problems by linking with the integrated system monitoring product 676
- diagram conventions 10
- differences among alarm evaluations
  - depending on combinations of alarm conditions 244
  - depending on whether Damping is enabled 247
- disabling alarm 310
- disk space 150, 155
  - checking for event data 155
  - for performance data 150
- display condition for event monitor window
  - setting 332
- display conditions
  - setting for report 203
- display format 177
  - reports 167
- display format of combination report
  - setting 216
- displaying
  - agent properties 116

- alarm properties (definition) 285
- combination report 212
- displaying agents bound to alarm table 281
- drilldown reports 205
- event history 333
- events 329
- info. about Store services (Store 2.0) 152
- latest event 330
- latest event info. 330
- list of alarm tables 313
- New Report window 172
- notes on displaying reports 229
- reports 199
- display period 176
- distributing
  - agent properties in batch 117
- drilldown reports 179
  - displaying 205
- duplicating
  - definition information 548
- duplicating definition information
  - procedure 548

## E

- editing
  - agent properties 117
  - alarms 272
  - reports 180
- editing in Web browser
  - Agents tree 98
- E-mail Address label 294
- E-mail label 292
- enabling alarm 311
- environment directory 413
- erasing
  - event data 156
  - performance data 151
- error handling procedure 680
- errors
  - list of different types 681
- evaluating alarms
  - when "State changes for each record instance" is not selected 248
  - when "State changes for each record instance" is selected 249
  - when monitoring time range and damping conditions are specified 248

- When monitoring time range and damping conditions are specified 249
- event data
  - backing up and restoring 392
  - checking disk space 155
  - erasing 156
  - exporting 155
  - managing 154
- event history
  - displaying 333
  - outputting in CSV format 336
- event history
  - outputting in CSV format 336
- Event History window 333
- Event ID label 295
- event log file (troubleshooting) 725
- Event Monitor window 330
- events
  - alarms 242, 330
  - changing max. num of records 154
  - displaying 329
  - displaying latest info. 330
  - JP1 event types 566
- example
  - creating definition file for log file trapping 677
  - detecting problem in PFM - Agent 638
  - detecting problem in PFM - RM 639
  - graph 169
  - list 168
  - operation monitoring by Performance Management with JP1/IM 563
  - table 168
  - using combination reports in real world 218
  - using health check function 652
- executing node 405
- execution mode for remote actions 541
- execution procedure of data collection command (troubleshooting) 749
- existing report
  - creating report by using 170
- export 149
- exporting
  - alarm tables 273
  - definition information 549
  - event data 155
  - performance data 149
  - reports 183

- reports in CSV or HTML by browser 223
- reports in CSV or HTML by command 224
- exporting definition information
  - PFM - Manager 549
  - PFM - Web Console 550
- <ex-product-detail> tag 140
- <ex-product-interval> tag 140
- <ex-product-log> tag 140

## F

- failover 405
  - cluster system 519
- failover method
  - planning 414
- failure recovery
  - cluster system 522
- features
  - multiple monitoring 526
- field-level drilldown report 179
- fields
  - filter conditions for report 175
  - searching for 174, 185, 265
  - setting for a report 174
- filter condition 175
- folders
  - deleting 194
  - for alarms 242
  - renaming for bookmarks 193
- font conventions 11
- functionality for binding multiple alarm tables 279, 304

## G

- general user permission 64
  - limiting available agents 103
- glossary 773
- graph 168
  - example 169
  - rearranging (tiling display) 197

## H

- HA cluster system 405
- health check function 637
  - configuring 640
  - examples of using 652
- historical (multiple agents) 173
- historical (single agent) 173



- historical report 166
- Host Name
  - output by jpc tool service list command 50
- Host Name label 88
- Host Not Available 648, 650, 651
- how to check service status 665
- how to collect dump information (troubleshooting) 749
- HTML format 226
  - outputting event history 336
- HTML output 223

## I

- importing
  - alarm tables 274
  - backup data (Store 2.0) 151
  - definition information 551
  - reports 184
- importing definition information
  - PFM - Manager 551
  - PFM - Web Console 551
- Incomplete 648, 651
- inherited information 206
- inittab 33, 37
- installation
  - when linking with JP1/IM 567
- integrated console
  - monitoring with 564
- integrated management
  - agents 516
- integrated scope
  - monitoring with 564
- interval for evaluating alarm 326
- Interval Records 127

## J

- JP1/AJS3 linkage
  - building system 620
  - monitoring 615
- JP1/Base 676
  - example of definition file for log file trapping 677
  - starting log file trapping function 678
- JP1/IM 563, 564
  - linking with Performance Management 565
- JP1/IM linkage
  - operation monitoring 562
- JP1/SLM 598

- changing configuration after linkage 610
- linkage 599
- linkage operations 613
- linkage prerequisites 600
- linked instances, number of 600
- monitoring performance data 613
- programs for linkage 600
- starting monitoring 613
- stopping monitoring 613
- JP1/SLM linkage 599
  - JP1 user authority 601
  - monitoring items 603
  - network settings 602
  - prerequisites 600
  - recording performance data 601
  - releasing 606
  - setup 605
  - user authentication mode and business groups 601
- JP1/SS linkage
  - building system 629
  - monitoring 625
- JP1 authentication mode 64, 84
- JP1 event attributes
  - when linking with JP1/IM 586
- JP1 Event label 293
- JP1 events 268
  - types of 566
- JP1 permission level 84
- JP1 resource group 84
- JP1 Resource Group Name label 88
- JP1 system event 566
- JP1 user 64
- JP1 user authority for JP1/SLM linkage 601
- JP1 user event 566
- jpc\_start 33
- jpc\_start.model 33
- jpc\_stop 42
- jpc\_stop.model 42
- jpccomm.ini 541, 677
- jpccconf agtree export 104
- jpccconf mgrhost define 540
- jpccconf primmgr notify 560
- jpctool config mglexport 549, 551
- jpctool db dmconvert 152
- jpctool db dump 149
- jpccsvr.ini 78
- jpccwbackup 550



## L

- LANG environment variable (troubleshooting) 725
- language of common message log (troubleshooting) 725
- latest event
  - displaying 330
- limitation on number of alarms 315
- limitation on number of instances evaluated in alarm 325
- linkage with JP1/AJS3
  - releasing 621
- linkage with JP1/IM
  - releasing 582
- linkage with JP1/SS
  - releasing 631
- linking with JP1/AJS3
  - notes 624
  - operations 623
  - prerequisites 618
  - setup 620
- linking with JP1/AJS3 (multiple monitoring) 540
- linking with JP1/IM
  - setup (settings for displaying reports from events in integrated console) 581
  - setup (settings for using JP1/IM to monitor events that occurred in Performance Management) 568
- linking with JP1/IM (multiple monitoring) 539
- linking with JP1/SLM (multiple monitoring) 540
- linking with JP1/SS
  - Entering information for Item elements 634
  - notes 635
  - prerequisites 627
  - setup 629
  - Viewing Performance Management reports from the JP1/SS interface 634
- link with other systems
  - multiple-monitoring environment 539
- list 168
  - example 168
- load-balancing cluster system 406
- local action 252
- local disk 413
- Log (ITSLM) 128
- log file trap 676
- logging off 48
- logging on 48
- logical host 412

- changing name during operation 449, 497
- LOGIF property 128
- <logif> tag 133
- log information (troubleshooting) 725
- logoff 48
- Log property 127
- Log Records 127
- logs
  - example for JP1/Base log file trapping function 677
  - JP1/Base log file trapping function, starting 678
  - type of log information 725

## M

- managing
  - event data 154
  - operation monitoring data 125
  - performance data 126
  - user accounts 516
- manual bind 244
- mathematical expressions
  - conventions 12
- message
  - alarms 262
- Message label 295
- messages
  - KAVE00105-E 159
  - KAVE00182-E 158
- Message Text label 290
- Message Text sub-subsection 294
- modifying
  - alarm definition 298
- monitored object 564
- monitoring
  - agents 95
  - agent status 106
  - by Agents tree 96
  - by using alarms 279
  - by using integrated console 564
  - by using integrated scope 564
  - for a set value 263
  - linking with JP1/AJS3 615
  - linking with the IT Service Management Product (JP1/Service Support) 625
  - operating status of host running monitoring agent 640
  - operating status of monitoring agent service 640
  - starting by using alarm 282
  - stopping by using alarm 282

- stopping by using alarm (command) 310
- suspending and resuming 337
- Monitoring (ITSLM) 128
- monitoring items for JP1/SLM linkage 603
- monitoring linked with JP1/AJS3
  - overview 616
- monitoring linked with JP1/SS
  - overview 626
- monitoring performance data in JP1/SLM 613
- monitoring suspension
  - automatic synchronization options of the settings information for the monitoring suspension function (for multiple-monitoring) 345
- monitoring suspension function
  - options 345
  - overview 338
  - prerequisites 338
  - setting 345
  - system linkage 340
- monitoring time range 248, 249
- multiple monitoring 526
  - definition information 528
  - features 526
  - setting PFM - Manager for connection destination 540
  - system configuration 533
- multiple-monitoring environment
  - before configuring 533
  - link with other systems 539
- multi-row record 174

## N

- name
  - alarms 262
- network configuration
  - planning 412
- network settings for JP1/SLM linkage 602
- new report
  - creating 170
- New Report window
  - displaying 172
- node that can be modified
  - properties 127
- non stand-alone mode
  - overview 56
- normal status 108
- note

- cluster system 523
- Not Supported 649–651
- number of alarms that can be registered 315
- number of events to be displayed
  - setting 332
- number of records 141

## O

- one-side execution mode 541
- operating alarm
  - using command 304
  - using Web browser 279
- operating statuses
  - checking 646
- operating status of server or agent is Unconfirmed or Not Supported (troubleshooting) 700
- operation
  - cluster system 513
  - planning 414
- operation monitoring
  - linking with Integrated Management Product JP1/IM 562
- operation monitoring data
  - collecting and managing 517
- operation monitoring data (event data)
  - checking 558
- operation monitoring data (performance data)
  - checking 558
- operation monitoring data matches
  - checking 558
- operations
  - linking with JP1/AJS3 623
  - linking with JP1/SS 634
- operation status logs (troubleshooting) 725, 727, 728
- order to start 27
- order to stop 28
- overview
  - cluster system 405
  - monitoring linked with JP1/AJS3 616
  - monitoring linked with JP1/SS 626
  - monitoring suspension function 338

## P

- password 79
  - changing 81
- performance data 126
  - backing up and restoring 394

- checking disk space for 150
- erasing 151
- exporting 149
- modifying for performance data (Store 1.0) 141
- modifying for performance data (Store 2.0) 134
- modifying recording options 126
- partial backups (Store 2.0) 397
- Performance Management
  - benefits of linking with JP1/AJS3 617
  - benefits of linking with JP1/SS 626
  - linking with JP1/IM 565
  - start and stop sequences 27
  - starting and stopping 513
  - user 64
- Performance Management linking with JP1/SS
  - operations 634
- Performance Management report from monitor window of JP1/AJS3 - Web Console
  - displaying 623
- Performance Management reports
  - displaying from monitor window of JP1/AJS3 - Web Console 623
- performance monitoring linked with JP1/Service Level Management (JP1/SLM) 597
- Period (Day) 136
- Period - Day Drawer (Week) 136
- Period - Hour Drawer (Day) 136
- Period - Minute Drawer (Day) 136
- Period - Month Drawer (Month) 136
- Period - Week Drawer (Week) 136
- Period - Year Drawer (Year) 136
- PFM - Agent
  - adding in cluster 443, 491
  - deleting in cluster 447, 495
  - installing upgrade in cluster 483
  - installing upgrade in logical host environment 434
- PFM authentication mode 64
- PFM - Manager
  - control command 476
  - exporting definition information 549
  - importing definition information 551
  - installing and setting up in cluster 417, 466
  - unsetup and uninstallation in cluster 435, 483
- PFM - Manager definition information
  - checking duplication 553
- PFM - Manager to which monitoring agent connects
  - checking settings 557
- PFM - RM
  - adding in cluster 443, 491
  - deleting in cluster 447, 495
  - installing upgrade in cluster 483
  - installing upgrade in logical host environment 434
- PFM - RM group agent 97
- PFM - RM remote agent 97
- PFM service automatic restart functionality 670
- PFM - Web Console
  - exporting definition information 550
  - importing definition information 551
  - installing and setting up in cluster 429, 478
  - logoff 48
  - logon 48
  - starting from JP1/SLM 613
  - unsetup and uninstallation in cluster 441, 489
- PFM - Web Console definition information
  - checking duplication 556
- physical host 413
- PID
  - output by jpc tool service list command 50
- Port
  - output by jpc tool service list command 50
- prerequisite (health check function) 640
- prerequisite program version for multiple monitoring 535
- prerequisites
  - linking with JP1/AJS3 618
  - linking with JP1/SS 627
  - monitoring suspension function 338
- prerequisites for multiple monitoring
  - related to PFM - Manager 535
  - related to PFM - Web Console 535
- primary execution mode 541
- primary Manager 526
  - batch switching 560
  - switching 561
- procedure
  - before setting alarm 252
  - duplicating definition information 548
  - for collecting data in event of trouble 749
  - for recovering from serious failures such as disk failure (troubleshooting) 755
  - setting up multiple monitoring 537
  - switching primary Manager and secondary Manager 559
  - unsetting up multiple monitoring 545

- Product Alarm - PA 154
- <product-detail> tag 148
- Product Interval - Day Drawer 143
- Product Interval - Hour Drawer 143
- Product Interval - Minute Drawer 142
- Product Interval - Month Drawer 143
- <product-interval> tag 147
- Product Interval - Week Drawer 143
- Product Interval - Year Drawer 143
- Product label 289
- <product-log> tag 148
- properties 116
  - alarms 331
  - batch distribution 117
  - description, setting, and node that can be modified 127
  - displaying agent properties 116
  - displaying alarm properties (definition) 285
  - editing agent properties 117
  - of bookmarks 195

## Q

- Quick Guide
  - creating reports 185
  - default values for reports 186

## R

- rc.jp1\_pc 33
- rc.jp1\_webcon 37
- rc.shutdown 43, 45
- realtime (single agent) 173
- realtime monitoring by alarm
  - cluster system 518
- realtime report 166
- rearranging
  - graphs (tiling display) 197
- reconfiguring PFM - Manager for connection destination
  - release multiple monitoring 547
- recording options 126
  - modifying for performance data 126
- recording performance data collected when linked with JP1/SLM 601
- records
  - changing max. num. for event data 154
- <record> tag 132
- record type 135

- refresh interval 53, 176
- registered report
  - tiling 195
- registering
  - baseline in combination bookmark 215
- related to PFM - Manager
  - prerequisites for multiple monitoring 535
- related to PFM - Web Console
  - prerequisites for multiple monitoring 535
- releasing
  - linkage with JP1/AJS3 621
  - linkage with JP1/SS 631
- releasing linkage with JP1/SLM 606
  - procedures 607
- releasing links with JP1/IM (multiple monitoring) 546
- releasing links with JP1/SLM (multiple monitoring) 546
- remote action 252
- remote actions
  - controlling 541
- renaming
  - bookmark 193
  - bookmark folder 193
  - folders and bookmarks 193
  - report folder 182
  - reports 182
- report cache files 231
- report cache filing function 231
- report creation
  - procedure 170
  - process flow 170
- report folder
  - deleting 183
  - renaming 182
- report-level drilldown report 179
- report properties
  - checking 203
- reports 166
  - associating with alarm 270
  - associating with another (drilldown) 179
  - combination reports, displaying 216
  - combination reports, display preparation 215
  - copying 180
  - creating, by using command 188
  - creating bookmarks 190
  - creating in cluster system 517
  - creating in Web browser (Quick Guide) 185
  - creating in Web browser (Reports tree) 172

- creating report folder 172
- creating with Quick Guide 185
- default values for Quick Guide 186
- deleting 183, 194
- deleting from bookmark 195
- deleting if unnecessary 189
- display format 167
- displaying 199
- displaying those associated with alarm 331
- editing 180
- exporting 183
- exporting in CSV or HTML by browser 223
- exporting in CSV or HTML by command 224
- general comments 166
- importing 184
- notes on creation 229
- notes on displaying 229
- output and customize 188
- renaming 182
- searching for fields 174
- setting display conditions 203
- setting display conditions for fields 175
- setting display format 177
- setting fields displayed in 174
- setting name and type 172
- types of 166
- report series paging 199, 234
  - cautionary notes 195, 234
- report type 173
- restoring 349
  - cluster system 518
  - event data 392
  - performance data 394
- restoring system (troubleshooting) 755
- resuming
  - monitoring 337
- resuming monitoring
  - range of monitoring suspended or resumed by agent 343
  - range of monitoring suspended or resumed by host 342
  - rang of suspending or resuming monitoring 342
  - resuming monitoring from Web browser 347
- retention conditions 141
  - modifying for performance data (Store 1.0) 141
  - modifying for performance data (Store 2.0) 134
- retention period 141, 157

- Running 648, 650, 651

## S

- saving of record to be evaluated in alarm 315
- scheduled restart functionality 670
- script file for starting services automatically (jpc\_start) 31
- script file for starting services automatically (jpcw\_start) 36
- script file for stopping services automatically (jpc\_stop) 42, 44
- searching for
  - field 265
- secondary Manager 526
  - batch switching 560
  - switching 561
- selection of authority 80
- sequential file (troubleshooting) 728
- series group 216
- ServiceID
  - output by jpc tool service list command 50
- Service Name
  - output by jpc tool service list command 50
- services
  - how to check status 665
  - starting 30
  - status, checking from web browser 51
  - stopping 40
- setting
  - display condition for event monitor window 332
  - display format of combination report 216
  - monitoring suspension function 345
  - number of events to be displayed 332
  - PFM - RM polling 643
  - prior to setting associated report 270
  - report name and type 172
- setting alarm
  - using command 287
- setting function
  - for measurement value output at alarm recovery 254
- setting PFM - Manager for connection destination
  - multiple monitoring 540
- setting up multiple monitoring
  - procedure 537
- setup
  - for JP1/SLM linkage 605
- shared disk 413

- single-row record 174
- SNMP trap 268
- stand-alone mode
  - overview 54
- standby node 405
- starting
  - JP1/Base log file trapping function 678
  - monitoring by using alarm 282, 311
  - monitoring from JP1/SLM 613
  - PFM - Web Console from JP1/SLM 613
  - sequence for Performance Management system 27
  - services 30
  - synchronizing PFM Manager, Base, Web Console 46
- starting and stopping
  - cautionary notes 54
  - Performance Management 513
- status
  - alarms 108
  - indicated by agent icon 107
  - indicated by folder icon 106
- Status
  - output by jpc tool service list command 51
- status management function 663
  - troubleshooting 668
- status of service, checking 50
- status of service, checking by command 50
- Stopped 648
- stopping
  - monitoring by alarm (command) 310
  - monitoring by using alarm 282
  - monitoring from JP1/SLM 613
  - sequence for Performance Management system 27
  - services 40
  - synchronizing PFM Manager, Base, Web Console 46
- Store database
  - reorganizing 162
  - size limits 157
- Store database storage method 392
- summary display 109
  - counting unit and range 114
  - printing 116
  - supported agent types 110
  - use to check operating status 109
- Suspended 647–651
- suspending
  - monitoring 337
- suspending monitoring
  - range of monitoring suspended or resumed by agent 343
  - range of monitoring suspended or resumed by host 342
  - range of suspending or resuming monitoring 342
  - suspending monitoring from Web browser 346
- Switch Alarm Level label 295
- switching
  - primary Manager 561
  - secondary Manager 561
- switching primary Manager and secondary Manager
  - procedure 559
- symbol conventions 11
- Sync Collection With property 128
- synchronizing monitoring settings after backing up or restoring PFM - Manager or JP1/SLM 614
- synchronizing service starting and stopping
  - PFM - Manager or PFM - Base and PFM - Web Console 46
- syslog file (troubleshooting) 725
- system configuration
  - multiple monitoring 533
- system log (troubleshooting) 725
- system user 64
- system users
  - available functions 66

## T

- table 167
  - alarms 242
  - example 168
- table name
  - alarms 261
- tiling
  - registered report 195
- tiling display 195
- time
  - for evaluating alarm 315
- timing of reporting alarm 247, 248
- trace logs (troubleshooting) 726, 732
- troubleshooting 681
  - agent management 700
  - alarm definition 704
  - collecting and managing performance data 707
  - detecting problems by linking with integrated system monitoring product 676
  - executing commands 699
  - logon 697

- monitoring suspension function 713
- report definition 702
- setup and service startup 683

## U

- unbind alarm table 307
- unbinding 279
  - alarm table bound to monitoring agent 306
- Unconfirmed 648–651
- unsetting up multiple monitoring
  - procedure 545
- URL to log on to PFM - Web Console 48
- user accounts 64
  - authentication mode 78
  - copying and customizing 80
  - creating for Performance Management 79
  - deleting 83
  - editing 81
  - management method 64
  - managing 516
  - setting authentication mode 78
- user name 79

## V

- version changes 759
- version number conventions 12

## W

- warning status 108
- Web browser
  - operating alarm by using 279
- while monitoring is suspended
  - alarms 339
  - health check 339
  - operating information 340
- wrap-around file (troubleshooting) 728

## X

- XML declaration 131, 146

---

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan

---