HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/Performance Management - Remote Monitor for Platform Description, User's Guide and Reference

3021-3-350-10(E)

Notices

■ Relevant program products

Job Management Partner 1/Performance Management - Manager (for Windows):

P-2W2C-AAAL Job Management Partner 1/Performance Management - Manager 10-50

The above product includes the following:

P-CC242C-AAAL Job Management Partner 1/Performance Management - Manager 10-50 (for Windows Server 2003)

P-CC2A2C-AAAL Job Management Partner 1/Performance Management - Manager 10-50 (for Windows Server 2008, Windows Server 2012)

Job Management Partner 1/Performance Management - Manager (for UNIX):

P-812C-AAAL Job Management Partner 1/Performance Management - Manager 10-50 (for Linux 5 (x86), Linux 5 (x64), Linux 5 Advanced Platform (x86), Linux 5 Advanced Platform (x64), Linux 6 (x86), Linux 6 (x64))

P-9D2C-AAAL Job Management Partner 1/Performance Management - Manager 10-50 (for Solaris 10 (SPARC))

P-1M2C-AAAL Job Management Partner 1/Performance Management - Manager 10-50 (for AIX V6.1, AIX V7.1)

Job Management Partner 1/Performance Management - Base (for Windows):

P-2W2C-AJAL Job Management Partner 1/Performance Management - Base 10-50

The above product includes the following:

P-CC242C-AJAL Job Management Partner 1/Performance Management - Base 10-50 (for Windows Server 2003)

P-CC2A2C-AJAL Job Management Partner 1/Performance Management - Base 10-50 (for Windows Server 2008, Windows Server 2012)

Job Management Partner 1/Performance Management - Base (for UNIX):

P-812C-AJAL Job Management Partner 1/Performance Management - Base 10-50 (for Linux 5 (x86), Linux 5 (x64), Linux 5 Advanced Platform (x86), Linux 5 Advanced Platform (x64), Linux 6 (x86), Linux 6 (x64))

Job Management Partner 1/Performance Management - Web Console (for Windows):

P-2W2C-ARAL Job Management Partner 1/Performance Management - Web Console 10-50

The above product includes the following:

P-CC242C-ARAL Job Management Partner 1/Performance Management - Web Console 10-50 (for Windows Server 2003)

P-CC2A2C-ARAL Job Management Partner 1/Performance Management - Web Console 10-50 (for Windows Server 2008, Windows Server 2012)

Job Management Partner 1/Performance Management - Web Console (for UNIX):

P-812C-ARAL Job Management Partner 1/Performance Management - Web Console 10-50 (for Linux 5 (x86), Linux 5 (x64), Linux 5 Advanced Platform (x86), Linux 5 Advanced Platform (x64), Linux 6 (x86), Linux 6 (x64))

Job Management Partner 1/Performance Management - Remote Monitor for Platform (for Windows):

P-2W2C-GCAL Job Management Partner 1/Performance Management - Remote Monitor for Platform 10-50

The above product includes the following:

P-CC242C-GCAL Job Management Partner 1/Performance Management - Remote Monitor for Platform 10-50 (for Windows Server 2003)

P-CC2A2C-GCAL Job Management Partner 1/Performance Management - Remote Monitor for Platform 10-50 (for Windows Server 2008, Windows Server 2012)

Job Management Partner 1/Performance Management - Remote Monitor for Platform (for UNIX):

P-812C-GCAL Job Management Partner 1/Performance Management - Remote Monitor for Platform 10-50 (for Linux 5 (x86), Linux 5 (x64), Linux 5 Advanced Platform (x86), Linux 5 Advanced Platform (x64), Linux 6 (x86), Linux 6 (x64))

These products include parts that were developed under licenses received from third parties.

■ Trademarks

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

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

HP-UX is a product name of Hewlett-Packard Development Company, L.P. in the U.S. and other countries.

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.

Itanium is a trademark of Intel Corporation in the United States and 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.

Microsoft and Visual C++ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft and Visual Studio 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.

RPM is an abbreviation of RPM Package Manager.

RSA is either a registered trademark or a trademark of EMC Corporation in the United States and/or 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.

SUSE is a registered trademark or a trademark of SUSE LLC in the United States and other countries.

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

Win32 is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or 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.

The following program products contain some parts whose copyrights are reserved by Oracle, its subsidiaries, or affiliates: P-9D2C-AAAL and P-9D2C-ARAL.

The following program products contain some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D2C-AAAL and P-9D2C-ARAL.

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

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, 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
Win32		Win32(R)
Windows Server 2003	Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
		Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows Server 2003 (x86)	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition
		Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard Edition

Abbreviation		Full name or meaning
Windows Server 2008	Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
		Microsoft(R) Windows Server(R) 2008 Standard
	Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard

Windows Server 2003, Windows Server 2008, and Windows Server 2012 are sometimes referred to collectively as *Windows*.

■ Issued

Dec. 2014: 3021-3-350-10(E)

■ Copyright

All Rights Reserved. Copyright (C) 2013, 2014, Hitachi, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-350-10(E)) and product changes# related to this manual.

Changes	Location
The following OSs are now supported: • Linux 5 (x64) • Linux 5 Advanced Platform (x64)	--
The timing of performance data collection by the collection process was changed.	*2.1.1(2)*
The following OSs are now supported as monitoring targets: • CentOS 6 (x64) • CentOS 6 (x86) • Oracle Linux 6 (x64) • Oracle Linux 6 (x86) • Solaris 11 (SPARC) • SuSE Linux 11 (x64) • SuSE Linux 11 (x86)	*3.1.1(6)*, *N.2*
The common account information function is now supported.	*3.1.4(2)*, *3.1.4(3)*, *3.1.5(5)*, *3.1.6(3)*, *3.1.6(4)*, *3.2.4(4)*, *3.2.5(3)*, *3.6.2(1)*, *3.6.3(1)*, *3.6.3(2)*, *9.2.1(6)*, *9.2.5(3)*, *E.2*, *E.3*, *Glossary*
The unit used in the formula for estimating the agent log size was changed from kilobytes to megabytes.	Table 3-20, Table 3-34
Information about the number of agent log files that can be collected per instance was added.	Table 3-20
`Over 10 Sec Collection Time` was added as a property related to performance data collection conditions for each record.	*Chapter 7*, *E.2*, *E.3*
The following messages were added: `KAVL17028-E`, `KAVL17029-W` to `KAVL17033-W`, `KAVL17034-E`, `KAVL17035-W`, `KAVL17036-W`	*8.2*, *8.3*, *8.4*
The following messages were changed: `KAVL17005-E`, `KAVL17017-W`, `KAVL17022-W`, `KAVL17023-W`, `KAVL17026-W`	*8.4*
The following files were added to agent logs: • `collect_core_`*nn* • `timer_core_`*nn*	Table 9-9, *F.1*
The agent log output method was changed from the wrap-around method to a sequential method.	Table 9-9, Table 9-10
A formula for estimating the amount of disk space used by agent logs per instance was added.	Table 9-9, Table 9-10
The following properties for multiple monitoring were added: • `Primary Manager` • `Secondary Manager`	*E.1*, *E.2*

Changes	Location
`Realtime Report Data Collection Mode` was added as a property that is used when historical data collection takes priority over real-time report display processing.	*E.3*
The following files were added: • `suspended.dat` • *monitoring target name*`_suspended.dat`	*F.1*, *F.2*

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

#

Includes the functions that were added between version 10-00 and version 10-50.

Preface

This manual describes the functions of JP1/Performance Management - Remote Monitor for Platform and the records that are collected by it.

In this manual, Job Management Partner 1 is abbreviated to *JP1*.

■ Intended readers

This manual describes JP1/Performance Management - Remote Monitor for Platform. The manual is intended for the following readers:

- Users who are interested in designing or building an operation monitoring system
- Users who are interested in defining conditions for collecting performance data
- Users who are interested in defining reports and alarms
- Users who are interested in referencing performance data that is collected for the purpose of monitoring a system
- Users who are interested in developing and evaluating corrective measures to take for a system based on monitoring results, or users who are interested in directing the implementation of such measures

This manual assumes that the reader is knowledgeable about the operation of the monitored systems and is familiar with their operating systems.

For details about setting up and operating a system that uses JP1/Performance Management, also see the following manuals:

- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management Planning and Configuration Guide* (3021-3-347(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management User's Guide* (3021-3-348(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management Reference* (3021-3-349(E))

■ Organization of this manual

This manual is organized into the following parts.

This manual is applicable to both Windows and UNIX operating systems (OSs). Any information specific to one of the OSs only is indicated as such in the manual.

PART 1: Overview

PART 1 provides an overview of JP1/Performance Management - Remote Monitor for Platform.

PART 2: Setup and Operation

PART 2 explains how to install and set up JP1/Performance Management - Remote Monitor for Platform, as well as how to uninstall and unsetup JP1/Performance Management - Remote Monitor for Platform. It also explains how to back up and restore files, how to collect process operating status information, and how to operate JP1/Performance Management - Remote Monitor for Platform in a cluster system.

PART 3: Reference

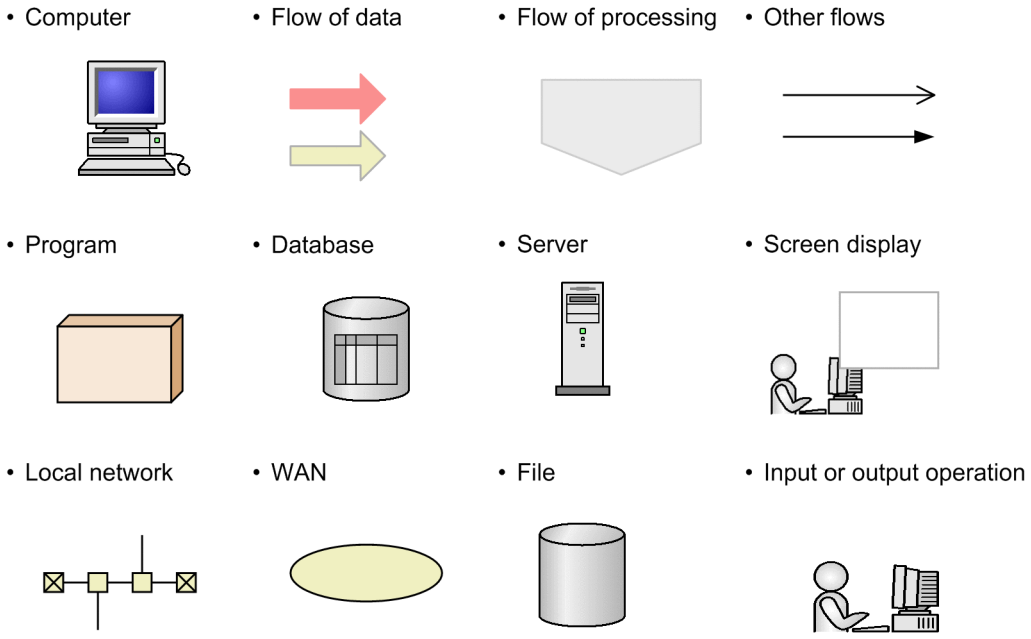
PART 3 describes the monitoring templates, records, and messages for JP1/Performance Management - Remote Monitor for Platform.

PART 4: Troubleshooting

PART 4 describes the procedures for handling problems in JP1/Performance Management - Remote Monitor for Platform.

■ Conventions: Diagrams

This manual uses the following conventions in diagrams:



■ Conventions: Fonts and symbols

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

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.

Text formatting	Convention
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

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

Conventions 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 6
Preface 8

Part 1: Overview

1 Overview of PFM - RM for Platform 19
1.1 Purposes of performance monitoring using PFM - RM for Platform 20
1.1.1 Finding the causes of system overload and identifying its effects on the system resources 20
1.1.2 Monitoring to see if the system is running normally 21
1.2 Features of PFM - RM for Platform 22
1.2.1 Monitoring multiple hosts remotely 22
1.2.2 Collecting performance data by attribute 24
1.2.3 Storing performance data 24
1.2.4 Using collected performance data effectively 24
1.2.5 Integrating monitoring and analysis of performance data for multiple monitored hosts 26
1.2.6 Easy setting of alarms and reports 27
1.2.7 Applicable to cluster systems 27

2 Functions of PFM - RM for Platform 29
2.1 Collecting and managing performance data 30
2.1.1 Flow of performance data collection 30
2.2 How to monitor performance 33
2.2.1 Example of monitoring a processor 33
2.2.2 Example of monitoring memory 38
2.2.3 Example of monitoring the disk 41
2.2.4 Example of monitoring the network 43
2.2.5 Example of monitoring processes and services 45

Part 2: Setup and Operation

3 Installation and Setup 49
3.1 Installation and setup of the Windows edition 50
3.1.1 Issues to consider before installing the Windows edition 50
3.1.2 Flow of installation and setup for the Windows edition 68
3.1.3 Installation procedure for the Windows edition 70
3.1.4 Setup procedure for the Windows edition 72

3.1.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows) 94
3.1.6 SSH connection setting method for Windows (when the PFM - RM host is running Windows and the monitored host is running UNIX) 100
3.1.7 Notes about installation and setup of the Windows edition 106
3.2 Installation and setup of the UNIX edition 109
3.2.1 Issues to consider before installing the UNIX edition 109
3.2.2 Flow of installation and setup for the UNIX edition 115
3.2.3 Installation procedure for the UNIX edition 117
3.2.4 Setup procedure for the UNIX edition 119
3.2.5 SSH (for UNIX) connection setting method 133
3.2.6 Notes about installation and setup of the UNIX edition 141
3.3 Uninstallation and unsetup of the Windows edition 143
3.3.1 Issues to consider before uninstalling and canceling the setup for the Windows edition 143
3.3.2 Procedure for canceling the setup for the Windows edition 144
3.3.3 Procedure for uninstalling the Windows edition 146
3.4 Uninstallation and unsetup of the UNIX edition 148
3.4.1 Issues to consider before uninstalling and canceling the setup for the UNIX edition 148
3.4.2 Procedure for canceling the setup for the UNIX edition 148
3.4.3 Procedure for uninstalling the UNIX edition 151
3.5 Changing the PFM - RM for Platform system configuration 153
3.6 Changing the PFM - RM for Platform operation method 154
3.6.1 Changing performance data storage locations 154
3.6.2 Updating an instance environment 155
3.6.3 Updating a monitoring target 159
3.7 Backing up and restoring PFM - RM for Platform 164
3.7.1 Backing up 164
3.7.2 Restoring 165
3.8 Settings for using a Web browser to reference manuals 166
3.8.1 Setup for referencing manuals 166
3.8.2 How to view manuals 167

4 Collecting Process Operation Status Information 168
4.1 Setup for collecting process operation status information 169
4.1.1 Setup using the Agents tree 169
4.1.2 Setting up monitoring targets in the Agents tree 169
4.1.3 Deleting monitoring target settings in Agents tree 176
4.1.4 Using an application definition template in the Agents tree 176
4.1.5 Setting up collection in Services 180
4.1.6 Setting up a monitoring target in Services 180
4.1.7 Checking or modifying the settings for monitoring targets in Services 185
4.1.8 Deleting the settings for monitoring targets in Services 185

4.1.9 Setup using non-interactive commands 186
4.1.10 Using commands to set up monitoring targets 186
4.1.11 Using commands to delete settings for a monitoring target 188
4.1.12 Specifying whether process or service names to be used as monitoring targets will be case-sensitive 190
4.2 Example of the procedure to follow when an alarm is issued during the collection of process operation status information 192

5 Operation in a Cluster System 194
5.1 Configuration of PFM - RM for Platform in a cluster system 195
5.2 Processing when a failover occurs 197
5.2.1 Failover when an error occurs at the PFM - RM host 197
5.2.2 Effects of PFM - Manager shutdown and the action to take 198
5.3 Installation and setup in a cluster system (for Windows) 200
5.3.1 Items to be checked before installing in a cluster system (for Windows) 200
5.3.2 Flow of installation and setup in a cluster system (for Windows) 204
5.3.3 Installation procedure in a cluster system (for Windows) 205
5.3.4 Setup procedure in a cluster system (for Windows) 205
5.3.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows) in a cluster system 212
5.3.6 SSH connection setting method in a cluster system (when the PFM - RM host is running Windows and the monitored host is running UNIX) (for Windows) 212
5.4 Installation and setup in a cluster system (for UNIX) 213
5.4.1 Items to be checked before installing in a cluster system (for UNIX) 213
5.4.2 Flow of installation and setup in a cluster system (for UNIX) 216
5.4.3 Installation procedure in a cluster system (for UNIX) 218
5.4.4 Setup procedure in a cluster system (for UNIX) 218
5.4.5 SSH connection setting method in a cluster system (for UNIX) 225
5.5 Uninstallation and unsetup in a cluster system (for Windows) 226
5.5.1 Flow of uninstallation and unsetup in a cluster system (for Windows) 226
5.5.2 Unsetup procedure in a cluster system (for Windows) 227
5.5.3 Uninstallation procedure in a cluster system (for Windows) 231
5.6 Uninstallation and unsetup in a cluster system (for UNIX) 232
5.6.1 Flow of uninstallation and unsetup in a cluster system (for UNIX) 232
5.6.2 Unsetup procedure in a cluster system (for UNIX) 233
5.6.3 Uninstallation procedure in a cluster system (for UNIX) 238
5.7 Changing the PFM - RM for Platform system configuration 239
5.8 Changing the PFM - RM for Platform operation method in a cluster system 240
5.8.1 Updating an instance environment in a cluster system 240
5.8.2 Updating a monitoring target in a cluster system 241
5.8.3 Importing and exporting the logical host environment definition file in a cluster system 242

Part 3: Reference

6 Monitoring Template 244

Overview of the monitoring template 245
Format of alarm explanations 246
Alarm table 247
Application Status 250
Available Memory 251
CPU Usage 252
Disk Busy % 253
Disk Free Size 254
Disk Service Time 255
Disk Space 256
I/O Wait Time 257
Kernel CPU 258
Network Received 259
Page Faults 260
Pagescans 261
Process Existence 262
Processor Queue 264
Run Queue 265
Service Stop 266
Service Stop(dsp nm) 268
Swap Outs 270
Target Host Status 271
Used Swap Mbytes 272
User CPU 273
Format of report explanations 274
Organization of report directories 275
List of reports 277
Application Process Count (historical report indicating the operation status of each process and service of an application) 279
Application Process Status (real-time report indicating the operation status of each process and service of an application) 280
Application Status (real-time report indicating the operation status of an application) 281
Avg Disk Time Status (real-time report indicating the average I/O time for the physical disk) 282
Avg Disk Time Status (historical report indicating the average I/O time for the physical disk) 283
CPU Per Processor Status (real-time report indicating the processor usage rate for each processor) 284
CPU Used Status (real-time report indicating the CPU usage status) 285
CPU Used Status (historical report indicating the CPU usage status (1 month)) 287
CPU Used Status (historical report indicating the CPU usage status (1 hour)) 288
CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 month)) 289
CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 day)) 290
Free Megabytes - Logical Disk (real-time report indicating the available area on the logical disk) 291
Free Megabytes - Logical Disk (historical report indicating the available area on the logical disk) 292

Memory Paging Status (real-time report indicating information about memory and paging) 293
Memory Paging Status (historical report indicating information about memory and paging (1 day)) 295
Memory Paging Status (historical report indicating information about memory and paging (1 hour)) 297
Memory Used Status (real-time report indicating the physical memory usage status in the system) 299
Memory Used Status (historical report indicating the physical memory usage status in the system (1 day)) 301
Memory Used Status (historical report indicating the physical memory usage status in the system (1 hour)) 303
Memory Used Status (Multi-Agent) (historical report indicating the physical memory usage status in multiple systems (1 month)) 305
Memory Used Status (Multi-Agent) (historical report indicating the physical memory usage status in multiple systems (1 day)) 306
Network Data (real-time report indicating the status of communication between networks) 307
Network Data (historical report indicating the status of communication between networks) 308
Physical Disk Busy Status (real-time report indicating the length of time the disk was busy) 309
Physical Disk Busy Status (historical report indicating the length of time the disk was busy) 310
Pool Nonpaged Status (real-time report indicating the size of physical memory in the system that cannot be paged out) 311
Pool Nonpaged Status (historical report indicating the size of physical memory in the system that cannot be paged out) 313
System Overview (real-time report indicating the system operation status) 315
System Overview (historical report indicating the system operation status) 317
Target Host Status (historical report indicating the status of the connection to the monitored host and information about the OS of the monitored host) 319

7 **Records 321**

Data model 322
Format of record explanations 323
List of ODBC key fields 326
Summarization rules 327
Grouping rules 329
List of data types 330
Field values 331
Fields that are added only when a record is recorded in the Store database 333
Notes on records 335
List of records 338
Application Process Count (PD_APPC) 339
Application Process Detail (PD_APPD) 341
Application Process Overview (PD_APS) 343
Application Service Overview (PD_ASVC) 346
Application Summary (PD_APP2) 349
Logical Disk Overview (PI_LDSK) 352
Network Interface Overview (PI_NET) 355
Physical Disk Overview (PI_PDSK) 357
Processor Overview (PI_CPU) 360
System Status (PD) 363
System Summary (PI) 366

8 Messages 372

8.1 Message format 373
8.1.1 Format of output messages 373
8.1.2 Format of message explanations 374
8.2 Message output destinations 376
8.3 List of messages output to the Windows event log and syslog 379
8.4 Messages 380

Part 4: Troubleshooting

9 Error Handling Procedures 392

9.1 Error handling procedures 393
9.2 Troubleshooting 394
9.2.1 Troubleshooting problems with setting up or starting a service 394
9.2.2 Troubleshooting problems with command execution 398
9.2.3 Troubleshooting problems with report definitions 399
9.2.4 Troubleshooting problems with alarm definitions 399
9.2.5 Troubleshooting problems with collection and management of performance data 400
9.2.6 Troubleshooting other problems 406
9.3 Log information to be collected for troubleshooting 407
9.3.1 Types of log information to be collected 407
9.3.2 Log files and directories to check 408
9.4 Data to be collected for troubleshooting 414
9.4.1 Data to be collected from a Windows environment 414
9.4.2 Data to be collected from a UNIX environment 418
9.5 How to collect data for troubleshooting 421
9.5.1 How to collect data in a Windows environment 421
9.5.2 How to collect data in a UNIX environment 423
9.6 Detecting problems within Performance Management 426
9.7 Recovering from Performance Management system errors 427

Appendixes 428

A Estimating System Requirements 429
A.1 Memory requirements 429
A.2 Disk space requirements 429
B List of Identifiers 430
C List of Processes 431
C.1 List of Processes (for Windows) 431
C.2 List of processes (for UNIX) 431
D List of Port Numbers 433
D.1 Port numbers for PFM - RM for Platform 433
D.2 Firewall passage directions 433

E Properties of PFM - RM for Platform 437
E.1 List of properties of the Remote Monitor Store service 437
E.2 List of properties of the Remote Monitor Collector service 441
E.3 List of properties of remote agents and group agents 453
F List of Directories and Files 463
F.1 List of folders and files (for Windows) 463
F.2 List of directories and files (for UNIX) 468
G Migration Procedure and Notes on Migration 474
H Version Compatibility 475
I Outputting Action Log Data 476
I.1 Types of events that are output to action logs 476
I.2 Storage format of action logs 476
I.3 Output format of action logs 477
I.4 Action log output settings 482
J Data Sources of Records 485
J.1 Data sources of records (when the monitored host is running Windows) 485
J.2 Data sources of records (when the monitored host is running UNIX) 497
K Linkage to JP1/ITSLM 510
L Communication in IPv4 and IPv6 Environments 511
M Version Changes 512
M.1 Changes in 10-50 512
M.2 Changes in 10-00 513
N Reference Material for This Manual 517
N.1 Related publications 517
N.2 Conventions: Abbreviations for product names 517
N.3 Conventions: Acronyms 519
N.4 Notation for product names, service IDs, and service keys in this manual 520
N.5 Meaning of "folder" and "directory" 521
N.6 Notation for folder path names in this manual 521
N.7 NNM products supported by Performance Management 521
N.8 Conventions: KB, MB, GB, and TB 522
O Glossary 523

Index 531

1 Overview of PFM - RM for Platform

This chapter provides an overview of PFM - RM for Platform.

1.1 Purposes of performance monitoring using PFM - RM for Platform

This section describes the purposes of using PFM - RM for Platform to monitor performance.

PFM - RM for Platform remotely monitors the performance of application servers. Performance monitoring is indispensable for maintaining stable system operations.

Specifically, performance monitoring involves the following tasks:

- Finding the causes of system overloading and identifying the effects of overloading on the system resources
- Monitoring the system to see whether it is running normally

By installing PFM - RM for Platform and monitoring your system's performance, you can identify the causes of system overloads and identify their effects on the system resources.

To use PFM - RM for Platform, you need PFM - Manager, PFM - Base, and PFM - Web Console. However, if you install PFM - RM for Platform on the same host as for PFM - Manager, there is no need to install PFM - Base.

1.1.1 Finding the causes of system overload and identifying its effects on the system resources

If the system load is high for specific reasons, you must restore the system to its normal status in order to minimize adverse effects on the entire system. Therefore, finding the causes of system overloads and identifying their effects on the system resources are important tasks for maintaining stable system operation.

If a performance problem arises, resulting in high system loading, possible causes are as follows:

- There is a memory shortage.
- A program is monopolizing use of specific resources.
- A subsystem has failed or is configured incorrectly.
- There is fluctuation in loading among subsystems.

Obtaining the statuses of the following system resources will assist in correcting these causes:

- Processor
- Memory
- Disk
- Network

PFM - RM for Platform can identify the system resources that are linked to the causes of system overloads by changing various conditions of performance monitoring (such as the number of users that are connected concurrently) and monitoring performance continuously.

Identifying the status of system resources is also useful for evaluating future system operation, such as when you change or adjust the system configuration or when you plan to upgrade the system's resources.

1.1.2 Monitoring to see if the system is running normally

To maintain stable system operation, it is important not only to correct the causes of system overloads but also to check routinely to see if the system is running normally.

You can check whether the system is running normally by monitoring the following operations:

- System-provided processes
- Invalid system processes
- Services required by the system

1.2 Features of PFM - RM for Platform

The following are the principal features of PFM - RM for Platform:

- Monitors multiple hosts remotely
- Collects and manages performance data by attribute
- Stores performance data
- Uses the collected performance data effectively
- Integrates monitoring and analysis of performance data for multiple monitored hosts
- Easy setting of alarms and reportsIs applicable to cluster systems

The subsections below describe these features.

1.2.1 Monitoring multiple hosts remotely

PFM - RM for Platform can be used to monitor performance remotely.

Remote monitoring is a function for monitoring the operation status of remote servers from a local host without having to install an agent at each application server.

This function enables you to monitor performance data without having to change the system configuration of the monitored application servers (hosts), because there is no need to install PFM - RM for Platform at the application servers. A single PFM - RM for Platform can collect and manage performance data for multiple hosts, and multiple instances of PFM - RM for Platform can collect and manage performance data for the same host.

In Performance Management, a host that is monitored by PFM - RM for Platform is called a *monitored host*.

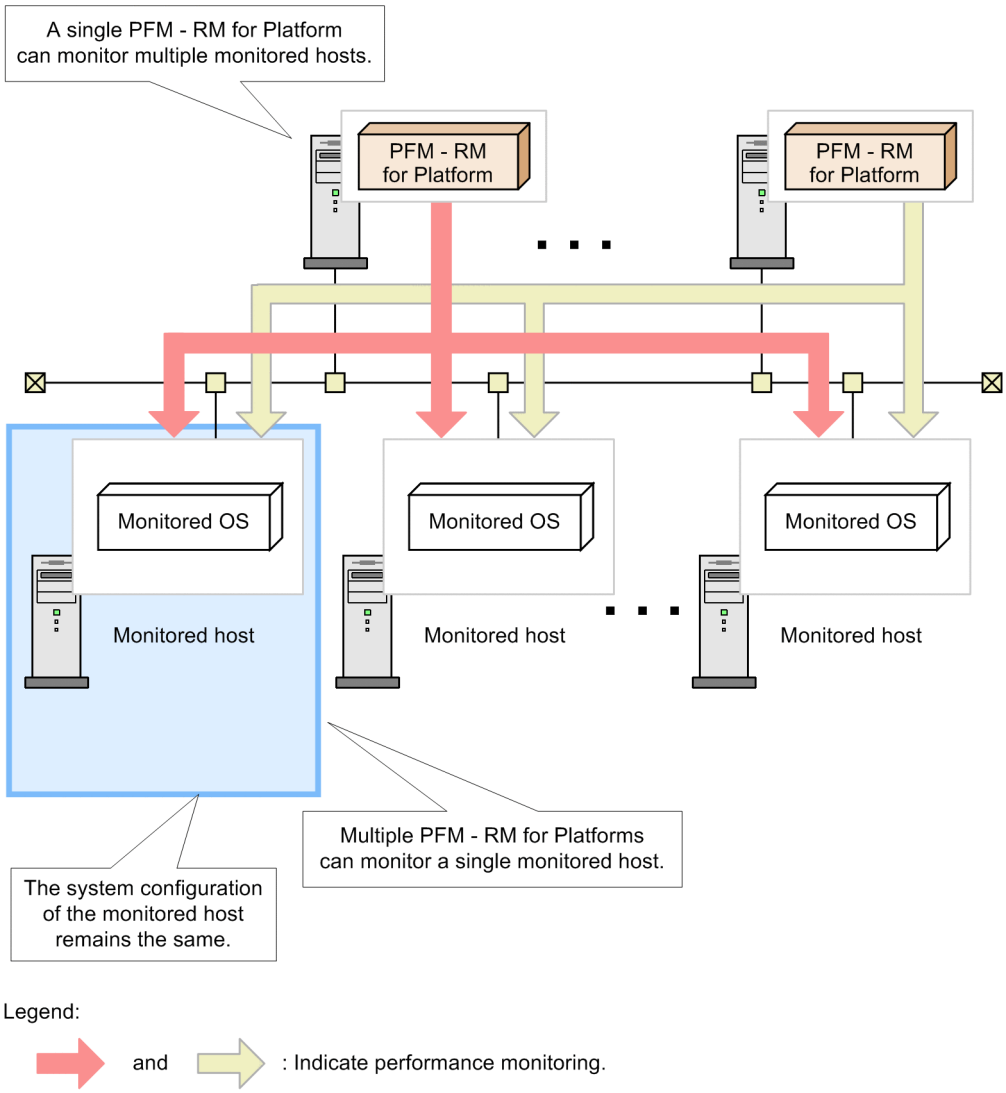
PFM - RM for Platform running in a Windows environment can remotely monitor hosts running in a Windows or UNIX environment. However, PFM - RM for Platform running in a UNIX environment can remotely monitor hosts running in a UNIX environment only.

For details about the OS environments in which PFM - RM for Platform supports monitoring, see *3.1.1 Issues to consider before installing the Windows edition* or *3.2.1 Issues to consider before installing the UNIX edition*.

You can also make the host on which PFM - RM for Platform is running the monitored host.

The following figure illustrates monitoring of multiple monitored hosts by multiple instances of PFM - RM for Platform.

Figure 1–1: Monitoring by PFM - RM for Platform



Legend:

and : Indicate performance monitoring.

(1) Common account information that enables multiple instance environments and monitoring targets to be centrally managed

PFM - RM for Platform uses the account information set up on the PFM - RM host to connect to monitoring targets remotely. Account information used by PFM - RM for Platform is classified into two types. The first is account information that is managed separately for each instance environment or monitoring target. The second is account information that is common to multiple instance environments and monitoring targets. Centrally managing common account information is more efficient. For example, when changing the passwords for instance environments and monitoring targets, you only need to change the common account information that is centrally managed.

Account information used by PFM - RM for Platform (individual account information and common account information)

Remote connection by PFM - RM for Platform needs account information for instance environments (for Windows) and for monitoring targets within the instance environments.

To use individual account information, set up account information separately for each instance environment and for each monitoring target.

To use common account information, set up account information common to all instance environments and monitoring targets (for Windows and UNIX). You can specify whether to use common account information when setting up an instance environment or monitoring target.

Important note

As common account information is used for all monitoring targets, there is a risk of greater negative impact if it is leaked. To avoid such a risk, determine whether to use common account information after considering security measures and information management.

1.2.2 Collecting performance data by attribute

In PFM - RM for Platform, performance data is collected in a format called *records*. A record is a unit for storing collected performance data in a database.

The types of performance data that can be collected have already been defined in PFM - RM for Platform. You use PFM - Web Console to select the records you wish to have collected. For details about how to use PFM - Web Console to select the records to be collected, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

Records are classified into two types, according to the characteristics of the performance data to be collected.

- Product Interval record type

  For records of the Product Interval record type, the system collects performance data for a specified interval, such as the CPU usage rate over 5 minutes. You can use these records to analyze changes or trends in the system status over time.

  The Product Interval record type is referred to hereafter as the *PI record type*.

- Product Detail record type

  For records of the Product Detail record type, the system collects performance data that indicates the system status at a specific point in time, such as detailed information about a host that is currently being monitored. You can use these records to obtain a snapshot of the system status at a particular time.

  The Product Detail record type is referred to hereafter as the *PD record type*.

Each record is further divided into smaller units called *fields*. In Performance Management, records and fields are referred to collectively as a *data model*. For details about each record, see *7. Records*.

1.2.3 Storing performance data

Collected performance data is stored in PFM - RM for Platform's database in the format of records. This database is called the *Store database*. You can use the performance data stored in the Store database to analyze trends in the operation status of the monitored hosts over time, such as from a point in the past up to the current time.

You use PFM - Web Console to set how performance data stored in the Store database is to be managed. For details about using PFM - Web Console to manage performance data, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

1.2.4 Using collected performance data effectively

PFM - RM for Platform enables you to use the performance data collected from monitored hosts effectively, such as for analyzing and identifying trends and the host's operation status.

(1) Graphically displaying the operation status at monitored hosts

By using PFM - Web Console, you can process and display in a graphical format various types of performance data collected by PFM - RM for Platform, such as the CPU usage rate. Because this feature enables you to check trends and changes in collected and summarized performance data graphically, you can easily analyze the operation status of multiple hosts.

In Performance Management, data that is processed and displayed in a graphical format is called a *report*. There are two types of reports:

- *Real-time reports*

  A real-time report indicates the current status of monitored hosts.

  This type of report is used to check the current status of the system and for possible problems. Performance data that is current at the time when such a report is displayed is depicted in a real-time report.

- *Historical reports*

  A historical report indicates the status of monitored hosts over a period of time, such as from some point in the past up to the present.

  This type of report is used to analyze trends in the operation status of the system. Collected performance data stored in PFM - RM for Platform's Store database is used to display historical reports.

(2) Taking appropriate action in the event of an operational problem at a monitored host

In the event of a problem at a monitored host, such as insufficient system resources, you can take appropriate action on the basis of judgment conditions and threshold values set by PFM - RM for Platform.

For example, you could define that a 90% usage rate of the physical CPU is to be set as the threshold value for a failure condition and that an email notification is to be sent when the threshold value is reached. Whenever this failure condition occurs, the system administrator will be notified of the problem in a timely manner.

If you set a judgment condition, as in this example, the appropriate action is taken automatically, thereby enabling the problem to be resolved at an early stage.

In Performance Management, the operation that is to be taken when a specified threshold value is reached is called an *action*. The following types of actions can be set:

- Sending an email
- Executing a command
- Issuing an SNMP trap
- Issuing a JP1 event

Defining a threshold together with an action constitutes an *alarm*. You use PFM - Web Console to set the alarms for the various type of performance data. For details about how to set alarms, see the chapter that describes operation monitoring by alarms in the *Job Management Partner 1/Performance Management User's Guide*.

When PFM - Web Console is used to set alarms, a table of the individual alarms is associated with PFM - RM for Platform. This table is called an *alarm table*; the association of an alarm table to PFM - RM for Platform is called *binding*.

Once an alarm table has been bound to PFM - RM for Platform, then whenever an item of performance data collected by PFM - RM for Platform reaches a threshold defined as an alarm, the defined action is executed.

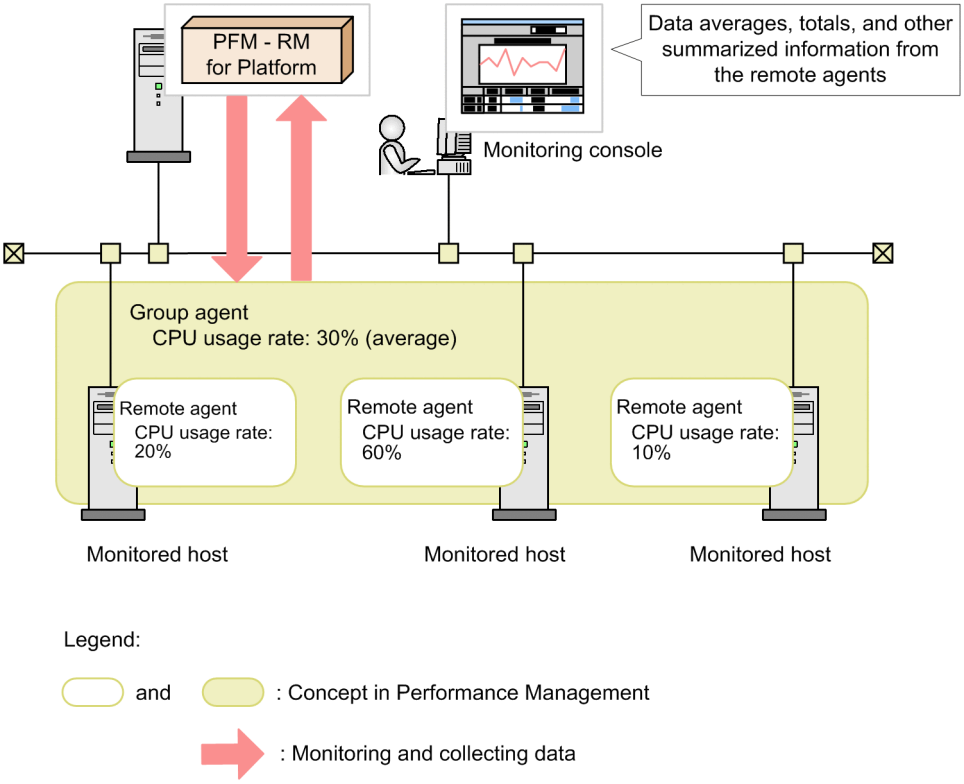
1.2.5 Integrating monitoring and analysis of performance data for multiple monitored hosts

PFM - RM for Platform can not only monitor and analyze performance data for each monitored host, but it can also monitor and analyze the performance data for all monitored hosts in an integrated manner.

PFM - RM for Platform treats each monitored host as a *remote agent*; the integration of remote agents is called a *group agent*.

The following figure shows the concept of remote agents and group agents.

Figure 1–2: Concept of remote agents and group agents



The information that is collected as a group agent includes performance data values for multiple monitored hosts, such as averages, totals, maximums, and minimums.

The remote agents that can be integrated as a group agent must belong to the same instance. Therefore, to integrate performance data, you must set the applicable monitored hosts in the same instance environment. For example, if you set instances as described below, you can visually analyze information for all the integrated monitored hosts:

- Setting, in the same instance, multiple guest OSs running in a virtual environment
- Setting, in the same instance, multiple servers that are operated for load distribution purposes

For details about remote agents and group agents, see the chapter that describes management of PFM - RM agents in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

1.2.6 Easy setting of alarms and reports

In order to use reports and alarms and to analyze and obtain the operation status and trends of hosts, you must first define the required monitoring items. In Performance Management, this definition is called a *monitoring template*, and it is provided by PFM - RM for Platform.

A monitoring template enables you to easily prepare for monitoring of the operation status of monitored hosts without having to create complex definitions. For details about the monitoring template, see *6. Monitoring Template*.

1.2.7 Applicable to cluster systems

You can also use PFM - RM for Platform in a cluster system.

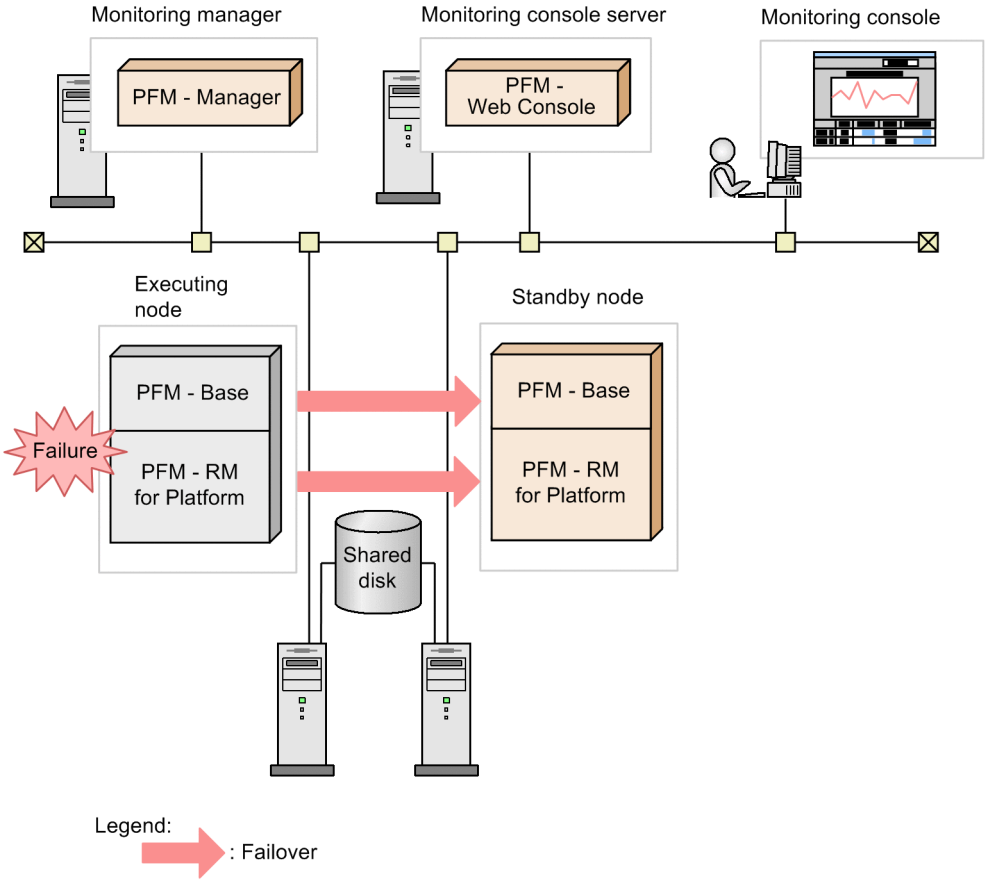
A cluster system links multiple server systems so that they can be run collectively as a single system.

You can run PFM - RM for Platform with a High Availability (HA) cluster system configuration.

Use of a cluster system enables you to configure a highly reliable system that is able to continue to operate, even in the event of a system problem. This enables you to achieve 24-hour/day operation and monitoring by Performance Management.

The following figure shows an example of the operation of Performance Management in the event of a problem on a monitored host in a cluster system.

Figure 1–3: Example of operation in the event of a problem on a monitored host in a cluster system



This example configures two environments with the same settings. It includes an *executing node* as the host used for normal operation and a *standby node* as the host used in the event of a failure.

For details about PFM - RM for Platform operation in a cluster system, see *5. Operation in a Cluster System*.

2 Functions of PFM - RM for Platform

This chapter explains the functions of PFM - RM for Platform.

2.1 Collecting and managing performance data

This section describes the collection and management of performance data.

The performance data collected by PFM - RM for Platform is stored in records of either the PI record type or the PD record type, depending on the characteristics of the data to be collected.

The record type determines the collection and management methods, such as when performance data is collected and whether the performance data is stored in the Store database. For details about the collection and management methods for each record type, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

You use PFM - Web Console to set the performance data management methods. For details about setting the methods, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

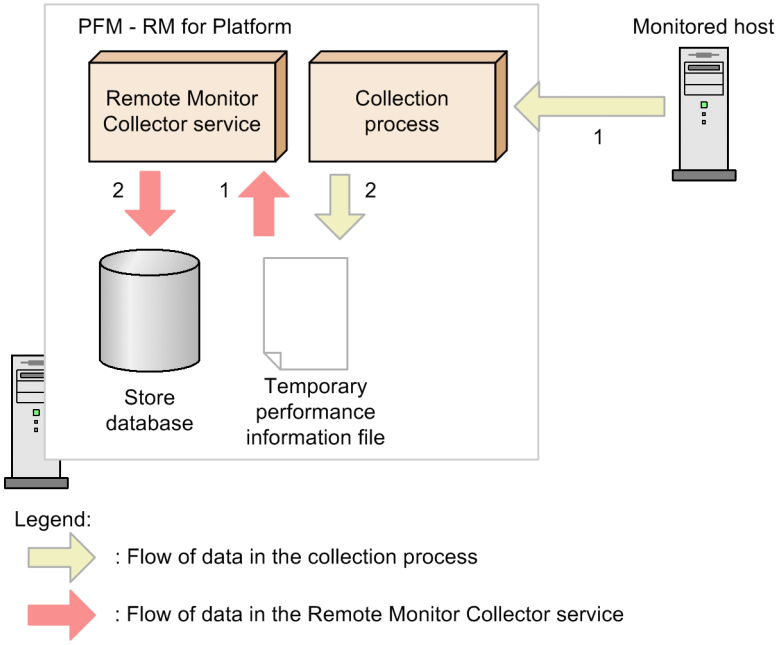
2.1.1 Flow of performance data collection

This subsection explains the flow of data and processing when PFM - RM for Platform collects performance data.

(1) Flow of data during performance data collection

The following figure shows the flow of data when performance data is collected.

Figure 2–1: Flow of data when performance data is collected



- Flow of data in the collection process
  1. Connects to the monitored host and collects its performance data.
  2. Outputs the collected performance data to the temporary performance information file.
- Flow of data in the Remote Monitor Collector service
  1. Loads the temporary performance information file that was output by the collection process.

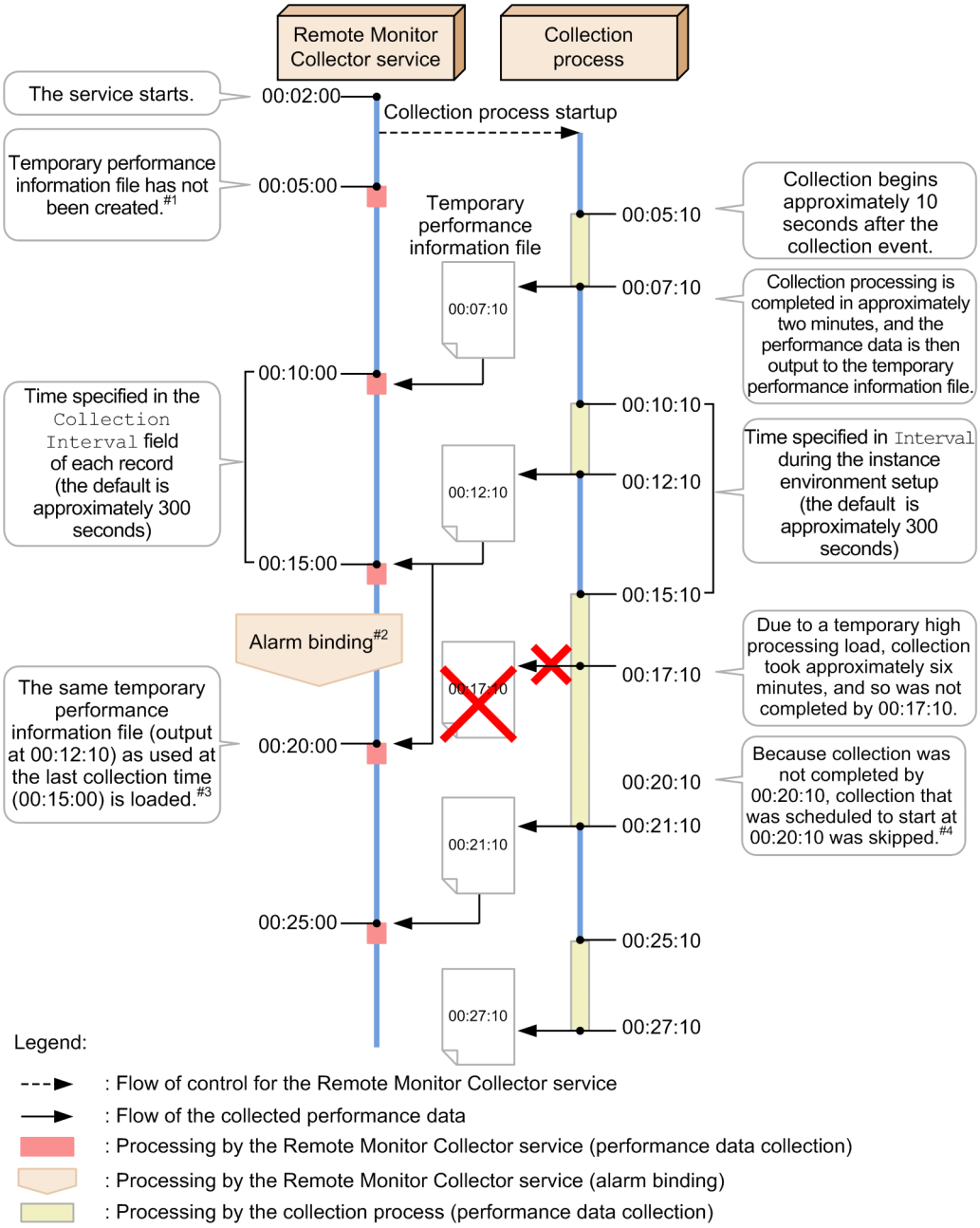
2. Stores the loaded performance data as records in the Store database.

The Remote Monitor Collector service and the collection processes operate separately, each on its own schedule.

(2) Flow of processing during performance data collection

The following figure shows an example of the flow of processing when performance data is collected.

Figure 2–2: Flow of processing when performance data is collected



#1

Because a temporary performance information file has not been created, data is not collected by collection processing at 00:05:00. The message `KAVL17017-W` is displayed.

#2

Consider the case when an alarm is bound between 00:15:00 and 00:20:00 during collection processing. This alarm might be evaluated at the 00:20:00 collection processing event (which is the first collection processing event after the alarm is bound). This depends on whether log information was collected in the record the alarm was bound to.

- The alarm is not evaluated if log information was collected.
- The alarm is evaluated if log information was not collected.

#3

As with collection processing at 00:15:00, the temporary performance information file output at 00:12:10 is loaded at the 00:20:00 collection processing.

If log information is being collected or if an alarm is to be evaluated, no performance data is collected. The message `KAVL17016-W` is displayed.

For collection processing based on real-time reports, the content of the temporary performance information file that was output at 00:12:10 is displayed, as was done at 00:15:00 of collection processing.

#4

Because the collection processing that started at 00:15:10 was not completed by 00:20:10, the collection processing that was scheduled to start at 00:20:10 is skipped.

Reference note

- When log information is stored in the Store database as performance data, the content being collected was actually created before the time of storage. The approximate time it takes from the collection of performance data to its storage in the Store database is at most the time specified in `Interval` during the instance environment setup (the default is approximately 300 seconds).
- The real-time report displays the content of the temporary performance information file that is in effect at the time the display operation is executed. If you refresh PFM - Web Console while a real-time report is being displayed, the content of the temporary performance information file that is in effect when you refreshed PFM - Web Console is displayed.
- Depending on the number of monitored hosts and the amount of data being collected, collection processing might lag.
- When you evaluate an alarm, the evaluation is performed on the performance data that was collected before the evaluation time. The approximate time it takes from the collection of performance data to the evaluation of an alarm is at most the time specified in `Interval` during the instance environment setup (the default is approximately 300 seconds).

  If you bind an alarm that uses a record that has not collected log information, the evaluation might be performed on the performance data that was collected farther back in the past depending on factors such as the timing of alarm binding and the lag in collection processing.

2.2 How to monitor performance

This section describes how to monitor performance.

Performance Management monitors the system operation status using baseline values as threshold values. The *baseline* is the performance data values that are assumed to be free of problems for system operation. Before you start monitoring performance, you must select a baseline on the basis of measurement results.

You should select an appropriate baseline by measuring system performance as follows:

- Measure system performance when the system is operating at peak status.

  We recommend that you select the baseline by measuring system performance when there are heavy loads in the operating environment.
- When you change system resources or the operating environment, measure the baseline again.

  The baseline might be affected significantly by the system configuration. When you change the system configuration, you should measure the baseline again.

The subsections below present examples of monitoring the performance of the following system resources:

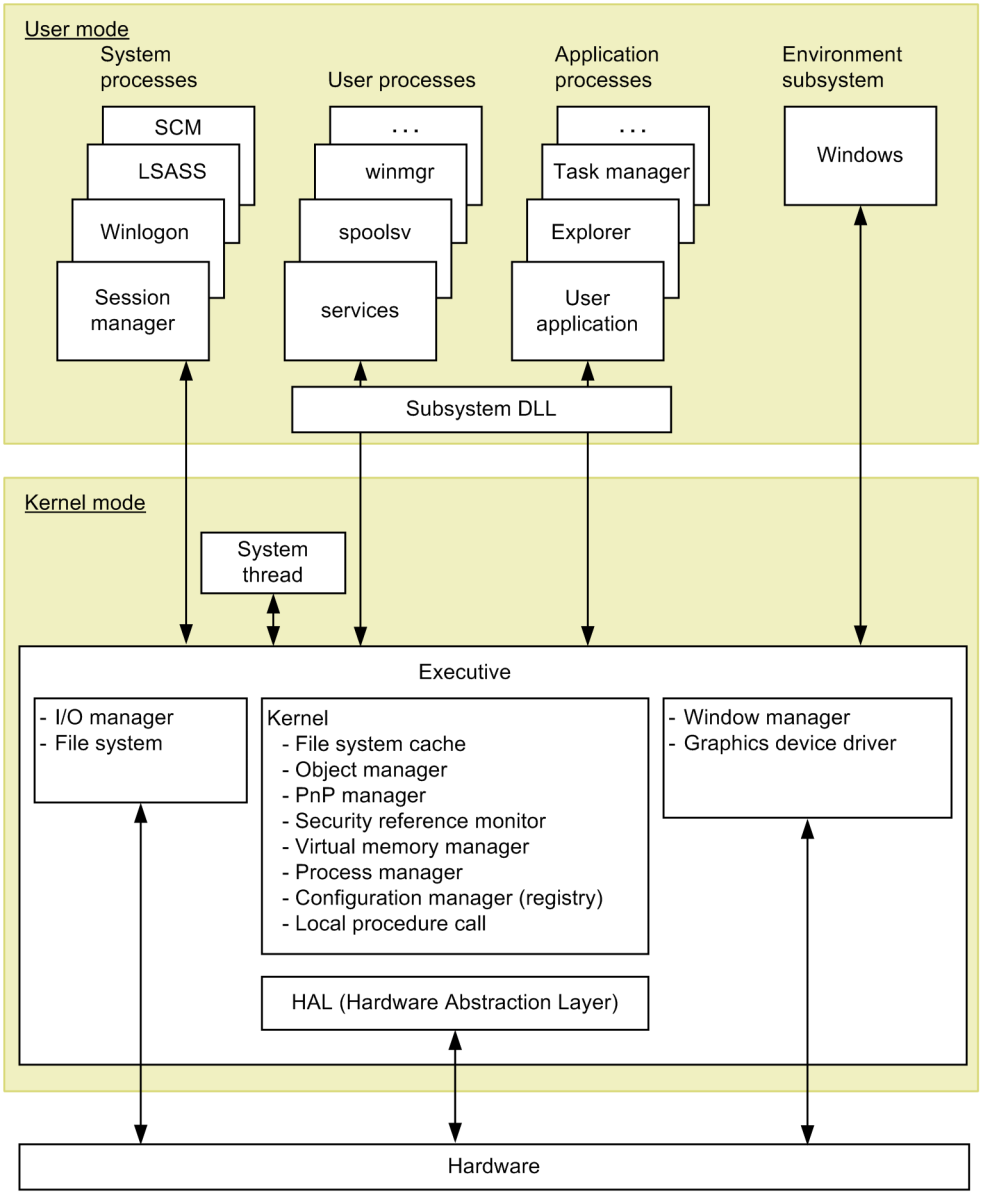
- Processor
- Memory
- Disk
- Network

2.2.1 Example of monitoring a processor

By monitoring processes, you can determine performance trends over the entire system.

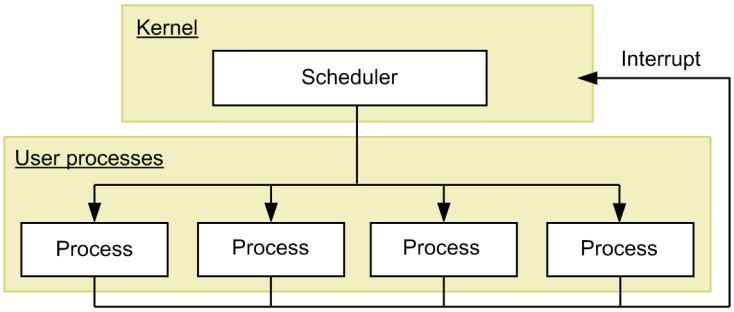
Windows processes consist of two types of processor access modes, called the user mode and the kernel mode. The following figure provides an overview of the Windows architecture.

Figure 2–3: Overview of the Windows architecture



UNIX processes consist of operations by kernel processes and operations by user processes. The following figure shows the relationship between the UNIX kernel and processes.

Figure 2–4: Relationship between the UNIX kernel and processes



(1) Overview of processor monitoring

Execution of jobs such as processes involves scheduling by the OS and allocation to the CPU. The queue request count that indicates the number of jobs waiting for CPU allocation tends to be proportional to the volume of loading in the entire system. Therefore, in general, you can obtain the processor usage status by monitoring the CPU usage rate and queue request count.

The following table lists and describes the records and fields that are used by PFM - RM for Platform for monitoring the processor.

Table 2–1: Records and fields used for processor monitoring

No.	Record	Field	Description of value	Interpretation of value
1	PI	Processor Queue Length	Queue request count	When this value continuously exceeds the threshold value, the processor might be busy.
2		Run Queue Avg 5 min	Average number of threads waiting in the execution queue	When this value is large, there might be a problem with processor utilization efficiency.
3		CPU %	CPU usage rate	When this value continuously exceeds the threshold value, the processor might be responsible for a system bottleneck.
4		System %	CPU usage rate in the kernel mode	When this value is large and the CPU % field of the PI record continuously exceeds the threshold value, there might be problems in a specific application process, such as a service or a system process.
5		User %	CPU usage rate in the user mode	When this value is large and the CPU % field of the PI record continuously exceeds the threshold value, there might be problems in a specific application process, such as a service.
6		Idle %	CPU idle rate	When this value is high, there might be no load on the CPU.
7		Interrupt Counts/sec	Hardware interrupt count (per second)	When the value of this field has increased greatly while the system workload is light, there might be a hardware interrupt problem, such as a slow device resulting in processor overloading.
8	PI_CPU#	CPU %	A processor's CPU usage rate	When this value continuously exceeds the threshold value, the processor might be responsible for a system bottleneck.
9		System %	CPU usage rate for a processor executed in the kernel mode	When this value is large and the CPU % field of the PI_CPU record continuously exceeds the threshold value, there might be problems in a specific application process, such as a service or a system process.
10		User %	CPU usage rate for a processor executed in the user mode	When this value is large and the CPU % field of the PI record continuously exceeds the threshold value, there might be problems in a specific application process, such as a service.
11		Interrupt Counts/sec	Hardware interrupt count (per second) for a processor	When the value of this field has increased greatly while the system workload is light, there might be a hardware interrupt problem, such as a slow device resulting in processor overloading.

#
Each field of the PI_CPU record is used to monitor the performance of one processor.

In a multiprocessor environment, the average value of all CPU usage rates is treated as the CPU usage rate for the system. Therefore, to obtain an accurate CPU usage rate, check the value for each CPU. To identify a process causing a bottleneck, check the CPU usage rate for each process.

You must use PFM - Agent for Platform to check the CPU usage rate for each process. For details about how to monitor processes, see the manual *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference*, for Windows systems, or *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference*, for UNIX systems.

(2) Example of a monitoring template for monitoring a processor

This subsection describes an example of alarms and reports that are provided as a monitoring template for monitoring a processor.

PFM - RM for Platform provides alarms and reports, such as the CPU Usage alarm and the `CPU Used Status (Multi-Agent)` report. To obtain more detailed performance information for a processor, you must monitor various aspects of the processor.

(a) Alarms

The following table lists and describes the processor-related alarms.

Table 2–2: Examples of alarms related to processor monitoring

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
1	CPU Usage	`PI`	CPU %	>= 90	>= 80	A processor usage rate of 80% or higher is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, the process might be causing a system bottleneck. If you find a process that makes excessive use of the processor, you must check the status of the process, and then take appropriate action. If there is no process that is using the processor excessively, you might need to consider upgrading the processor or adding a new processor.
2	Kernel CPU	`PI`	System %	> 75	> 50	A CPU usage rate in the kernel mode of higher than 50% is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, there might be a problem in the OS or system operating procedures. Check to see if more processes than the kernel scheduling can overcome have been created or deleted in a short period of time, or if there is a process that uses the processor excessively, and then take appropriate action. If there is no process that is using the processor excessively, you might need to consider upgrading the processor or adding a new processor.

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
3	Processor Queue	PI	Processor Queue Length	>= 10	>= 2	A consecutive queue request count of 2 or greater is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, the process might be causing a system bottleneck. If you find a process that makes excessive use of the processor, you must check the status of the process and take appropriate action. If there is no process that is using the processor excessively, you might need to consider upgrading the processor or adding a new processor.
4	Run Queue	PI	Run Queue Avg 5 min	> 8	> 4	An average thread count greater than 4 in the execution queue is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, there might be a problem in the OS or system operating procedures or with a specific application. Check to see if more processes than the kernel scheduling can overcome have been created or deleted in a short period of time, or if there is a process that uses the processor excessively, and then take appropriate action. If there is no process that is using the processor excessively, you might need to consider upgrading the processor or adding a new processor.
5	User CPU	PI	User %	> 85	> 65	A CPU usage rate higher than 65% in the user mode is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, there might be a problem with a specific application. Check to see if more processes than the kernel scheduling can overcome have been created or deleted in a short period of time, or if there is a process that uses the processor excessively, and then take appropriate action. If there is no process that is using the processor excessively, you might need to consider upgrading the processor or adding a new processor.

(b) Reports

The following table lists and describes the processor-related reports.

Table 2–3: Examples of reports related to processor monitoring

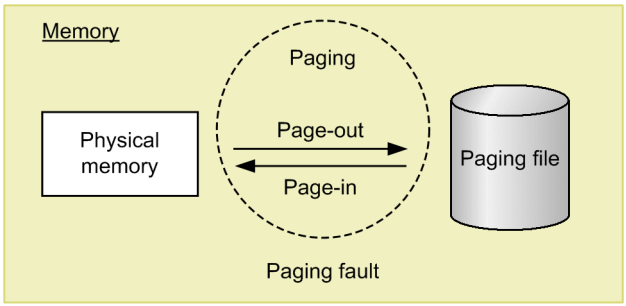
No.	Report name	Information displayed in the report
1	`CPU Used Status (Multi-Agent)`	Displays the CPU usage status in multiple systems.
2	`CPU Used Status`	Displays the CPU usage status in the system.
3	`CPU Per Processor Status`	Displays the processor usage status for each processor.

2.2.2 Example of monitoring memory

By monitoring memory, you can detect a shortage of physical memory or illegal operations by processes.

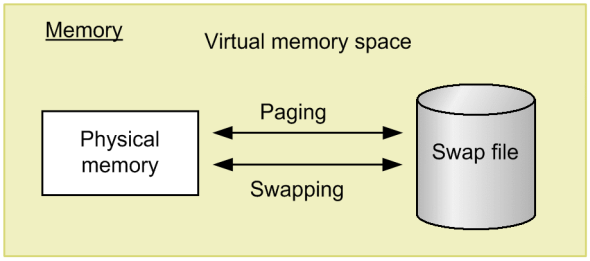
In Windows, memory consists of a physical memory and a paging file. The following figure shows the concept of memory in Windows.

Figure 2–5: Concept of memory in Windows



In UNIX, memory consists of a physical memory and a swap file. The following figure shows the concept of memory in UNIX.

Figure 2–6: Concept of memory in UNIX



(1) Overview of memory monitoring

In general, if there is a memory shortage in the physical memory and paging file (swap file), which use physical areas in RAM, the entire system's performance is affected adversely. However, a memory shortage alone is not always the cause of a bottleneck in the system.

Of the large amount of memory referenced by programs, the areas that are not accessed for more than a specific amount of time are saved in the paging file and loaded into the physical memory as needed. Because the speed of accessing this paging file (swap file) is much lower than the speed of accessing the physical memory, the efficiency of memory utilization is compromised.

Therefore, paging and page faults can be the cause of impaired system processing speed.

- *Paging* and *swapping*

  Paging and swapping refer to the movement of codes and data between the physical memory and the paging file (swap file). Loading data from the paging file (swap file) into the physical memory is called *page-in*, and saving data from the physical memory into the paging file (swap file) is called *page-out*.

- *Page faults*

  Page faults refers to accessing an area that does not exist in the physical memory.

We recommend that you monitor the efficiency of memory utilization, such as paging and page faults, as well as the memory usage. Note that paging occurs even during normal processing. Measure the baseline during stable system operation to determine an appropriate threshold value.

The following table lists and describes the records and fields that are used for monitoring the memory.

Table 2–4: Records and fields used for monitoring the memory

No.	Record	Field	Description of value	Interpretation of value
1	PI	Paging Pages/sec	Paging count (per second)	When the threshold value is exceeded continuously, the memory might be causing a system bottleneck due to frequent paging. Exceeding the threshold value temporarily is acceptable.
2		Page Fault Counts/sec	Number of page faults (per second)	When the threshold value is exceeded continuously, the memory might be causing a system bottleneck due to frequent page faults.
3		Total Mem Mbytes	Capacity of physical memory	Check the capacity of the physical memory.
4		Free Mem Mbytes	Free physical memory capacity	Check the free physical memory space.
5		Used Mem Mbytes	Amount of physical memory used	When this value is high, a large amount of physical memory might be in use.
6		Used Mem %	Physical memory usage rate	When this value is high, a large amount of physical memory might be in use.
7		Total Swap Mbytes	Capacity of virtual memory	Check the capacity of virtual memory.
8		Free Swap Mbytes	Free virtual memory capacity	Check the free virtual memory space.
9		Used Swap Mbytes	Amount of virtual memory used	When the threshold value is exceeded continuously, you might need a larger physical memory.
10		Used Swap %	Virtual memory usage rate	When the threshold value is exceeded continuously, you might need to expand the paging file.

A memory shortage can also occur due to defective programs.

Take appropriate action as necessary, such as identifying a process that unnecessarily uses a large amount of memory or whose memory usage increases continuously without limit, or monitor each process's memory usage.

You must use PFM - Agent for Platform to monitor each process's memory usage. For details about how to monitor processes, see the manual *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* for Windows systems or *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* for UNIX systems.

(2) Example of a monitoring template for monitoring memory

This subsection describes an example of alarms and reports that are provided as a monitoring template for monitoring memory.

PFM - RM for Platform provides alarms and reports, such as the Available Memory alarm and the `Memory Used Status (Multi-Agent)` report. To obtain more detailed performance information for the memory, you must monitor various aspects of the memory.

(a) Alarms

The following table lists and describes the memory-related alarms.

Table 2–5: Examples of alarms related to memory monitoring

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
1	Available Memory	`PI`	Free Mem Mbytes	< 3	< 4	Free physical memory capacity below 4 is treated as the warning or abnormal status. When this value becomes smaller than the threshold value set in the warning or abnormal condition, a shortage of physical memory might have occurred. If you find a process that makes excessive use of the memory, you must check the status of the process, and then take appropriate action. If there is no process that is using the memory excessively, you must take an action such as expanding the memory.
2	Page Faults		Page Fault Counts/sec	>= 5	>= 4	A page fault count of 4 or greater per second is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, a memory shortage might have occurred.
3	Pagescans		Page Scan Counts/sec	> 150	> 100	A page scan count per second that exceeds 100 is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, a memory shortage might have occurred.
4	Swap Outs		Swapped-Out Pages/sec	> 200	> 100	If more than 100 pages are swapped out per second by swap-out processing, the system treats it as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, a memory shortage might have occurred.
5	Used Swap Mbytes		Used Swap Mbytes	>= 1024[#1]	>= 1024[#2]	If the amount of virtual memory used exceeds the value of the Total Swap Mbytes field, the system treats it as the warning or abnormal status.

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
5	Used Swap Mbytes	PI	Used Swap Mbytes	>= 1024#1	>= 1024#2	When this value becomes greater than the threshold value set in the warning or abnormal condition, a memory shortage might have occurred.

#1
Set a value that is about 90% of the value of the Total Swap Mbytes field.

#2
Set the same value as for the Total Mem Mbyte field.

(b) Reports

The following table lists and describes the memory-related reports.

Table 2–6: Examples of reports related to memory monitoring

No.	Report name	Information displayed in the report
1	Memory Used Status (Multi-Agent)	Displays the status of physical memory usage in multiple systems.
2	Memory Used Status	Displays the status of physical memory usage in the system.
3	Pool Nonpaged Status	Displays the size of physical memory that cannot be paged out.
4	System Overview	Displays the operation status of the system.

2.2.3 Example of monitoring the disk

By monitoring the disk, you can detect a shortage of disk resources and identify a bottleneck caused by the disk. If you monitor the disk continuously, you can also identify trends in increasing disk usage, which can help you determine the system configuration and the timing of expansion.

(1) Overview of disk monitoring

The disk stores programs and the data used by the programs. If a shortage of free space occurs on the disk, not only does the system's response become slower but problems such as data loss also occur. A shortage of free disk space might also lead to other types of performance deterioration, such as a reduction in process response speed.

If there is not enough free disk space, a response wait status might occur when programs input data from the disk and output data to the disk. If the disk is suspected of being responsible for a bottleneck, such as because of a shortage of free disk space, first check if the disk has become fragmented. Next, check if an unreasonably large amount of disk space is being used by invalid files and if sufficient free space has been allocated.

The following table lists and describes the records and fields that are used for monitoring the disk.

Table 2–7: Records and fields used for disk monitoring

No.	Record	Field to be used	Description of value	Interpretation of value
1	PI_PDSK	Busy %	Disk busy rate	When the threshold value is exceeded continuously, there might be a concentration of processing that uses the disk.

No.	Record	Field to be used	Description of value	Interpretation of value
2	PI_PDSK	Avg Disk Time	Average disk I/O operation time	When the threshold value is exceeded continuously, there might be a concentration of processing that uses the disk.
3		Total MBytes/sec	Number of bytes transferred between disks (per second)	When this value is high, the system is considered to be running efficiently.
4	PI_LDSK	Free Mbytes %	Free disk space percentage	When this value is low, there might be a shortage of disk capacity.
5		Free Mbytes	Free disk space	When this value is low, there might be a shortage of disk capacity.

(2) Example of a monitoring template for monitoring the disk

This subsection describes examples of alarms and reports that are provided as a monitoring template for monitoring the disk.

PFM - RM for Platform provides alarms and reports, such as the Disk Busy % alarm and the `Avg Disk Time Status` report. To obtain more detailed performance of the disk, you must monitor various aspects of the disk.

(a) Alarms

The following table lists and describes the disk-related alarms.

Table 2–8: Examples of alarms related to disk monitoring

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
1	Disk Busy %	PI_PDSK	ID	<> _Total	<> _Total	A disk busy rate of 80% or higher is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, disk access might be busy.
2			Busy %	>= 90	>= 80	
3	Disk Service Time	PI_PDSK	Avg Disk Time	> 0.1	> 0.06	An average disk I/O operation that exceeds 0.06 second is treated as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, a very large I/O operation might have occurred.
4	Disk Space	PI_LDSK	Free Mbytes %	< 5	< 15	A free disk space percentage rate that is less than 15% is treated as the warning or abnormal status. When this value becomes less than the threshold value set in the warning or abnormal condition, a shortage of free disk space might have occurred. You need to take an appropriate action, such as deleting unneeded files, compressing files, optimizing the disk, or expanding the disk.
5	I/O Wait Time	PI	Wait %	> 80	> 60	A disk I/O wait time that exceeds 60% is treated as the warning or abnormal status.

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
5	I/O Wait Time	PI	Wait %	> 80	> 60	When this value becomes greater than the threshold value set in the warning or abnormal condition, a delay in I/O operations might have occurred, such as a delay in database update processing.
6	Disk Free Size	PI_LDSK	ID	<> _Total	<> _Total	Unused disk space of less than 10,240 megabytes is treated as the warning or abnormal status. When this value becomes less than the threshold value set in the warning or abnormal condition, a shortage of unused disk space might have occurred. You need to take an appropriate action, such as deleting unneeded files, compressing files, optimizing the disk, or expanding the disk.
7			Free Mbytes	< 5120	< 10240	

(b) Reports

The following table lists and describes the disk-related reports.

Table 2–9: Examples of reports related to disk monitoring

No.	Report name	Information displayed in the report
1	Avg Disk Time Status	Displays the average I/O operation time for the physical disk.
2	Free Megabytes - Logical Disk	Displays information about the logical disk space being used.
3	Physical Disk Busy Status	Displays the percentage of time during which the disk was busy.

2.2.4 Example of monitoring the network

By monitoring network information, you can check the status of response speeds for system-provided functions. Also, continuous monitoring of the network, such as of the amount of data transfer in the network, can assist in evaluating the network configuration and planning for future expansion.

(1) Overview of network monitoring

Identifying a bottleneck in the network requires examination of various factors, such as hardware, client operations, and data transfer rates between servers and clients.

PFM - RM for Platform provides alarms and reports, such as the Network Received alarm and the Network Data report. To obtain more detailed information on network performance, you must monitor various aspects of the network.

The following table lists and describes the records and fields that are used for monitoring the network.

Table 2–10: Records and fields used for network monitoring

No.	Record	Field	Description of value	Interpretation of value
1	PI_NET	Total Bytes/sec	Amount of data transferred (per second)	If NIC is always used to transfer data and this value is often equal to or less than the threshold value, NIC might be causing the bottleneck. When this value is typically

No.	Record	Field	Description of value	Interpretation of value
1	PI_NET	Total Bytes/sec	Amount of data transferred (per second)	greater than the threshold value, a large amount data can be transferred successfully.
2		Rcvd Bytes/sec	Amount of data received (per second)	If NIC is always used to receive data and this value is often equal to or less than the threshold value, NIC might be causing the bottleneck. When this value is typically greater than the threshold value, a large amount data can be received successfully.
3		Sent Bytes/sec	Amount of data sent (per second)	If NIC is always used to send data and this value is often equal to or less than the threshold value, NIC might be causing the bottleneck. When this value is typically greater than the threshold value, a large amount data can be sent successfully.

(2) Example of a monitoring template for monitoring the network

This subsection describes an example of using the alarms and reports that are provided as a monitoring template for monitoring the network.

PFM - RM for Platform provides alarms and reports, such as the Network Received alarm and the `Network Data` report.

(a) Alarms

The following table lists and describes the network-related alarms.

Table 2–11: Examples of alarms related to network monitoring

No.	Alarm	Record	Field	Abnormal condition	Warning condition	Interpretation of value
1	Network Received	PI_NET	Rcvd Bytes/sec	>= 50000#1	>= 50000#2	When the amount of data received per second exceeds about 50% of the NIC bandwidth, the system treats it as the warning or abnormal status. When this value becomes greater than the threshold value set in the warning or abnormal condition, you need to take appropriate action, such as upgrading NIC or the physical network.

#1
Set a value that is about 70% of the NIC bandwidth.

#2
Set a value that is about 50% of the NIC bandwidth.

(b) Reports

The following table lists and describes the network-related reports.

Table 2–12: Examples of reports related to network monitoring

No.	Report name	Information displayed in the report
1	`Network Data`	Displays the status of communication between networks.

2.2.5 Example of monitoring processes and services

By monitoring processes and services, you can check whether the system is running normally.

(1) Overview of process and service monitoring

A system functions based on individual processes and services. Therefore, knowing the operating statuses of these processes and services is essential for stable system operation.

If the processes or services that provide the system's functionality terminate abnormally, the system will stop, resulting in serious adverse effects on operations. Therefore, it is important to monitor the initiation, termination, and startup status of processes and services, and to detect any errors quickly so that you develop corrective measures.

Using PFM - RM for Platform, you can collect the process operation status information from multiple monitored hosts and monitor it from PFM - Web Console. You specify the collection of process operation status information interactively using PFM - Web Console or by using commands.

PFM - RM for Platform monitors processes by collecting information from them. Therefore, note that even when processes and services are being monitored, their statuses are only reported when PFM - RM for Platform collects information from them, and not when their statuses actually change.

If collection processing that uses WMI or SSH is treated as a separate process (a core collection process) and this core collection process does not terminate within the specified time, performance information cannot be collected from a monitored target having the same instance for which collection has not been completed. A time-out occurs.

The following table lists and describes the records and fields that are used for monitoring the processes and services.

Table 2–13: Records and fields used for monitoring processes and services

No.	Record	Field to be used	Description of value	Interpretation of value
1	PD_APP2	Application Exist	Status of the application specified as a monitoring target	If this value is ABNORMAL, either all processes and services being monitored on a per-application basis are stopped, or more processes and services than necessary are running.
2		Application Status	Status of the application specified as a monitoring target	If this value is ABNORMAL, either one of the processes and services being monitored on a per-application basis is stopped, or more processes and services than necessary are running.
3	PD_APS	Command Line	Command line for executing programs	If no records have been collected, the process might be stopped.
4		Program Name	Program name	
5	PD_ASVC	Display Name	Name used by the user interface program to identify a service	In all cases except when the application service (process) is running, the service might be stopped.
6		Service Name	Name of the service being used by the service control manager database	
7		State	Status of a service when data is being collected	

You can use PFM - RM for Platform to collect process operation status information by using one of the following methods:

- Collecting the status on a per-process or per-service basis

- Collecting the status on a per-application basis by grouping multiple processes or services

The following table shows the records used for each of these methods.

Table 2–14: Records used for collecting process operation status information (on a per-process or per-service basis)

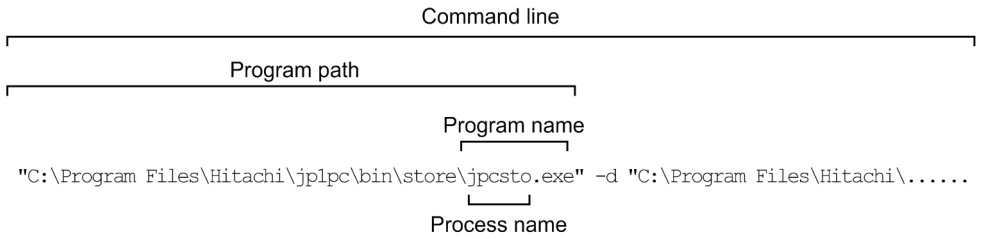
No.	Record	Monitoring target	Information to be stored	Collection method
1	PD_APS	Processes in a Windows or UNIX environment	Stores performance data indicating the status of the monitored host's process at a given time.	Real-time
2	PD_ASVC	Services in a Windows environment	Stores performance data indicating the status of an application service registered in the monitored host's service control manager (SCM), such as a Win32 process.	Real-time

Table 2–15: Records used for collecting process operation status information (on a per-application basis)

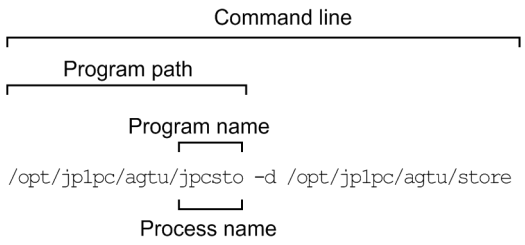
No.	Record	Monitoring target	Information to be stored	Collection method
1	PD_APP2	• Processes in a Windows or UNIX environment • Services in a Windows environment	Stores performance data that summarizes the records stored in the Application Process Overview (PD_APS) or Application Service Overview (PD_ASVC) record in the status, at a given point in time, on a per-application basis.	• Real-time • History
2	PD_APPC		Stores as performance data the records stored in the Application Process Overview (PD_APS) or Application Service Overview (PD_ASVC) record in the status, at a given point in time, on each process and service being monitored, on a per-application basis.	
3	PD_APPD		Stores performance data that summarizes the records stored in the Application Process Overview (PD_APS) or Application Service Overview (PD_ASVC) record in the status, at a given point in time, on each process and service being monitored, on a per-application basis. This stored performance data is more detailed than the Application Process Count (PD_APPC) records.	Real-time

The relationships between the process name, program name, program path, and command line used for setting up process status monitoring are explained below using examples.

When the monitored host is Windows



When the monitored host is UNIX



(2) Usage example of templates related to monitoring of processes and services

This subsection shows a usage examples of alarms and reports, which are provided as monitoring templates, related to process and service monitoring.

PFM - RM for Platform provides templates such as the Process Existence alarm and the Application Status report.

(a) Alarms

The following table lists and describes alarms related to monitoring of process and service statuses.

Table 2–16: Usage examples of alarms related to monitoring of process and service statuses

No.	Alarm	Record used	Field used	Error condition	Warning condition	Interpretation of value
1	Application Status	PD_APP2	Application Exist	Application Name = * AND Application Exist = ABNORMAL AND Application Status = ABNORMAL	Application Name = * AND Application Exist = NORMAL AND Application Status = ABNORMAL	Either one of the processes or services being monitored on a per-application basis is stopped, or more processes and services than necessary are running.
2			Application Name			
3			Application Status			
4	Process Existence	PD_APS	Program Name	Program Name <> jpcsto.exe#1	Program Name <> jpcsto.exe#1	If no records have been collected, a warning or error state has occurred.
5	Service Stop	PD_ASVC	Service Name State	Service Name = JP1PCAGT_7S#2 AND State <> Running	Service Name = JP1PCAGT_7S#2 AND State <> Running	If the monitoring-target service has not started, a warning or error state has occurred.
6	Service Stop(dsp nm)	PD_ASVC	Display Name State	Display Name = PFM - Remote Monitor for Platform#3 AND State <> Running	Display Name = PFM - Remote Monitor for Platform#3 AND State <> Running	If the monitoring-target service has not started, a warning or error state has occurred.

#1

Specify the name of the program to be monitored.

#2

Specify the name of the service to be monitored.

#3

Specify the display name of the service to be monitored.

(b) Reports

The following table lists and describes the reports related to monitoring of process and service statuses.

Table 2–17: Usage examples of reports related to monitoring of process and service statuses

No.	Report name	Displayed content of the report
1	Application Process Count	Operating state of the processes or services being monitored on a per-application basis
2	Application Process Status	
3	Application Status	Operating state of an application

3 Installation and Setup

This chapter explains how to install and set up PFM - RM for Platform. For details about how to install and set up the entire Performance Management system, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

3.1 Installation and setup of the Windows edition

This section describes the procedures for installing and setting up PFM - RM for Platform in a Windows environment.

3.1.1 Issues to consider before installing the Windows edition

This subsection describes issues to be considered before you install PFM - RM for Platform.

(1) Prerequisite OS

PFM - RM for Platform can run on the following operating system (OS):

- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

(2) Setting up a network environment

To use Performance Management to run PFM - RM for Platform, you must set up a network environment, such IP addresses and port numbers.

(a) Setting IP addresses

You must set up the environment for PFM - RM for Platform in such a way that it can resolve an IP address from a host name. PFM - RM for Platform will not start in an environment in which an IP addresses cannot be resolved.

In Performance Management, a host such as a PFM - RM for Platform host that is used in the Performance Management system is called a *monitoring host*.

You use one of the following methods to set host names and IP addresses:

- `jpchosts` file (Performance Management's host information configuration file)
- `hosts` file
- DNS

For the monitoring host name, use either the real host name or the alias name.

- Using the real host name

  In a Windows environment, specify the name in such a way that the IP address can be resolved from a host name that can be checked with the execution results of the `hostname` command.

  Note that Performance Management supports DNS, but not FQDN. This means that when you set the IP address, you must use the host name obtained by the `hostname` command without the domain name.
- Using an alias name

  Set up the environment in such a way that the IP address can be resolved from a specified alias name.

For details about setting the name of the monitoring host, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note that the IP address specified in the `jpchosts` file is not used for IP address resolution with the monitored host.

Notes about setting IP addresses

- If you use Performance Management in multiple LAN environments, use the `jpchosts` file to set IP addresses. For details about using the `jpchosts` file to set IP addresses, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
- Performance Management will not run on a host where IP addresses are assigned dynamically by DHCP. You must set fixed IP addresses for all monitoring hosts.

(b) Settings for using IPv6

Performance Management supports both IPv4 and IPv6 network environments. Therefore, you can run Performance Management even in a network environment where IPv4 and IPv6 coexist.

PFM - RM for Platform can use IPv6 to communicate with PFM - Manager. However, this applies only when the OS of the host on which PFM - RM for Platform and PFM - Manager are installed is Windows Server 2008 R2, Windows Server 2012, or Linux. For details about the applicable scope of communication in the IPv4 and IPv6 environments, see *L. Communication in IPv4 and IPv6 Environments*.

To communicate using IPv6, you must enable the use of IPv6 on both the PFM - Manager host and the PFM - RM host. You specify this setting by executing the `jpcconf ipv6 enable` command. The following explains the conditions to use for determining whether you need to execute this command.

Cases in which you need to execute the `jpcconf ipv6 enable` command:

- If all hosts are being changed from an IPv4 environment to an IPv6 environment.
- In an environment where IPv4 and IPv6 coexist, if PFM - Manager is being changed from an IPv4 environment to an IPv6 environment.

Cases in which you do not need to execute the `jpcconf ipv6 enable` command:

- If all hosts are already in an IPv6 environment.
- In an environment where IPv4 and IPv6 coexist, if PFM - Manager is already set up as an IPv6 environment.

An execution example of the `jpcconf ipv6 enable` command follows:

```
jpcconf ipv6 enable
```

For details about the `jpcconf ipv6 enable` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*. For details about the conditions and timing for executing the `jpcconf ipv6 enable` command, see the chapter that describes an example of a network configuration that includes an IPv6 environment in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

When PFM - RM for Platform will use IPv6 to communicate with monitored hosts, specify a monitored host name that can be resolved.

PFM - RM for Platform uses a resolvable IP address to communicate with a monitoring target. When PFM - RM for Platform communicates with a monitoring target in an environment where IPv4 and IPv6 coexist, PFM - RM for Platform will not try to communicate using another IP address if communication using a resolvable IP address fails.

For example, if a connection attempt using IPv4 fails, PFM - RM for Platform will not retry using IPv6. Similarly, if a connection attempt using IPv6 fails, PFM - RM for Platform will not retry using IPv4. Therefore, make sure that connection can be established before starting PFM - RM.

(c) Setting port numbers

You must assign a port number to each service of the programs used in Performance Management. Set up the network in such a manner that the port numbers assigned to PFM - RM for Platform can be used for communication.

The table below lists and describes the default port number assigned to various services. For other services, an unused port number is assigned automatically each time the service starts.

Table 3–1: Default port numbers for services (for Windows)

No.	Supported function	Service name	Parameter	Port number	Description
1	Service configuration information management function	Name Server	`jp1pcnsvr`	`22285`	Port number used by PFM - Manager's Name Server service. This port number is set at all hosts of Performance Management.
2	NNM linkage facility	NNM Object Manager	`jp1pcovsvr`	`22292`	Port number used for communication between the map manager and the object manager when the NNM linkage facility is used with PFM - Manager and PFM - Base. This port number is set at the host where PFM - Manager and PFM - Base are installed.
3	Service status management function	Status Server	`jp1pcstatsvr`	`22350`	Port number used by the Status Server service of PFM - Manager and PFM - Base. This port number is set at the host where PFM - Manager and PFM - Base are installed.
4	Monitoring console communication function	View Server	`jp1pcvsvr`	`22286`	Port number used by the View Server service of PFM - Manager. This port number is set at the host where PFM - Manager is installed.
5	Web service function	Web Service	--	`20358`	Port number used by the Web Service service of PFM - Web Console.
6	Web container function	Web Console	--	`20359` `20360`	Port number used by the Web Console service of PFM - Web Console.
7	JP1/ITSLM linkage facility	JP1/ITSLM	--	`20905`	Port number specified in JP1/ITSLM.

Legend:
--: Not applicable

When you use Performance Management in an environment that includes a firewall, you must use fixed port numbers. For details about how to use fixed port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(3) OS user permissions required for installation

When you install PFM - RM for Platform, make sure that you use an account that has Administrator permissions.

(4) Prerequisite programs

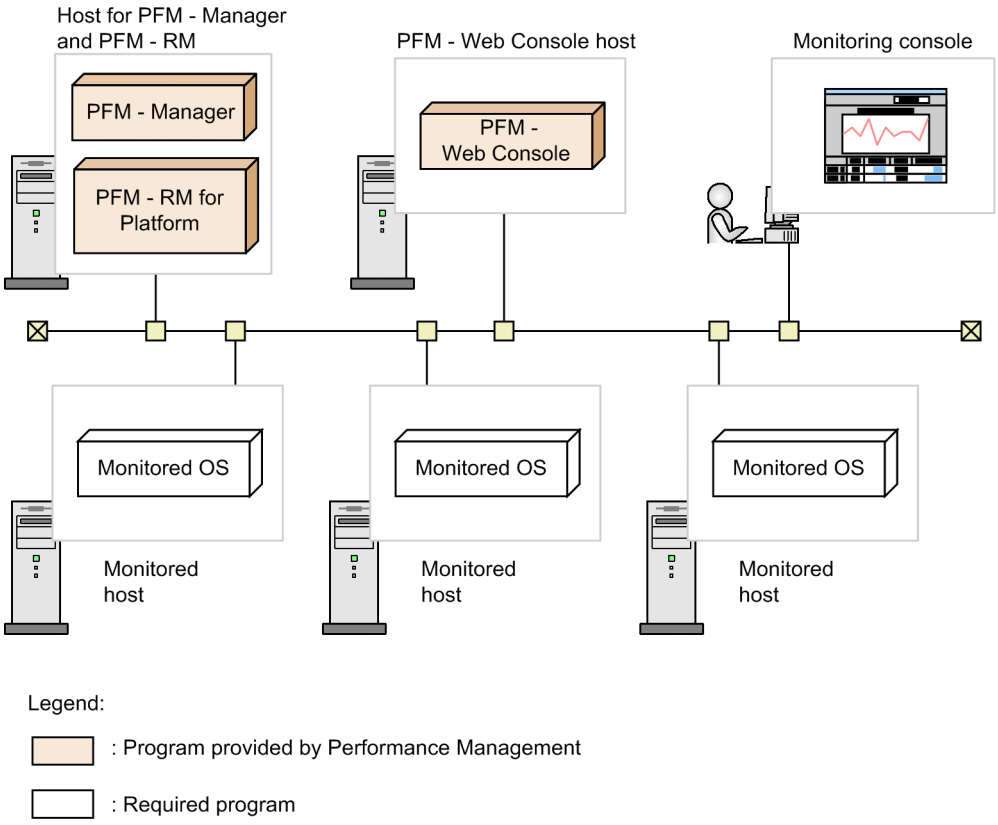
This subsection describes the configuration of programs required in order to install PFM - RM for Platform.

There are two major types of program configurations, as described below. Evaluate the program configurations from the perspective of your system environment.

(a) When installing PFM - RM for Platform on the PFM - Manager host

With this program configuration, PFM - RM for Platform is installed on the same host as PFM - Manager. The following figure shows the program configuration.

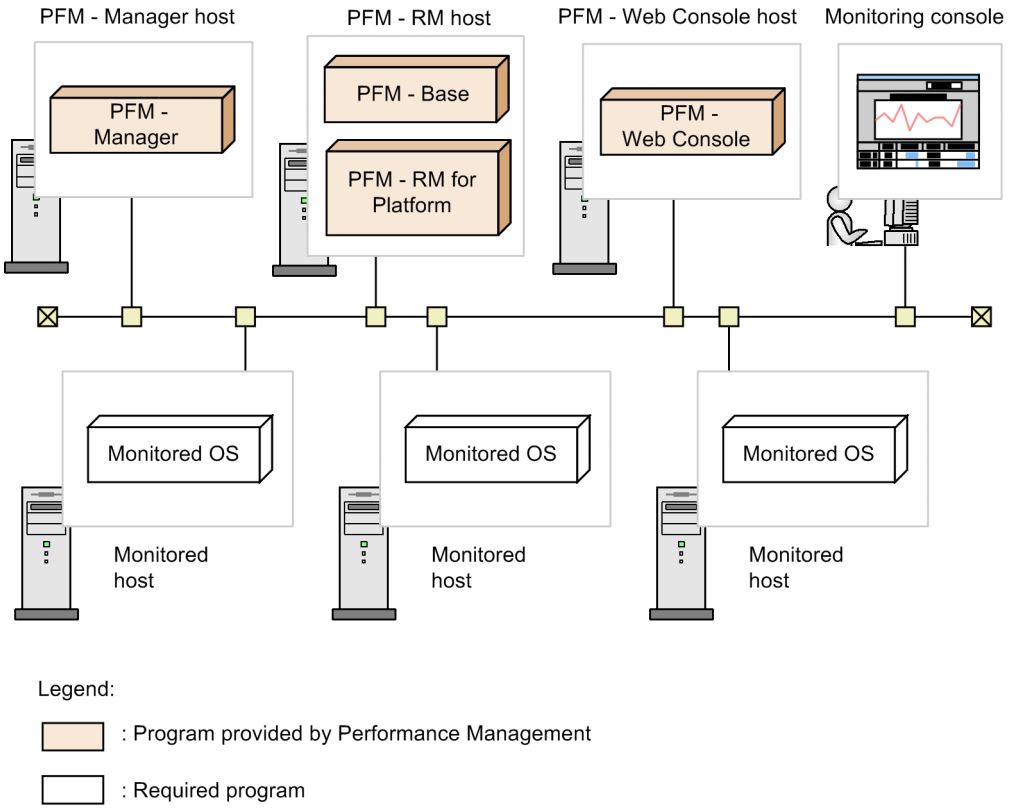
Figure 3–1: Program configuration (when PFM - RM for Platform and PFM - Manager are installed on the same host (for Windows))



(b) When installing PFM - RM for Platform on a host other than the PFM - Manager host

With this program configuration, PFM - RM for Platform is installed on a host other than the PFM - Manager host. If you use this program configuration, you must install PFM - Base on the same host as for PFM - RM for Platform. The following figure shows the program configuration.

Figure 3–2: Program configuration (when PFM - RM for Platform and PFM - Base are on the same host (for Windows))



(c) Prerequisite OSs for monitored hosts

A monitored host must be using one of the following OSs:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- HP-UX
- Solaris
- AIX
- Linux

(d) Prerequisite programs for Performance Management

PFM - Manager or PFM - Base must be available on the host where PFM - RM for Platform is installed.

If you install PFM - RM for Platform on a host where PFM - Manager is available, PFM - Base is not required. If you install multiple PFM - RMs on a host where PFM - Base is available, you need only one PFM - Base.

You also need PFM - Web Console in order to use PFM - RM for Platform to monitor the operation of monitored hosts.

(5) Environment settings required for collecting performance data (when both the PFM - RM host and the monitored hosts are running Windows)

PFM - RM for Platform uses WMI to collect performance data from monitored hosts when these hosts are running Windows. Performance data cannot be collected if WMI connection settings have not been specified. Therefore, you must specify WMI settings at the PFM - RM host as well as at the monitored hosts.

The following describes the required WMI settings.

(a) Setting the user accounts

To use WMI, you need a local user account or domain account for the PFM - RM host, and a local user account for the monitored host.

PFM - RM for Platform collects information using the account that is specified for connection in WMI's name space.

- PFM - RM host account

  To set up the host account, specify the values appropriate to the `RMHost_User`, `RMHost_Password`, and `RMHost_Domain` settings shown in Table *3-20 Instance environment setting items and values for PFM - RM for Platform (for Windows)*. You specify this account when you set up an instance.

  If you run PFM - RM for Platform in a cluster system, set up the account for the PFM - RM host so that it is possible to log on to both the executing system and the standby system by specifying the same user name and password.

  When the PFM - RM host itself is the monitoring target, the specified account also affects the WMI connection. The type of records that can be collected differs depending on the account type. The following table shows various account types and whether records can be collected.

  Table 3–2: PFM - RM host account types and whether records can be collected (when the monitored host is the local host and is running Windows Server 2003)

Account type	Can records be collected?	
	Records that stores process operation status information#1	Records that stores information other than process operation status#2
Administrator (Built-in Administrator)	Y	Y
Administrators group member	Y	Y
Performance Log Users group member	N	Y
Performance Monitor Users group member	N	Y

Legend:

Y: Can be collected.

N: Cannot be collected.

#1

Applies to `PD_APS`, `PD_ASVC`, `PD_APP2`, `PD_APPC`, and `PD_APPD` records.

#2

Applies to `PI`, `PI_CPU`, `PI_LDSK`, `PI_NET`, `PI_PDSK`, and `PD` records.

Table 3–3: PFM - RM host account types and whether records can be collected (when the monitored host is the local host and is running Windows Server 2008 or Windows Server 2012)

Account type	Can records be collected?	
	Records that stores process operation status information#1	Records that stores information other than process operation status#2
Administrator (Built-in Administrator)	Y	Y
Administrators group member (UAC enabled)	N	N
Administrators group member (UAC disabled)	Y	Y
Performance Log Users group member	N	Y
Performance Monitor Users group member	N	Y

Legend:

Y: Can be collected.

N: Cannot be collected.

#1

Applies to `PD_APS`, `PD_ASVC`, `PD_APP2`, `PD_APPC`, and `PD_APPD` records.

#2

Applies to `PI`, `PI_CPU`, `PI_LDSK`, `PI_NET`, `PI_PDSK`, and `PD` records.

- Monitored host accounts

  To set up a monitored host account, specify the values appropriate to the `User`, `Password`, and `Domain` settings shown in Table *3-27 Setting items and values for a monitored host in PFM - RM for Platform*. You specify such an account when you set up each monitoring target.

  Note that a monitored host account must be set as a member of the Administrators, Performance Log Users, or Performance Monitor Users group.

  You need permissions to perform operations such as Windows security audits.

  The type of records that can be collected differs depending on the account type. The following table shows various account types and whether records can be collected.

Table 3–4: Account types and whether records can be collected (when the monitored host is running Windows Server 2003)

Account type	Can records be collected?	
	Records that stores process operation status information#1	Records that stores information other than process operation status#2
Administrator (Built-in Administrator)	Y	Y
Administrators group member	Y	Y
Performance Log Users group member	N	Y
Performance Monitor Users group member	N	Y

Legend:

Y: Can be collected.

N: Cannot be collected.

#1

Applies to `PD_APS`, `PD_ASVC`, `PD_APP2`, `PD_APPC`, and `PD_APPD` records.

#2

Applies to PI, PI_CPU, PI_LDSK, PI_NET, PI_PDSK, and PD records.

Table 3–5: Account types and whether records can be collected (when the monitored host is running Windows Server 2008 or Windows Server 2012)

Account type		Can records be collected?	
		Record that stores process operation status information#1	Record that stores information other than process operation status#2
Local account	Administrator (Built-in Administrator)	Y	Y
	Administrators group member (UAC enabled and LocalAccountTokenFilterPolicy not specified)	N	N
	Administrators group member (UAC enabled and LocalAccountTokenFilterPolicy specified)	Y	Y
	Administrators group member (UAC disabled)	Y	Y
	Performance Log Users group member	N	Y
	Performance Monitor Users group member	N	Y
Domain account	Administrator (Built-in Administrator)	Y	Y
	Administrators group member (UAC enabled)	Y	Y
	Administrators group member (UAC disabled)	Y	Y
	Performance Log Users group member	N	Y
	Performance Monitor Users group member	N	Y

Legend:

Y: Can be collected.

N: Cannot be collected.

#1

Applies to PD_APS, PD_ASVC, PD_APP2, PD_APPC, and PD_APPD records.

#2

Applies to PI, PI_CPU, PI_LDSK, PI_NET, PI_PDSK, and PD records.

(b) Setting the WMI service

Set the WMI service startup option for monitored hosts to a value other than **Disabled**. If it is set to **Disabled**, performance data will not be collected.

(c) WMI connection settings

Specify the WMI connection settings at both the PFM - RM host and the monitored hosts. For details about the WMI connection settings, see *3.1.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows)*.

(d) Setting up WMI remote connection that uses UAC

If either Windows Server 2008 or Windows Server 2012 is used, the UAC function restricts the permissions granted to local users who have Administrator permissions (except for the Administrator user who is created during OS installation). Consequently, if WMI remote connection to monitored servers running Windows Server 2008 or Windows Server 2012 is executed as a local user who has Administrator permissions, a problem might occur. That is, because the

connection attempt will be made with ordinary user permissions instead of Administrator permissions, the access might be refused, resulting in an error. To avoid this, take one of the following steps if UCA is enabled:

- For the user to be used for authentication, use the Administrator user who is created during OS installation.
- Execute the following command with Administrator permissions to update the registry value to make UAC permit remote connection.

  ```
  reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
  LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
  ```

  To cancel the remote connection permitted by UAC, execute the following command:

  ```
  reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
  \System /v LocalAccountTokenFilterPolicy /f
  ```

If UAC is disabled, use a member of the Administrator group as the user to be used for authentication.

(6) Environment settings required for collecting performance data (when the PFM - RM host is running Windows and the monitored hosts are running UNIX)

PFM - RM for Platform uses SSH to collect performance data from monitored hosts when these hosts are running UNIX. To use SSH, you must install PuTTY and ActivePerl on the PFM - RM host. Performance data cannot be collected if SSH connection settings have not been specified. Because SSH authentication uses the public key authentication method, you must specify public key authentication settings. You might also need to install other appropriate software and packages on the PFM - RM host and the monitored hosts because OS commands are used to collect performance data.

Notes on installing PuTTY and ActivePerl

- To perform the installation, you must use an account that has Administrators permissions.
- Do not install into a folder whose path name includes a multi-byte character.

(a) User account settings

To use SSH, both PFM - RM host and monitored host accounts are required.

- PFM - RM host account

  To set up an account, specify the values using the settings for `RMHost_User`, `RMHost_Password`, and `RMHost_Domain` in Table *3-20 Instance environment setting items and values for PFM - RM for Platform (for Windows)*. The account that is set up must be specified during instance setup.

  If you run PFM - RM for Platform in a cluster system, specify the same user and password for the PFM - RM host account at both the active server and the standby server so that the account can log on to both servers.

- Monitored host account

  If the OS of the connection-target monitored host is AIX and a user other than `root` user is to collect information, that user must belong to both the `adm` group and the `system` group; otherwise, some information will not be collected.

  To ensure that the user belongs to both groups (`adm` and `system`), execute the following command at the connection-target monitored host:

  ```
  $ id
  uid=xxx(xxx) gid=x(xxx) groups=0(system),4(adm)
  ```

For details about the information that is not collected, see *7. Records*. If the OS of the monitored host is not AIX, this user limitation is not applicable.

(b) Installing software and packages

■ Software required for the PFM - RM host

The table below lists the software required for the PFM - RM host. For details, see the *Release Notes* for this product.

Table 3–6: Software required for the PFM - RM host

No.	Software name	OS	Default
1	PuTTY	Windows Server 2003 (x86)	N
2		Windows Server 2003 (x64)	N
3		Windows Server 2008 (x86)	N
4		Windows Server 2008 (x64)	N
5		Windows Server 2012	N
6	ActivePerl	Windows Server 2003 (x86)	N
7		Windows Server 2003 (x64)	N
8		Windows Server 2008 (x86)	N
9		Windows Server 2008 (x64)	N
10		Windows Server 2012	N

Legend:
N: Not installed by default.

■ Packages required for monitored hosts (SSH)

The set of packages (SSH) required for a monitored host depends on the OS of the monitored host. For details, see the *Release Notes* for this product.

The following table lists the packages required when a monitored host's OS is HP-UX.

Table 3–7: Software required for monitored hosts (for HP-UX)

No.	Software name	OS	Default
1	HP-UX Secure Shell	HP-UX 11i V3 (IPF)	Y

Legend:
Y: Installed by default.

The following table lists the packages required when a monitored host's OS is Solaris.

Table 3–8: Packages required for monitored host (for Solaris)

No.	Software name	OS	Default
1	SunSSH	Solaris 10 (SPARC)	Y
2		Solaris 10 (x64)	Y
3		Solaris 10 (x86)	Y
4		Solaris 11 (SPARC)	Y

Legend:
Y: Installed by default.

The following table lists the packages required when a monitored host's OS is AIX.

Table 3–9: Packages required for monitored host (for AIX)

No.	Software name	OS	Default
1	OpenSSH	AIX V6.1	N
2		AIX V7.1	N

Legend:
N: Not installed by default.

The following table lists the packages required when a monitored host's OS is Linux.

Table 3–10: RPM packages required for monitored hosts (for Linux)

No.	Software name	OS	Default
1	OpenSSH	CentOS 6 (x64) and CentOS 6 (x86)	--
2		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
3		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
4		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
5		Linux 6 (x64) and Linux 6 (x86)	Y
6		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
7		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--

Legend:
Y: Installed by default.
--: After installing the OS, make sure that the software or package is installed.

■ Packages required for monitored hosts (commands)

You can determine which packages are required for a monitored host by executing the appropriate command shown in the following table.

Table 3–11: Commands for determining the required packages and file sets

No.	OS	Command execution format
1	HP-UX	`/usr/sbin/swlist -l file | grep {`*command-name*`}`
2	Solaris 10	`/usr/sbin/pkgchk -l -p {`*command-name*`}`
3	Solaris 11 or later	`/usr/bin/pkg search -l -H -o pkg.name {`*command-name*`}`
4	AIX	`/usr/bin/lslpp - w {`*command-name*`}`
5	Linux	`/bin/rpm -q --whatprovides {`*command-name*`}`

The commands to be used and the packages are described below.

The following table lists the commands required for the records to be collected.

Table 3–12: Commands required for the records to be collected

No.	Record name	Command name			
		HP-UX	Solaris	AIX	Linux
1	• Application Process Count (PD_APPC) • Application Process Detail (PD_APPD) • Application Process Overview (PD_APS) • Application Service Overview (PD_ASVC) • Application Summary (PD_APP2)	• date • ps	• date • ps	• date • ps	• date • ps
2	Logical Disk Overview (PI_LDSK)	• date • df	• date • df	• date • df	• date • df
3	Network Interface Overview (PI_NET)	• date • netstat	• date • netstat	• date • netstat	• date • netstat
4	Physical Disk Overview (PI_PDSK)	• date • iostat • sar	• date • iostat	• date • sar	• date • iostat
5	Processor Overview (PI_CPU)	• date • sar	• date • mpstat	• date • mpstat • sar	• date • mpstat
6	System Status (PD)	• date • uname	• date • uname	• date • uname	• date • uname
7	System Summary (PI)	• crashconf • date • sar • swapinfo • uptime • vmstat	• date • mpstat • prtconf • sar • swap • uptime • vmstat	• date • mpstat • pstat • sar • uptime • vmstat	• date • free • mpstat • sar • uptime • vmstat

The table below lists the packages required for the records to be collected. For details, see the *Release Notes* for this product.

Table 3–13: Software required for monitored hosts (for HP-UX)

No.	Command name	OS	Default
1	crashconf	HP-UX 11i V3 (IPF)	Y
2	date	HP-UX 11i V3 (IPF)	Y
3	df	HP-UX 11i V3 (IPF)	Y
4	ioscan	HP-UX 11i V3 (IPF)	Y

No.	Command name	OS	Default
5	iostat	HP-UX 11i V3 (IPF)	Y
6	netstat	HP-UX 11i V3 (IPF)	Y
7	ps	HP-UX 11i V3 (IPF)	Y
8	sar	HP-UX 11i V3 (IPF)	Y
9	swapinfo	HP-UX 11i V3 (IPF)	Y
10	uname	HP-UX 11i V3 (IPF)	Y
11	uptime	HP-UX 11i V3 (IPF)	Y
12	vmstat	HP-UX 11i V3 (IPF)	Y

Legend:

Y: Installed by default.

Table 3–14: Packages required for monitored hosts (for Solaris)

No.	Command name	OS	Default
1	date	Solaris 10 (SPARC)	Y
2		Solaris 10 (x64)	Y
3		Solaris 10 (x86)	Y
4		Solaris 11 (SPARC)	Y
5	df	Solaris 10 (SPARC)	Y
6		Solaris 10 (x64)	Y
7		Solaris 10 (x86)	Y
8		Solaris 11 (SPARC)	Y
9	iostat	Solaris 10 (SPARC)	Y
10		Solaris 10 (x64)	Y
11		Solaris 10 (x86)	Y
12		Solaris 11 (SPARC)	Y
13	mpstat	Solaris 10 (SPARC)	Y
14		Solaris 10 (x64)	Y
15		Solaris 10 (x86)	Y
16		Solaris 11 (SPARC)	Y
17	netstat	Solaris 10 (SPARC)	Y
18		Solaris 10 (x64)	Y
19		Solaris 10 (x86)	Y
20		Solaris 11 (SPARC)	Y
21	pagesize	Solaris 10 (SPARC)	Y
22		Solaris 10 (x64)	Y
23		Solaris 10 (x86)	Y

No.	Command name	OS	Default
24	`pagesize`	Solaris 11 (SPARC)	Y
25	`prtconf`	Solaris 10 (SPARC)	Y
26		Solaris 10 (x64)	Y
27		Solaris 10 (x86)	Y
28		Solaris 11 (SPARC)	Y
29	`ps`	Solaris 10 (SPARC)	Y
30		Solaris 10 (x64)	Y
31		Solaris 10 (x86)	Y
32		Solaris 11 (SPARC)	Y
33	`sar`	Solaris 10 (SPARC)	Y
34		Solaris 10 (x64)	Y
35		Solaris 10 (x86)	Y
36		Solaris 11 (SPARC)	Y
37	`swap`	Solaris 10 (SPARC)	Y
38		Solaris 10 (x64)	Y
39		Solaris 10 (x86)	Y
40		Solaris 11 (SPARC)	Y
41	`uname`	Solaris 10 (SPARC)	Y
42		Solaris 10 (x64)	Y
43		Solaris 10 (x86)	Y
44		Solaris 11 (SPARC)	Y
45	`uptime`	Solaris 10 (SPARC)	Y
46		Solaris 10 (x64)	Y
47		Solaris 10 (x86)	Y
48		Solaris 11 (SPARC)	Y
49	`vmstat`	Solaris 10 (SPARC)	Y
50		Solaris 10 (x64)	Y
51		Solaris 10 (x86)	Y
52		Solaris 11 (SPARC)	Y

Legend:

Y: Installed by default.

Table 3–15: Packages required for monitored hosts (for AIX)

No.	Command name	OS	Default
1	`date`	AIX V6.1	Y
2		AIX V7.1	Y

No.	Command name	OS	Default
3	df	AIX V6.1	Y
4		AIX V7.1	Y
5	mpstat	AIX V6.1	Y
6		AIX V7.1	Y
7	netstat	AIX V6.1	Y
8		AIX V7.1	Y
9	ps	AIX V6.1	Y
10		AIX V7.1	Y
11	pstat	AIX V6.1	Y
12		AIX V7.1	Y
13	sar	AIX V6.1	Y
14		AIX V7.1	Y
15	uname	AIX V6.1	Y
16		AIX V7.1	Y
17	uptime	AIX V6.1	Y
18		AIX V7.1	Y
19	vmstat	AIX V6.1	Y
20		AIX V7.1	Y

Legend:

Y: Installed by default.

Table 3–16: Packages required for monitored hosts (for Linux)

No.	Command name	OS	Default
1	date	CentOS 6 (x64) and CentOS 6 (x86)	--
2		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
3		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
4		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
5		Linux 6 (x64) and Linux 6 (x86)	Y
6		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
7		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
8	df	CentOS 6 (x64) and CentOS 6 (x86)	--
9		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
10		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
11		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
12		Linux 6 (x64) and Linux 6 (x86)	Y
13		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--

No.	Command name	OS	Default
14	df	SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
15	free	CentOS 6 (x64) and CentOS 6 (x86)	--
16		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
17		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
18		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
19		Linux 6 (x64) and Linux 6 (x86)	Y
20		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
21		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
22	iostat	CentOS 6 (x64) and CentOS 6 (x86)	--
23		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	N
24		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	N
25		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	N
26		Linux 6 (x64) and Linux 6 (x86)	N
27		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
28		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
29	mpstat	CentOS 6 (x64) and CentOS 6 (x86)	--
30		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	N
31		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	N
32		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	N
33		Linux 6 (x64) and Linux 6 (x86)	N
34		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
35		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
36	netstat	CentOS 6 (x64) and CentOS 6 (x86)	--
37		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
38		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
39		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
40		Linux 6 (x64) and Linux 6 (x86)	Y
41		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
42		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
43	ps	CentOS 6 (x64) and CentOS 6 (x86)	--
44		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
45		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
46		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
47		Linux 6 (x64) and Linux 6 (x86)	Y
48		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--

No.	Command name	OS	Default
49	`ps`	SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
50	`uname`	CentOS 6 (x64) and CentOS 6 (x86)	--
51		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
52		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
53		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
54		Linux 6 (x64) and Linux 6 (x86)	Y
55		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
56		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
57	`uptime`	CentOS 6 (x64) and CentOS 6 (x86)	--
58		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
59		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
60		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
61		Linux 6 (x64) and Linux 6 (x86)	Y
62		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
63		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
64	`sar`	CentOS 6 (x64) and CentOS 6 (x86)	--
65		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	N
66		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	N
67		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	N
68		Linux 6 (x64) and Linux 6 (x86)	N
69		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
70		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--
71	`vmstat`	CentOS 6 (x64) and CentOS 6 (x86)	--
72		Linux 5 (IPF) and Linux 5 Advanced Platform (IPF)	Y
73		Linux 5 (x64) and Linux 5 Advanced Platform (x64)	Y
74		Linux 5 (x86) and Linux 5 Advanced Platform (x86)	Y
75		Linux 6 (x64) and Linux 6 (x86)	Y
76		Oracle Linux 6 (x64) and Oracle Linux 6 (x86)	--
77		SuSE Linux 11 (x64) and SuSE Linux 11 (x86)	--

Legend:

Y: Installed by default.

N: Not installed by default.

--: After installing the OS, make sure that the software or package is installed.

(c) SSH connection settings

Specify the SSH connection settings on both the PFM - RM host and the monitored hosts. For details about the SSH connection settings, see *3.1.6 SSH connection setting method for Windows (when the PFM - RM host is running Windows and the monitored host is running UNIX)*.

(7) Prerequisite when setting the process operation monitoring condition to 4,096 bytes

When using version 10-00 or later of PFM - Manager and PFM - Web Console, you can set the monitoring condition to be used for monitoring performance to a maximum of 4,096 bytes.

When installing PFM - Base or PFM - Manager on the PFM - RM host, use version 10-00 or later.

(8) Preparing to collect information when an error occurs

When a problem occurs, you might have to collect information such as memory dumps, crash dumps, and user-mode process dumps. If you want to collect these types of information when a problem occurs, enable the output of memory dumps, crash dumps, and user-mode process dumps before starting PFM - RM.

(a) Setting method in Windows Server 2003

- Memory dump output settings

1. From **Control Panel**, double-click **System**.
2. Under the **Advanced** tab, choose **Startup and Recovery**, and then click **Settings**.
3. Under **Write debugging information**, choose **Kernel memory dump**, and then specify an output destination file.

Note:

The memory dump size varies according to the size of the physical memory. If a large amount of physical memory is installed, the memory dump size will be large. Therefore, allocate a disk area that is large enough for collecting the memory dump. For details, see the documentation for the OS.

- Crash dump output settings

1. From the **Start** menu, choose **Run**.
2. Enter `drwtsn32` in the text box and click the **OK** button.

   The Dr. Watson for Windows dialog box appears.
3. Select the **Create Crash Dump File** check box and specify the output destination file in the **Crash Dump** text box.
4. Click the **OK** button.

Note:

The information that is output in a crash dump includes problem information on Job Management Partner 1 as well as other application programs. When a crash dump is output, it uses disk space. Therefore, when you are specifying that a crash dump is to be output, allocate sufficient disk space.

(b) Setting method in Windows Server 2008 or Windows Server 2012

- Output settings for user-mode process dump

By entering the following registry, you can instantly collect user-mode process dump for investigation purposes if an application program terminates abnormally:

```
\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting
\LocalDumps
```

Specify the following registry values in the registry key:

- `DumpFolder : REG_EXPAND_SZ` <*dump-output-destination-folder-name*>
  (You must have permissions to write data to the output destination folder.)
- `DumpCount : REG_DWORD` <*number-of-dumps-to-be-saved*>
- `DumpType : REG_DWORD 2`

Note:

- Setting up this registry entry enables you to output user-mode process dumps in Job Management Partner 1 as well as other application programs. Be aware of this point when deciding to output user-mode process dump.
- When a user-mode process dump is output, it uses disk space. Therefore, when you decide to output user-mode process dump, make sure that sufficient disk space is allocated to the specified dump output destination folder.

3.1.2 Flow of installation and setup for the Windows edition

This subsection describes the procedures for installing and setting up PFM - RM for Platform.

For details about how to install and set up PFM - Manager and PFM - Web Console, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The following figure shows the procedures for installing and setting up PFM - RM for Platform.

Figure 3–3: Installation and setup procedures (for Windows)

Note:

These procedures are applicable when PFM - RM for Platform is installed on a host other than the PFM - Manager host.

For setup commands that require a user input, you can choose whether to execute the commands in the interactive or non-interactive mode.

When a command is executed in the interactive mode, the user must enter a value by following the instruction from the command.

When a command is executed in the non-interactive mode, no user input is required because an option specification or a definition file replaces the input step required during command execution. Furthermore, batch processing or remote execution can automate the setup procedure, thereby reducing the workload on the administrator and the cost of operations.

For details about commands, see the manual *Job Management Partner 1/Performance Management Reference*.

3.1.3 Installation procedure for the Windows edition

This subsection describes how to install PFM - RM for Platform in a Windows environment.

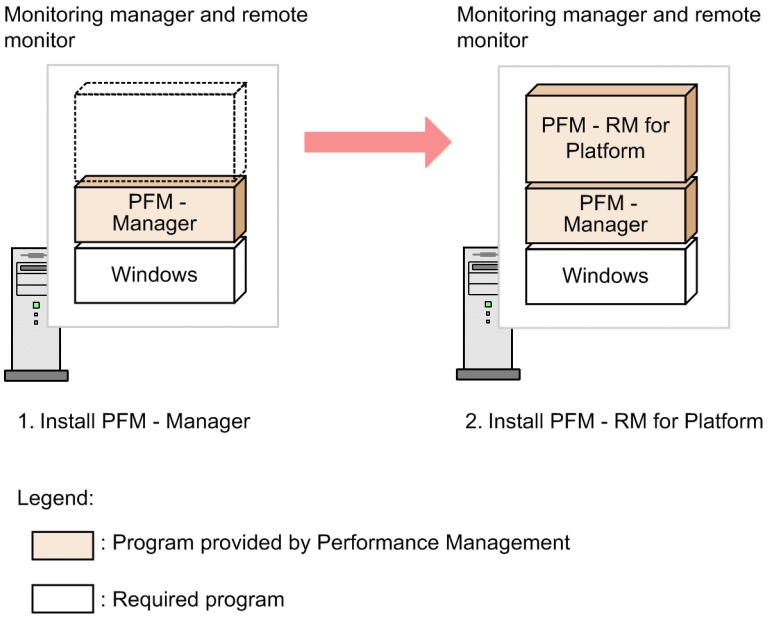
(1) Program installation sequence

This subsection describes the order in which PFM - RM for Platform and its prerequisite programs are to be installed.

When installing PFM - RM for Platform on the PFM - Manager host

Install PFM - Manager first, and then install PFM - RM for Platform.

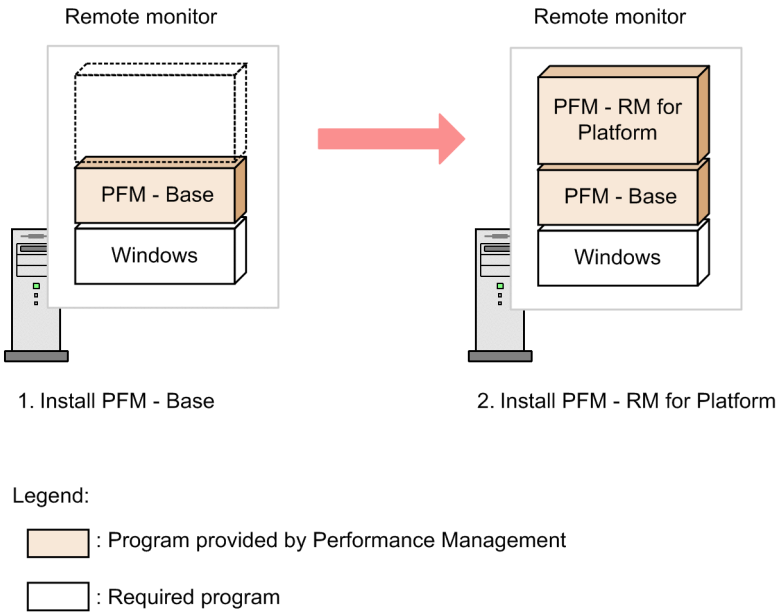
Figure 3–4: Program installation sequence (when PFM - RM for Platform and PFM - Manager are on the same host (for Windows))



When installing PFM - RM for Platform on a host other than the PFM - Manager host

Install PFM - Base first, and then install PFM - RM for Platform.

Figure 3–5: Program installation sequence (when PFM - RM for Platform and PFM - Base are on the same host (for Windows))



If you install multiple PFM - RMs on the same host, you can install the individual PFM - RMs in any order.

(2) Installation procedure

This subsection describes how to install PFM - RM for Platform.

There are two ways to install PFM - RM for Platform in a Windows environment: by using the distribution media or by using JP1/Software Distribution for remote installation. For details about the method that uses JP1/Software Distribution, see the *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

Note regarding all operating systems

If any Performance Management programs and services are running on the host where the program is to be installed, stop all the active programs and services. For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

Note regarding installation in a Windows Server 2008 or Windows Server 2012 environment

If user account control functionality (UAC) is enabled on the operating system, the User Account Control dialog box might be displayed during installation. If this dialog box is displayed, click the **Continue** button to continue installation, or click the **Cancel** button to cancel installation.

To install from the distribution media:

1. At the host where PFM - RM for Platform is to be installed, log on as a user with Administrator permissions.

2. Stop all services of Performance Management programs that are running.

   If any services of Performance Management programs are running, stop all of them.

   Note concerning the services to be stopped

   You must stop all Performance Management services on physical and logical hosts. For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3. Insert the distribution media into the appropriate drive.

   The installer starts. Install the program by entering necessary information, in accordance with the installer's instructions.

   Note:

   You can specify a desired Performance Management program installation folder the first time you install each Performance Management program on the target host; the exception to this capability is for PFM - Web Console.

   During any subsequent installation procedure, the installation folder specified during the initial installation is assumed.

3.1.4 Setup procedure for the Windows edition

This subsection describes how to set up PFM - RM for Platform.

Optional indicates the following setup items:

- Setup item required depending on the environment in use
- Setup item for changing a default setting

(1) Registering PFM - RM for Platform

To achieve central management of PFM - RM for Platform in the Performance Management system, you must register PFM - RM for Platform into PFM - Manager and PFM - Web Console.

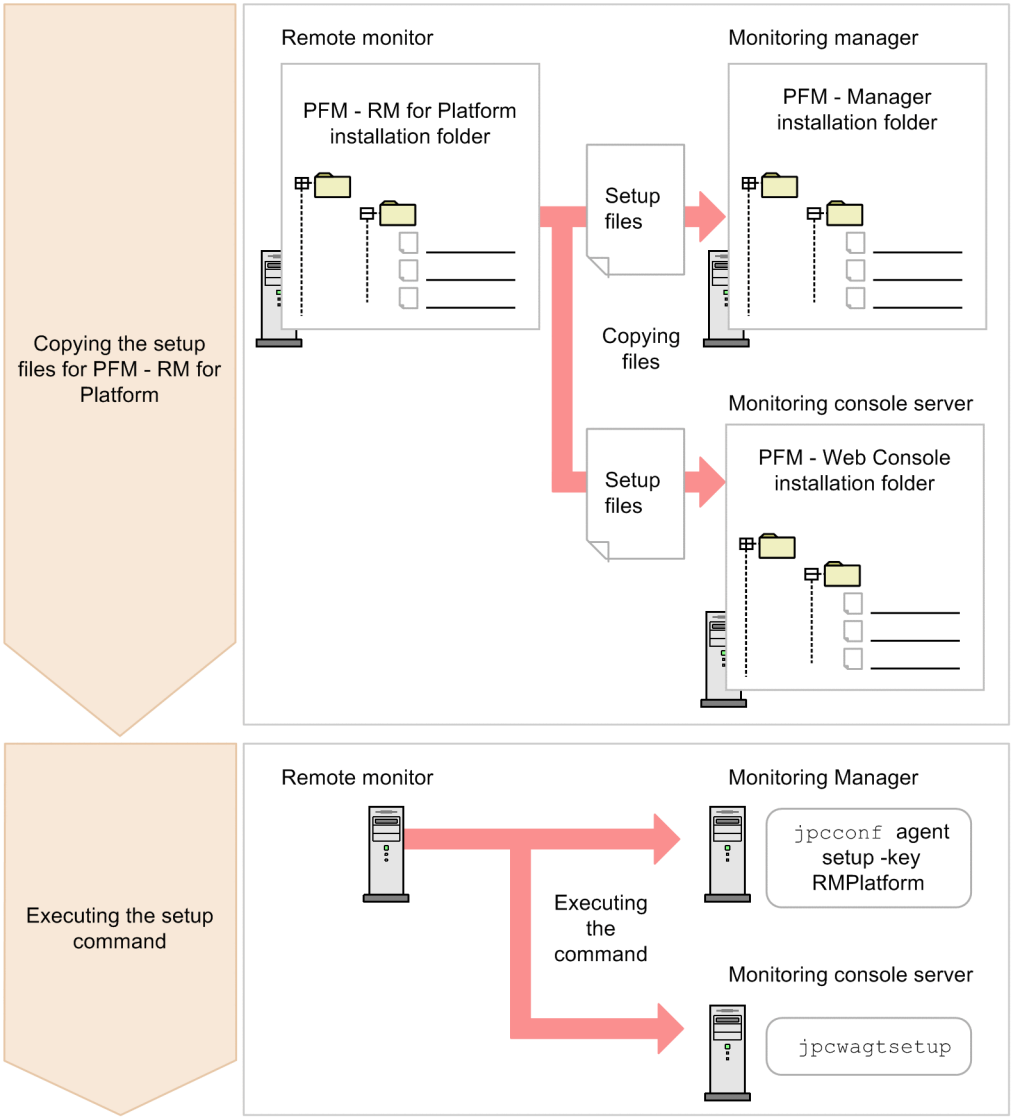
You must register PFM - RM for Platform at the following times:

- Whenever you add a new PFM - RM for Platform to the Performance Management system.

  Note: If a PFM - RM for Platform has already been registered and you are adding a new PFM - RM for Platform of the same version, there is no need to register the new PFM - RM for Platform.
- When you update the Data model version for the registered PFM - RM for Platform.

The following figure shows the procedure for registering PFM - RM for Platform.

Figure 3–6: Procedure for registering PFM - RM for Platform (for Windows)



Notes about registering PFM - RM for Platform

- Register PFM - RM for Platform before you set up an instance environment.
- If you install different versions of PFM - RM for Platform on separate hosts, set up old versions before you set up new versions.
- If you install PFM - RM for Platform on the same host as where PFM - Manager is installed, the `jpcconf agent setup` command executes automatically.
- When PFM - RM for Platform is registered, folders named `RM Platform` are created on the **Reports** and **Alarms** pages of PFM - Web Console. If you have already created a folder or file named `RM Platform` on the **Reports** page, you must rename it before starting the registration procedure.

The following subsections describe how to register PFM - RM for Platform.

(a) Copying the setup files for PFM - RM for Platform

Copy the setup files from the PFM - RM host to the hosts where PFM - Manager and PFM - Web Console are installed.

To copy the setup files:

1. Stop PFM - Web Console.
   If PFM - Web Console is running, stop it.

2. Copy the setup files in the binary mode.
   Copy the files from the PFM - RM host to the PFM - Manager and PFM - Web Console hosts.
   The following table lists the source file storage locations and the copy destination locations.

Table 3–17: Setup files to be copied (for Windows)

No.	Source (setup files for PFM - RM for Platform)	Target		
		Program name	OS	Target folder
1	*installation-folder*\setup\jpcagt7w.EXE	PFM - Manager	Windows	*PFM-Manager-installation-folder*\setup
2	*installation-folder*\setup\jpcagt7u.Z		UNIX	/opt/jp1pc/setup/
3	*installation-folder*\setup\jpcagt7w.EXE	PFM - Web Console	Windows	*PFM-Web-Console-installation-folder*\setup
4	*installation-folder*\setup\jpcagt7u.Z		UNIX	/opt/jp1pcwebcon/setup/

(b) Executing the setup command at the PFM - Manager host

At the PFM - Manager host, execute the setup command for PFM - RM for Platform.

Execute the following command:

```
jpcconf agent setup -key RMPlatform
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf agent setup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Notes about executing the command

Before you execute the command, stop all Performance Management programs and services. An error might occur if the `jpcconf agent setup` command is executed before all Performance Management programs and services have stopped completely. If an error has occurred, re-execute the `jpcconf agent setup` command.

After you have executed the setup command at the PFM - Manager host, you might delete the setup files for PFM - RM for Platform that were copied to the PFM - Manager.

(c) Executing the setup command at the PFM - Web Console host

At the PFM - Web Console host, execute the setup command for PFM - RM for Platform.

Execute the following command:

```
jpcwagtsetup
```

After you have executed the setup command at the PFM - Web Console host, you might delete the setup files for PFM - RM for Platform that were copied to the PFM - Web Console.

(2) Setting up an instance environment

Set up an instance environment for PFM - RM for Platform on the PFM - RM host. To set up multiple instance environments, repeat this procedure. With PFM - RM for Platform, you can define a maximum of 50 monitoring targets in a single instance environment.

Monitored hosts running Windows and those running UNIX can coexist within a single instance.

Using common account information in an instance environment

If you specify `Y` for the `UseCommonAccount` instance environment setting item, common account information (pfmhost) that was created beforehand for the instance environment is used.

The following table lists the correspondence between instance environment setting items and common account information setting items.

Table 3–18: Correspondence between instance environment setting items and common account information setting items

Instance environment setting item	Common account information (pfmhost) setting item	Description
`RMHost_User`	`User`	User name
`RMHost_Password`	`Password`	Password
`RMHost_Domain`	`Domain`	Domain name

Note 1:

Common account information can only be used in an environment where both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

Note 2:

Common account information must be created on the PFM - RM host beforehand. Use the `jpcconf acc setup` command to create common account information. For details about the `jpcconf acc setup` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Note 3:

The settings and precautions required for creating common account information (pfmhost) are the same as for the corresponding instance environment setting items. See the corresponding instance environment setting items in Table 3-20.

Notes about setting up instance environments

- Before you set up an instance environment, make sure that the applicable procedure described in one of the following sections has been completed and the correct environment has been set up:

  - *3.1.1(5) Environment settings required for collecting performance data (when both the PFM - RM host and the monitored hosts are running Windows)*

  - *3.1.1(6) Environment settings required for collecting performance data (when the PFM - RM host is running Windows and the monitored hosts are running UNIX)*

- Even if an invalid value is specified in the instance environment settings, the command for generating an instance environment terminates normally. However, if you begin collecting records with invalid settings, performance data is not collected. For details about troubleshooting when performance data is not collected, see *9.2.5(3) PFM - RM for Platform was started, but no performance data is being collected*.

(a) Instance environment setting items that must be specified depending on the OS of the monitored host in the instance

The instance environment setting items that must be specified differ depending on the OS of the monitored host in the instance. The following table lists and describes the instance environment setting items that must be specified for each OS of the monitored hosts in the instance.

Table 3–19: Instance environment setting items that must be specified for each OS of the monitored hosts in the instance

Item name	OS of the monitored hosts in the instance		
	Windows environment only	UNIX environment only	Windows and UNIX environments coexist
`UseCommonAccount`	D	D	D
`Interval`	D	D	D
`Std_Category`	D	D	D
`Disk_Category`	D	D	D
`Network_Category`	D	D	D
`Ps_Category`	D	D	D
`RMHost_User`	Y	Y	Y
`RMHost_Password`	Y	Y	Y
`RMHost_Domain`	D	D	D
`SSH_Client`	N	Y	Y
`Perl_Module`	N	Y	Y
`Log_Size`	D	D	D

Legend:

Y: Specification is required.

D: Specification is required if the default value is to be changed.

N: Specification is not required.

(b) Instance environment setting items and values

The table below lists and describes the instance environment setting items and values. Check this information before you start operations.

Use the `jpcconf inst setup` command to set up an instance environment.

For details about how to execute the `jpcconf inst setup` command, see *(d) Execution in the interactive mode* and *(e) Execution in the non-interactive mode*.

For details about the `jpcconf inst setup` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Table 3–20: Instance environment setting items and values for PFM - RM for Platform (for Windows)

No.	Item name#1	Description	Setting	Default
1	`UseCommonAccount`	Specifies whether to use common account information.	Specify one of the following values:	`N`

No.	Item name[#1]	Description	Setting	Default
1	UseCommonAccount	Specifies whether to use common account information.	• Y: Use • N: Do not use	N
2	Interval	Specifies a collection interval for the collection process.	Specify a value in the range from 60 to 3,600 (seconds).	300
3	Std_Category[#2]	Specifies whether the collection process is to collect basic information (PI and PI_CPU records).	Specify one of the following values: • Y: Collect • N: Do not collect	Y
4	Disk_Category[#2]	Specifies whether the collection process is to collect disk information (PI_PDSK and PI_LDSK records).	Specify one of the following values: • Y: Collect • N: Do not collect	Y
5	Network_Category[#2]	Specifies whether the collection process is to collect network information (PI_NET record).	Specify one of the following values: • Y: Collect • N: Do not collect	Y
6	Ps_Category[#2]	Specifies whether the collection process is to collect process information (PD_APS, PD_ASVC, PD_APP2, PD_APPC, and PD_APPD records).	Specify one of the following values: • Y: Collect • N: Do not collect	Y
7	RMHost_User[#3]	Specifies the user account[#4] used on the PFM - RM host.	From 1 to 256 bytes of characters can be specified. The tab character cannot be used.	--
8	RMHost_Password	Specifies the password for the account used on the PFM - RM host. The characters entered in this item are not displayed on the screen. If you specify this password, you are prompted to confirm the password by entering it again.	From 1 to 256 bytes of characters can be specified. The tab character cannot be used.	--
9	RMHost_Domain[#5]	Specifies the domain name to which the account used on the PFM - RM host belongs. There is no need to specify this item if the account belongs to a workgroup.	From 0 to 256 bytes of characters can be specified. The tab character cannot be used.	No domain name is specified.
10	SSH_Client[#5]	Specifies an absolute path for the execution module (plink.exe) of the SSH client (PuTTY). Even if the file path contains a space, there is no need to enclose the file path in double quotation marks (")). There is no need to specify this item if all of the monitored hosts in the instance are only running Windows.	From 0 to 256 bytes of characters can be specified. The tab character cannot be used.	No SSH client execution module is specified.
11	Perl_Module[#5]	Specifies an absolute path for the execution module (perl.exe) of Perl (ActivePerl). Even if the file path contains a space, there is no need to enclose the file path in double quotation marks (")). There is no need to specify this item if all of the monitored hosts in the instance are only running Windows.	From 0 to 256 bytes of characters can be specified. The tab character cannot be used.	No Perl execution module is specified.
12	Log_Size	Specifies the maximum size of one agent log file. [#7]	Specify a value in the range from 1 to 32 (megabytes).	3

Legend:

--: No default is set.

#1

When the `jpcconf inst setup` command is executed in the non-interactive mode, this item name is used as a product-specific label in the definition file. For details about commands in the non-interactive mode, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

#2

The settings for `Std_Category`, `Disk_Category`, `Network_Category`, and `Ps_Category` are given higher priority than the collection settings for the individual records.

For example, if you set `Std_Category` to `N` (do not collect), a PI record is handled as follows:

- The PI record information is not recorded in the Store database.

- If an attempt is made to display a real-time report based on PI records from the PFM - Web Console, the `KAVJS5001-I` error message is displayed.

- If an alarm is bound to a PI record, that alarm does not function.

#3

PFM - RM for Platform starts the collection process by using the user account specified in `RMHost_User`. When adding or modifying an instance environment, you need to create a new user account and specify it for `RMHost_User`. However, if a profile for the newly created user account already exists, collection of performance data might fail. In such a case, log on to Windows again by using the newly created user account.

If the system is being run with enhanced file permissions, the user specified for `RMHost_User` must belong to the PFM operation group. For details about operations with enhanced file permissions, see the chapter that describes file permission enhancement in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

If the local host is specified as a monitored host and the following two conditions are satisfied, specify the local account's Built-in Administrator for `RMHost_User` in the instance settings.

- The OS of the PFM - RM host is Windows Server 2008 or Windows Server 2012.

- The PFM - RM host's user account control functionality (UAC) is enabled.

Note that the following check boxes in the **General** tab of the **Administrator Properties** window must not be selected:

- **User must change password at next logon**

- **Account is disabled**

These notes also apply when `User` in common account information (pfmhost) is used. In this case, read these notes with `User` replacing `RMHost_User` in common account information (pfmhost).

#4

If you run PFM - RM for Platform in a cluster system, specify an account that can log on to both the active node and the standby node by using the same user name and password.

This also applies when `User` is used in the common account information (pfmhost).

#5

If both of the following conditions are met when the local host is monitored, specify the local host name for `RMHost_Domain`:

- The PFM - RM host is running Windows Server 2008.

- The PFM - RM host is a participant in a domain.

#6

You must specify this item if the instance includes a monitored host running UNIX. Additionally, when operating PFM - RM for Platform in a cluster system, specify a file path that can be accessed from both the active server and the standby server.

#7

Use the following formula for estimating the agent log size:

agent-log-size (megabytes) = ((*a* **x** 24 **x** 3,600) / *b* **x** 4) / (4 **x** 1,024)

Legend:

a: Number of days to retain the agent log

b: Instance interval value

In the agent log, a maximum of (16 + *number-of-monitoring-targets* **x** 4) files are collected per instance.

If the hard disk does not have sufficient free space, the agent log generates an output error. For details about the agent log, see *9.3 Log information to be collected for troubleshooting*.

(c) Instance environment setting items that are not displayed

Instance environment setting items are usually displayed by executing a command, but some might not be displayed depending on the contents of other setting items or for some other reason. The table below lists and describes conditions that prevent instance environment setting items from being displayed. It also shows the input values that are used in such cases.

Table 3–21: Conditions that prevent instance environment setting items from being displayed, and input values that are used

Item name	Conditions that prevent instance environment setting items from being displayed, and input values that are used
`UseCommonAccount`	This item is not displayed in an environment where common account information cannot be used.
`RMHost_User`	These items are not displayed when `Y` is specified for `UseCommonAccount` in an environment where common account information can be used. Input value: The value in the corresponding common account information is used as the input value. For details about the corresponding common account information, see Table 3-18.
`RMHost_Password`	
`RMHost_Domain`	

Note:

Here, *an environment where common account information can be used* refers to an environment where both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

(d) Execution in the interactive mode

1. Execute the `jpcconf inst setup` command.

   The following example sets up an instance environment using `inst1` as the instance name:

```
jpcconf inst setup -key RMPlatform -inst inst1
```

2. Set up an instance environment for PFM - RM for Platform.

   Enter each instance environment setting item for PFM - RM for Platform according to the instructions given by the command. For details about each instance environment setting item, see Table 3-20. After you input each setting item, press the **Enter** key. To use a displayed default value, simply press the **Enter** key.

   The following is a setting example in which the instance includes a monitored host running UNIX:

```
C:\Program Files\Hitachi\jp1pc\tools>jpcconf inst setup -key RMPlatform -
inst inst1
 UseCommonAccount#1   [N]                  :<Enter>
 Interval             [300]                :<Enter>
 Std_Category         [Y]                  :<Enter>
 Disk_Category        [Y]                  :<Enter>
 Network_Category     [Y]                  :<Enter>
 Ps_Category          [Y]                  :<Enter>
 RMHost_User#2                             :rmuser<Enter>
 RMHost_Password#2                         :rmpass#3<Enter>
 Re-enter#2                                :rmpass#3<Enter>
 RMHost_Domain#2      []                   :<Enter>
 SSH_Client           [] :C:\Program Files\PuTTY\plink.exe#4<Enter>
 Perl_Module          [] :C:\Perl\bin\perl.exe#4<Enter>
 Log_Size (MB)        [3]                  :<Enter>
KAVE05080-I The instance environment is now being created.
(servicekey#5=RMPlatform, inst=inst1)
```

```
KAVE05081-I The instance environment has been created.
(servicekey#5=RMPlatform, inst=inst1)
```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

This item is not displayed when `Y` is specified for `UseCommonAccount`.

#3

Re-entry of the password is prompted. The entered password is not displayed on the screen.

#4

Enter this line if the instance includes monitored hosts running UNIX. There is no need to enter this line if all monitored hosts in the instance are running Windows.

#5

If the PFM - Manager's product name display function is disabled, `agt7` is displayed for `servicekey`.

(e) Execution in the non-interactive mode

1. Execute the `jpcconf inst setup` command to create a definition file template.

   Execute the command as follows:

   ```
   jpcconf inst setup -key RMPlatform -noquery -template definition-file-name
   ```

   Sections and labels that correspond to the instance environment setting items are output to a definition file. Note that the label of the `Instance Definitions` section is left blank.

2. Edit the definition file template created in step 1.

   Edit the setting values as required for the instance environment.

   For details about the product-specific labels to be specified in the definition file, see Table 3-20.

   Shown below is an example of a definition file for an instance environment in which the instance includes monitored hosts running UNIX. Specify values for the labels in the `Instance Definitions` section as required for the instance environment.

   ```
   [Common Definitions]
   Definition File Version=0001

   [Product Information]
   Product ID=7

   [Instance Definitions]
   UseCommonAccount#1=
   Interval=
   Std_Category=
   Disk_Category=
   Network_Category=
   Ps_Category=
   RMHost_User#2=rmuser
   RMHost_Password#2=rmpass
   RMHost_Domain#2=
   SSH_Client= C:\Program Files\PuTTY\plink.exe#3
   Perl_Module= C:\Perl\bin\perl.exe#3
   Log_Size=
   ```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

There is no need to specify values for these items if `Y` is specified for `UseCommonAccount`.

#3

Enter this line if the instance includes monitored hosts running UNIX. There is no need to enter this line if all monitored hosts in the instance are running Windows.

3. Execute the `jpcconf inst setup` command to set up an instance environment for PFM - RM for Platform.

   The following example sets up an instance environment using `inst1` as the instance name. For the `-input` option, specify the definition file edited in step 2.

```
jpcconf inst setup -key RMPlatform -inst inst1 -noquery -input definition-file-name
```

Note:

If the definition file contains confidential information such as passwords, save the definition file in a secure location, and delete it after you have used it. If you want to transfer the definition file between hosts, we recommend that you use a secure file transfer protocol, such as Secure File Transfer Protocol (SFTP), which is FTP over an SSH tunnel.

When all of the settings have been completed, an instance environment can be built. The following table shows the folder structure of an instance environment.

Table 3–22: Folder structure of an instance environment (for Windows)

No.	Storage folder	File name	Description
1	*installation-folder*[#1]`\agt7\agent\`*instance-name*	`jpcagt.ini`	Service startup initialization file of Remote Monitor Collector
2		`jpcagt.ini.lck`	Lock file for the service startup initialization file of Remote Monitor Collector (for each instance)
3		`jpcagt.ini.model`[#2]	Sample of a service startup initialization file of Remote Monitor Collector
4		`status.dat`	Intermediate file for internal processing
5		`tstatuses.dat`	Virtual Agent status information[#3]
6		`targetlist.ini`	List of monitoring targets
7		`grouplist.ini`	List of groups
8		`GARULES.DAT`	Grouping rule description file
9		`targets`	Storage folder for remote agent
10		`groups`	Storage folder for group agent
11		`log`	Storage folder for log files
12	*installation-folder*[#1]`\agt7\store\`*instance-name*	`*.DB`	Performance data file
13		`*.IDX`	Index files for performance data files
14		`*.LCK`	Lock files for performance data files
15		`jpcsto.ini`	Service startup initialization file of Remote Monitor Store

No.	Storage folder	File name	Description
16	*installation-folder*#1`\agt7\store\`*instance-name*	`jpcsto.ini.model`#2	Model file for the service startup initialization file of Remote Monitor Store
17		`status.dat`	Intermediate file for internal processing
18		`*.DAT`	Definition file for a data model
19		`dump`	Export folder
20		`backup`	Backup folder
21		`partial`	Partial backup folder
22		`import`	Import folder
23		`log`	Storage folder for log files

#1

If you run a logical host, replace *installation-folder* with *environment-folder*`\jp1pc`. An environment folder is a folder on the shared disk that is specified when the logical host is created.

#2

Use these sample files when you want to restore the settings to their initial values from when the instance environment was configured.

#3

Created when the health check function is enabled.

To change an instance environment, re-execute the `jpcconf inst setup` command, and then update each instance environment setting. For details about updating the instance environment settings, see *3.6.2 Updating an instance environment*.

You can change some settings by using PFM - Web Console to edit properties. For details about the information that can be changed by editing properties, see *E.1 List of properties of the Remote Monitor Store service*.

In an instance environment, the service IDs and Windows service names are as follows:

Service IDs in an instance environment

- For the Remote Monitor Collector service
  `7A`*instance-number instance-name*`[`*host-name*`]`
- For the Remote Monitor Store service
  `7S`*instance-number instance-name*`[`*host-name*`]`
- For the Group Agent service
  `7A`*instance-number instance-name*`[All@`*host-name*`]`

In PFM - RM for Platform, the instance name specified in the `jpcconf inst setup` command is displayed.

If the host name of the PFM - RM host is `host1`, and `inst1` is specified as the instance name, the service IDs will be as follows:

- For the Remote Monitor Collector service
  `7A1inst1[host1]`
- For the Remote Monitor Store service
  `7S1inst1[host1]`
- For the Group Agent service
  `7A1inst1[All@host1]`

For details about the service IDs, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Windows service names in an instance environment

- For the Remote Monitor Collector service

  `PFM - RM for Platform` *instance-name*

- For the Remote Monitor Store service

  `PFM - RM Store for Platform` *instance-name*

If `inst1` is specified as the instance name, the service names will be as follows:

- For the Remote Monitor Collector service

  `PFM - RM for Platform inst1`

- For the Remote Monitor Store service

  `PFM - RM Store for Platform inst1`

For details about the Windows service names, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. For details about the Windows service names when a logical host is used for operation, see the chapter that describes cluster system configuration and operation in the *Job Management Partner 1/Performance Management User's Guide*.

You cannot set up an instance environment by using PFM - Web Console's facility to distributing agent-specific properties.

(3) Setting the monitored host

Set information about the monitored host for the instance specified in *(2) Setting up an instance environment*. You can set a maximum of 50 monitored hosts for a single instance. To set multiple monitored hosts, repeat this procedure. However, if the number of monitored hosts is large, the desired performance might not be achieved depending on the machine's performance and environment. In such a case, reduce the number of monitored hosts. Carefully validate performance before starting operations.

You must specify physical hosts as monitoring targets. PFM - RM for Platform does not support monitoring of logical hosts.

Using common account information for monitored hosts

If `Y` is set for `UseCommonAccount` in the setting items for the monitored host, common account information (wmi or ssh) that is created beforehand for the monitored host is used.

The type of the common account information to be used differs depending on whether the OS of the monitored host is Windows or UNIX. The following table lists the correspondence between the OS of the monitored host and the type of common account information.

Table 3–23: Correspondence between the OS of the monitored host and the type of common account information

OS of the monitored host	Type of common account information
Windows	wmi
UNIX	ssh

The following tables list the correspondence between the setting items for the monitored host and those for common account information.

Table 3–24: Correspondence between the setting items for the monitored host and those for common account information (when the OS of the monitored host is Windows)

Setting items for the monitored host	Setting items for common account information (wmi)	Description
`User`	`User`	User name
`Password`	`Password`	Password
`Domain`	`Domain`	Domain name

Table 3–25: Correspondence between the setting items for the monitored host and those for common account information (when the OS of the monitored host is UNIX)

Setting items for the monitored host	Setting items for common account information (ssh)	Description
`User`	`User`	User name
`Private_Key_File`	`Private_Key_File`	Private key file name

Note 1:

Common account information can only be used in an environment where both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

Note 2:

Common account information must be created on the PFM - RM host beforehand. Use the `jpcconf acc setup` command to create common account information. For details about the `jpcconf acc setup` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Note 3:

The settings and precautions required for creating common account information (wmi or ssh) are the same as for the corresponding monitoring target setting items. See the corresponding monitoring target setting items in Table 3-27.

Important note

To use common account information, you need to unify the account information settings so that you can connect to multiple monitoring targets by using a single set of account information. For this reason, there is a risk of greater negative impact if common account information is leaked. To avoid such a risk, determine whether to use common account information after considering security measures and information management.

Notes about setting a monitored host

- Before you set up a monitored host, make sure that the applicable procedure in one of the following sections has been completed and the correct environment has been set up:

  - *3.1.1(5) Environment settings required for collecting performance data (when both the PFM - RM host and the monitored hosts are running Windows)*

  - *3.1.1(6) Environment settings required for collecting performance data (when the PFM - RM host is running Windows and the monitored hosts are running UNIX)*

- Even if an invalid value is specified in the monitored host settings, the command for generating a monitoring target terminates normally. However, if you begin collecting records with invalid settings, performance data will not be collected. For details about troubleshooting when performance data is not collected, see *9.2.5(3) PFM - RM for Platform was started, but no performance data is being collected*.

(a) Monitoring target setting items that must be specified depending on the OS type

The monitoring target setting items that must be specified differ depending on the OS of the monitored host. The following table lists and describes these monitoring target setting items.

Table 3–26: Monitoring target setting items that depend on the OS of the monitored host

Item name	OS of the monitored host	
	Windows environment	UNIX environment
`Target Host`	Y	Y
`UseCommonAccount`	D	D
`TargetType`	T	Y
`User`	Y	Y
`Password`	Y	N
`Domain`	D	N
`Private_Key_File`	N	Y
`Port`	N	D

Legend:

Y: Specification is required.

D: Specification is required if the default value is being changed.

T: There is no need to change the default value.

N: Specification is not required.

(b) Monitoring target setting items and values

The table below lists and describes the setting items and values for a monitored host. Check this information before you start operations.

Use the `jpcconf target setup` command to set up a monitored host.

For details about how to execute the `jpcconf target setup` command, see *(d) Execution in the interactive mode* and *(e) Execution in the non-interactive mode*.

For details about the `jpcconf target setup` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Table 3–27: Setting items and values for a monitored host in PFM - RM for Platform

No.	Item name[#1]	Description	Setting	Default
1	`Target Host`	Specifies the name of the monitored host. Specify a host name that can be resolved.[#2] The specified monitored host name is used during performance data collection and health checking. If JP1/IM or NNM is linked, this name is also used as the event host name.	From 1 to 32 bytes of alphanumeric characters and the hyphen (-) are permitted. The name cannot begin with a hyphen (-). The specified value must be unique within the instance.[#3]	No monitored host name is specified.[#4]
2	`UseCommonAccount`	Specifies whether to use common account information.	Specify one of the following values: • `Y`: Use • `N`: Do not use	`N`
3	`TargetType`	Specifies the method for connecting to the monitored host.	• Specify `wmi` if the monitored host is running Windows.	`wmi`

No.	Item name#1	Description	Setting	Default
3	`TargetType`	The value to be specified differs depending on whether the monitored host is running Windows or UNIX.	• Specify `ssh` if the monitored host is running UNIX.	`wmi`
4	`User`	Specifies the user#5, #6 used to connect to the monitored host.	From 1 to 256 bytes of characters are permitted. The tab character is not permitted.	--
5	`Password`#7	Specifies the password used to connect to the monitored host. The characters entered in this item are not displayed on the screen. When the password is specified, re-entry of the password is requested. There is no need to specify this item if the monitored host is running UNIX.	From 0 to 256 bytes of characters are permitted. The tab character is not permitted.	No password is specified.
6	`Domain`	Specifies the name of the domain#8 to which the monitored host belongs. There is no need to specify this item if the monitored host belongs to a work group. There is no need to specify this item if the monitored host is running UNIX.	From 0 to 256 bytes of characters are permitted. The tab character is not permitted.	No domain name is specified.
7	`Private_Key_File`#9	Specifies an absolute path for the name of the private key file used in the SSH public key method. Even if the file path contains a space, there is no need to enclose the file path in double quotation marks (`"`). There is no need to specify this item if the monitored host is running Windows.	From 0 to 256 bytes of characters are permitted. The tab character is not permitted.	A private key file name is not specified.
8	`Port`	Specifies the port number of the SSH server on the monitored host. This item is not used if the monitored host is running Windows. In this case, leave the default value.	1 to 65,535	`22`

Legend:

--: No default is set.

#1

When the `jpcconf target setup` command is executed in the non-interactive mode, this item name is used as a product-specific label in the definition file. For details about commands in the non-interactive mode, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

#2

To collect performance data and perform health checking, the name must be resolvable at least by the PFM - RM host.

If the JP1/IM linkage facility is used, the name must be resolvable by the JP1/IM host. If the NNM linkage facility is used, the name must be resolvable by both the PFM - Manager host and the NNM host.

#3

`All` cannot be used because it is a reserved word for group agents.

#4

If the specification is omitted, the host name of the PFM - RM host is assumed.

#5

If the monitored host is running Windows, the specified user must be a member of the monitored host's Administrators group, Performance Log Users group, or Performance Monitor Users group.

To perform operations such as Windows security audit, you also need permissions to execute such operations.

The type of records that can be collected differs according to the account type. For details about various account types and whether records can be collected, see *3.1.1(5)(a) Setting the user accounts*.

If the monitored host is running Windows, note that the following check boxes in the **General** tab of the **Administrator Properties** window must not be selected:

- User must change password at next logon

- Account is disabled

In addition, if the monitored host specifies a domain user in an Active Directory environment, click the **Account** tab for that user, and then click the **Log On To** button to display the **Logon Workstations** window. In the **Logon Workstations** window, make sure that one of either of the conditions listed below exists there:

- The **All computers** option is selected.

- The **following computers** option is selected, and the host name of the monitored host is already registered.

If the monitored host resides in a work group environment, execute the `gpedit.msc` command to display the **Local Computer Policy** window, and select **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, and then **Security Options**. Then, make sure that the **Network access: Sharing and security model for local accounts** option is set to **Classic - local users authenticate as themselves**.

These notes also apply when `User` in common account information (wmi) is used.

#6

When the monitored host is running UNIX, use `bash`, `bsh`, or `ksh` for the login shell of the user to be specified.

This also applies when `User` in common account information (ssh) is used.

#7

This item is required if the monitored host is running Windows.

This also applies when `Password` in common account information (wmi) is used.

#8

When monitoring the local host, specify a local host name if all of the following conditions are satisfied:

- The PFM - RM host is running Windows Server 2008 or Windows Server 2012.
- The PFM - RM host is a participant in a domain.
- The user of the PFM - RM host is used for connecting to the monitored host.

This also applies when `Domain` in common account information (wmi) is used. When using common account information, specify the local host name for `Domain` in common account information (wmi).

#9

This item is required if the monitored host is running UNIX.

Also, when operating PFM - RM for Platform in a cluster system, specify a file path that can be accessed from both the active server and the standby server.

This also applies when `Private_Key_File` in common account information (ssh) is used.

(c) Monitored host setting items that are not displayed

Monitored host setting items are usually displayed by executing a command, but some are not displayed depending on the contents of other setting items or for some other reason. The table below describes conditions that prevent monitored host setting items from being displayed. It also shows the input values that are used in such cases.

Table 3–28: Conditions that prevent monitored host setting items from being displayed, and input values that are used

Item name	Conditions that prevent monitored host setting items from being displayed, and input values that are used
`UseCommonAccount`	This item is not displayed in an environment where common account information cannot be used.
`User`	This item is not displayed when `Y` is specified for `UseCommonAccount` in an environment where common account information can be used. Input value: The value in the corresponding common account information is used as the input value. For details about the corresponding common account information, see Table 3-24 or Table 3-25.
`Password` `Domain`	• These items are not displayed (because not required) when `Y` is specified for `UseCommonAccount` and `ssh` is specified for `TargetType` in an environment where common account information can be used. • These items are not displayed when `Y` is specified for `UseCommonAccount` and `wmi` is specified for `TargetType` in an environment where common account information can be used. Input value: The value in the corresponding common account information is used as the input value. For details about the corresponding common account information, see Table 3-24.
`Private_Key_File`	• This item is not displayed (because not required) when `Y` is specified for `UseCommonAccount` and `wmi` is specified for `TargetType` in an environment where common account information can be used. • This item is not displayed when `Y` is specified for `UseCommonAccount` and `ssh` is specified for `TargetType` in an environment where common account information can be used. Input value: The value in the corresponding common account information is used as the input value. For details about the corresponding common account information, see Table 3-25.
`Port`	This item is not displayed when `wmi` is specified for `TargetType` in the following kind of environment: both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

Note:

Here, *an environment where common account information can be used* refers to an environment where both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

(d) Execution in the interactive mode

1. Execute the `jpcconf target setup` command.

   In PFM - RM for Platform, we recommend that you specify the host name of the monitored host as the name of the monitoring target.

   The following example sets the monitored host `targethost1` with instance name `inst1` as the monitoring target:

   ```
   jpcconf target setup -key RMPlatform -inst inst1 -target targethost1
   ```

2. Set up the monitoring target for PFM - RM for Platform.

   Enter setting items for the monitored host according to the instructions given by the command. For details about the setting items for the monitored host, see Table 3-27. After you input each setting item, press the **Enter** key to set it. To use a displayed default value, simply press the **Enter** key.

   The following is an example of the settings when the monitored host is running Windows:

   Conditions for the monitored host to be set up

   - Host name: `targethost1`

- User: `user1`
- Password: `pass1`
- Domain: `domain1`

```
C:\Program Files\Hitachi\jp1pc\tools>jpcconf target setup -key RMPlatform
-inst inst1 -target targethost1
 Target Host          []                    :targethost1<Enter>
 UseCommonAccount#1   [N]                   :<Enter>
 TargetType           [wmi]                 :<Enter>
 User#2                                     :user1<Enter>
 Password#2                                 :pass1#3<Enter>
 Re-enter#2                                 :pass1#3<Enter>
 Domain#2             []                    :domain1<Enter>
 Private_Key_File     []                    :<Enter>
 Port#4               [22]                  :<Enter>
KAVE05361-I The monitoring target is now being added.
(servicekey#5=RMPlatform, inst=inst1, target=targethost1)
KAVE05362-I The monitoring target has been added.
(servicekey#5=RMPlatform, inst=inst1, target=targethost1)
```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

This item is not displayed when `Y` is specified for `UseCommonAccount`.

#3

Re-entry of the password is prompted. The entered password is not displayed on the screen.

#4

This item is not displayed when both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later. Even if this item is displayed, there is no need to set the item if the monitored host is running Windows.

#5

If PFM - Manager's product name display function is disabled, `agt7` is displayed for `servicekey`.

The following is an example of the settings when the monitored host is running UNIX:

Conditions for the monitored host to be set up

- Host name: `targethost2`
- User: `ssh-user`

```
C:\Program Files\Hitachi\jp1pc\tools>jpcconf target setup -key RMPlatform
-inst inst1 -target targethost2
 Target Host          []                    :targethost2<Enter>
 UseCommonAccount#1   [N]                   :<Enter>
 TargetType           [wmi]                 :ssh<Enter>
 User#2                                     :ssh-user<Enter>
 Password#2                                 :<Enter>
 Domain#2             []                    :<Enter>
 Private_Key_File     [] :C:\Program Files\PuTTY\agt7.ppk<Enter>
 Port                 [22]                  :<Enter>
KAVE05361-I The monitoring target is now being added.
(servicekey#3=RMPlatform, inst=inst1, target=targethost2)
```

```
KAVE05362-I The monitoring target has been added.
(servicekey#3=RMPlatform, inst=inst1, target=targethost2)
```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

This item is not displayed when `Y` is specified for `UseCommonAccount`.

#3

If PFM - Manager's product name display function is disabled, `agt7` is displayed for `servicekey`.

(e) Execution in the non-interactive mode

1. Execute the `jpcconf target setup` command to create a definition file template.

   Execute the command as follows:

   ```
   jpcconf target setup -key RMPlatform -noquery -template definition-file-name
   ```

   Sections and labels that correspond to the monitored host setting items are output to a definition file. Note that the value for the label of the `Target Definitions` section is left blank.

2. Edit the definition file template created in step 1.

   Edit the template setting values as required for the monitored host.

   For details about the product-specific labels to be specified in the definition file, see Table 3-27.

   Shown below is an example of the coding of a definition file when the monitored host is running Windows. Specify values for the labels in the `Target Definitions` section as required for the monitored host.

   ```
   [Common Definitions]
   Definition File Version=0001

   [Product Information]
   Product ID=7

   [Target Definitions]
   Target Host=targethost1
   UseCommonAccount#1=
   TargetType=
   User#2=user1
   Password#2=pass1
   Domain#2=domain1
   Private_Key_File=
   Port#3=
   ```

   #1

   This item is not displayed in an environment where common account information cannot be used.

   #2

   There is no need to specify a value for this item when `Y` is specified for `UseCommonAccount`.

   #3

   This item is not displayed when both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later. Even if this item is displayed, there is no need to set the item if the monitored host is running Windows.

Shown below is an example of the coding of a definition file when the monitored host is running UNIX. Specify values for the labels in the `Target Definitions` section as required for the monitored host.

```
[Common Definitions]
Definition File Version=0001

[Product Information]
Product ID=7

[Target Definitions]
Target Host=targethost2
UseCommonAccount#1=
TargetType=ssh
User#2=ssh-user
Password=
Domain=
Private_Key_File#2= C:\Program Files\PuTTY\agt7.ppk
Port=
```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

There is no need to specify a value for this item when `Y` is specified for `UseCommonAccount`.

3. Execute the `jpcconf target setup` command to set up the monitoring target for PFM - RM for Platform.

   The following example sets up a monitoring target where `inst1` is the instance name and `targethost1` is the monitored host. For the `-input` option, specify the definition file edited in step 2.

```
jpcconf target setup -key RMPlatform -inst inst1 -target targethost1 -
input definition-file-name -noquery
```

Note:

If the definition file contains confidential information such as passwords, save the definition file in a secure location, and delete it after you have used it. If you want to transfer the definition file between hosts, we recommend that you use a secure file transfer protocol, such as Secure File Transfer Protocol (SFTP), which is FTP over an SSH tunnel.

When all of the settings have been completed, a monitoring target environment can be built. The following table shows the folder structure of the monitoring target environment.

Table 3–29: Folder structure of the monitoring target environment

No.	Storage folder	File name	Description
1	*installation-folder*#`\agt7\agent\`*instance-name*`\targets`	*monitoring-target-name*`.ini`	Monitoring target settings file
2		*monitoring-target-name*`.ini.model`	Sample of a monitoring target settings file
3	*installation-folder*#`\agt7\agent\`*instance-name*`\targets\`*monitoring-target-name*	--	Work folder for the monitoring target

Legend:

--: Not applicable

#
If you run a logical host, replace *installation-folder* with *environment-folder*`\jp1pc`.

The following service IDs are added by the monitoring target settings:

Service IDs to be added

- Remote Agent service

  `7A`*instance-number instance-name* `[`*monitoring-target-name*`@`*host-name*`]`

  The instance name and monitoring target name will be the values specified in the `jpcconf target setup` command.

  If you specify `host1` as the host name of the PFM - RM host, `inst1` as the instance name, and `targethost1` as the monitoring target name, the service ID will be as follows:

  `7A1inst1[targethost1@host1]`

For details about the service IDs, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

If you want to change information about the monitoring target, re-execute the `jpcconf target setup` command and update the information. For details about updating a monitoring target, see *3.6.3 Updating a monitoring target*.

You can change some settings by using PFM - Web Console to edit properties. For details about the information that can be changed by editing properties, see *E.3 List of properties of remote agents and group agents*.

(4) Network settings Optional

You must specify network settings only if you need to change the network environment settings for the network configuration where Performance Management is used.

There are two types of network environment settings, as described below. Change network settings as necessary.

- IP address setting

  Set this information to use Performance Management in a network that is connected to multiple LANs. You set multiple IP addresses by defining the host names and IP addresses in the `jpchosts` file. Make sure that the specified `jpchosts` file is consistent throughout the entire Performance Management system.

  For details about the IP address settings, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Port number setting

  Set the port numbers used by Performance Management. To avoid confusion during operation, make sure that the specified port numbers and service names are consistent throughout the entire Performance Management system.

  For details about the port number settings, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(5) Changing the log file size Optional

The operation status of Performance Management is output to log files unique to Performance Management. This setting is required in order to change the size of these log files.

These unique log files are called the *common message log*.

For the common message log, two files with a size of 2,048 kilobytes each are used by default. For details about changing the common message log, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(6) Changing performance data storage locations Optional

These settings are required in order to change the following settings for the performance data that is managed by PFM - RM for Platform:

- Database storage location
  By default, *installation-folder*`\agt7\store\`*instance-name* is set.
- Backup location
  By default, *installation-folder*`\agt7\store\`*instance-name*`\backup` is set.
- Partial backup location
  By default, *installation-folder*`\agt7\store\`*instance-name*`\partial` is set.
- Export location
  By default, *installation-folder*`\agt7\store\`*instance-name*`\dump` is set.
- Import location
  By default, *installation-folder*`\agt7\store\`*instance-name*`\import` is set.

Note:
If you use a logical host for operation, replace *installation-folder* with *environment-folder*`\jp1pc`.

For details about changing performance data storage locations, see *3.6.1 Changing performance data storage locations*.

(7) Setting the connection-target PFM - Manager

You must specify on the PFM - RM host information about the PFM - Manager that manages PFM - RM for Platform. The `jpcconf mgrhost define` command is used to make this setting.

Notes about setting the connection-target PFM - Manager

- Only one PFM - Manager can be set as the connection destination even when multiple PFM - RMs are installed on the same host. A different PFM - Manager cannot be specified for each PFM - RM.
- If PFM - RM for Platform and PFM - Manager are installed on the same host, then the PFM - Manager on the local host is the connection-target PFM - Manager. In this case, you cannot change the connection-target PFM - Manager to any other PFM - Manager. To connect to PFM - Manager on a remote host, install PFM - RM for Platform on a different host than for PFM - Manager.

To set the connection-target PFM - Manager:

1. Stop the Performance Management programs and services.
   If any Performance Management programs and services are running on the local host, stop all of them before starting the setup procedure. If Performance Management programs and services are running during execution of the `jpcconf mgrhost define` command, a message is displayed that asks you to terminate them.
   For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

2. Execute the `jpcconf mgrhost define` command with the host name of the connection-target PFM - Manager specified.
   The following shows an example of command execution when the connection-target PFM - Manager is located on the `host01` host:

   ```
   jpcconf mgrhost define -host host01
   ```

This example shows execution in the interactive mode, but you can also execute the `jpcconf mgrhost define` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(8) Action log output settings Optional

These settings are required in order to output action logs at the following times:

- When a PFM service starts
- When a PFM service stops
- When the PFM - Manager connection status is changed

An action log contains log information about exceeded threshold values caused by factors such as system overloads; its output is linked with the alarm function. For details about the action log output settings, see *I. Outputting Action Log Data*.

3.1.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows)

This subsection explains how to set up the WMI connection settings necessary for collecting performance data from a monitored host running Windows.

To connect WMI, settings for the following are required:

- DCOM

  The DCOM setting must be made at both the PFM - RM host and the monitored hosts.

  If you run the PFM - RM host in a cluster system, the DCOM setting must be made at both the executing node and the standby node.
- Firewall

  Set the firewall on each monitored host, as necessary.
- WMI namespace

  Set the WMI namespace on each monitored host, as necessary.

When you have finished making the settings, check that you can connect from the PFM - RM host to the monitored hosts.

Notes about WMI connection setting

- Data cannot be collected when **Disabled** is set as the startup type of the Windows Management Instrumentation service (service name: `WinMgmt`) that provides system administration information for the OS of a monitored host.
- The type of records that can be collected differs according to the account type. For details about various account types and whether records can be collected, see *3.1.1(5)(a) Setting the user accounts*.

(1) DCOM setting

This subsection describes how to set DCOM at the PFM - RM host and the monitored hosts.

(a) Setting at the PFM - RM host

Set DCOM at the PFM - RM host.

To set DCOM:

1. From the Windows **Start** menu, choose **Run**.
2. Enter `dcomcnfg.exe`, and then click the **OK** button.
   The Component Services window appears.
3. Click **Component Services** and **Computers** to expand the tree.
4. Choose **My Computer**, and then from the right-click menu, choose **Properties**.
   The My Computer Properties dialog box appears.
5. Choose the **Default Properties** tab, and then select **Enable Distributed COM on this computer**.
6. Click the **OK** button.
   The My Computer Properties dialog box closes.
7. Restart the machine.
   This step is not needed if you have not changed the setting of **Enable Distributed COM on this computer**.

(b) Setting at a monitored host

Set DCOM at each monitored host.

Some parts of the procedure might differ depending on the OS environment of a specific monitored host, as described below:

- If the OS of the monitored host is Windows Server 2003 with no service pack applied, there is no **Edit Limits** button, which means that there is no need to perform steps 6 through 11.
- If the OS of the monitored host is Windows Server 2008 or Windows Server 2012 and the UAC security facility is enabled, set DCOM for the user itself or for a group to which the user belongs, except for the Users or Administrators group.

To set DCOM:

1. From the Windows **Start** menu, choose **Run**.
2. Enter `dcomcnfg.exe`, and then click the **OK** button.
   The Component Services dialog box appears.
3. Click **Component Services** and **Computers** to expand the tree.
4. Choose **My Computer**, and then from the right-click menu, choose **Properties**.
   The My Computer Properties dialog box appears.
5. Choose the **Default Properties** tab, and then select **Enable Distributed COM on this computer**.
6. Choose the **COM Security** tab, and then click the **Edit Limits** button for **Access Permissions**.
   The Access Permission dialog box appears.

Check to see if the user who connects to the monitored host or the group to which the user belongs is displayed in **Group or user names**.
If it is not displayed, click the **Add** button, and then add the user or the group to which the user belongs.

7. In **Group or user names**, select the user who connects to the monitored host or the user's group.
   Check to see if **Allow** is selected in **Remote Access**. If this option is not selected, select it.

8. Click the **OK** button.
   The Access Permission dialog box closes.

9. Choose the **COM Security** tab, and then click the **Edit Limits** button for **Launch and Activation Permissions**.
   The Launch Permission dialog box appears.
   Check to see if the user who connects to the monitored host or the group to which the user belongs is displayed in **Group or user names**.
   If it is not displayed, click the **Add** button, and then add the user or the group to which the user belongs.

10. In **Group or user names**, select the user who connects to the monitored host or the user's group.
    Check to see if **Allow** is selected for both **Remote Launch** and **Remote Activation**. If it is not selected, select it.

11. Click the **OK** button.
    The Launch Permission dialog box closes and the My Computer Properties dialog box is displayed again.

12. Click the **OK** button.
    The My Computer Properties dialog box closes.

13. Restart the machine.
    This step is not needed if you have not changed the setting of **Enable Distributed COM on this computer**.

(2) Firewall setting

This setting is required when a Windows firewall is enabled.

To determine if the firewall setting is enabled or disabled, from the Windows **Start** menu, choose **Control Panel,** and then **Windows Firewall**.

If the OS of the monitoring target is Windows Server 2003 with no service pack applied, then the Windows firewall function is not supported, and this setting is not needed.

To set the firewall:

1. From the Windows **Start** menu, choose **Run**.

2. Enter `gpedit.msc`, and then click the **OK** button.
   The Group Policy dialog box appears.

3. Click **Computer Configuration**, **Administrator Templates**, **Network**, **Network Connections**, and **Windows Firewall** to expand the tree.

4. Click **Standard Profile**,[#1] and then in the right-hand pane, from the right-click menu of **Windows Firewall: Allow remote administration exception**,[#2] choose **Properties**.
   The Windows Firewall: Allow remote administration exception Prop. dialog box appears.

#1

If the host machine is a domain environment, this will be **Domain Profile**.

#2

If the OS of the monitored host is Windows Server 2008 or Windows Server 2012, this will be **Windows Firewall: Allow remote administration exception**.

5. Choose the **Setting** tab, and then select **Enabled**.

6. Click the **OK** button.
   The Windows Firewall: Allow remote administration exception Prop. dialog box closes.

(3) WMI namespace setting

This subsection explains the procedure for setting the WMI namespace.

If the OS of the monitored host is Windows Server 2008 or Windows Server 2012 and the UAC security facility is enabled, set the WMI namespace security for the user itself or for a group to which the user belongs, except for the Users or Administrators group.

To set the WMI namespace security:

1. From the Windows **Start** menu, choose **Run**.

2. Enter `wmimgmt.msc`, and then click the **OK** button.
   The Windows Management Infrastructure (WMI) dialog box appears.

3. Choose **WMI Control (Local)**, and then from the right-click menu, choose **Properties**.
   The WMI Control (Local) Properties dialog box appears.

4. Choose the **Security** tab, and then click **Root** and **CIMV2** to expand the tree.

5. Click the **Security** button.
   The Security for ROOT\CIMV2 dialog box appears.
   Check to see if the user who connects to the monitored host or the user's group is displayed in **Group or user names**. If it is not displayed, click the **Add** button, and then add the user or the group to which the user belongs.

6. In **Group or user names**, select the user who connects to the monitored host or the group to which the user belongs.
   Check to see if **Allow** is selected for both **Enable Account** and **Remote Enable**. If it is not selected, select it.

7. Click the **OK** button.
   The Security for ROOT\CIMV2 dialog box closes, and the WMI Control (Local) Properties dialog box is displayed again.

8. Click the **OK** button.
   The WMI Control (Local) Properties dialog box closes.

9. In the Windows Management Infrastructure (WMI) dialog box, click **File**, and then **Exit** to close the dialog box.

(4) Setting up LocalAccountTokenFilterPolicy

Note the following when the OS of the monitoring target is Windows Server 2008 or Windows Server 2012: If you specify a local user who has Administrator permissions (except for the Administrator user who is created during OS installation) as the user in monitoring target setting, UAC will restrict the permission and connection will be made as

an ordinary user. Consequently, access might be refused and you might not be able to collect performance data. To avoid this, either disable the monitoring target's UAC or specify the following setting at the monitoring target:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

To return to the original setting, execute the following command:

```
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
\System /v LocalAccountTokenFilterPolicy /f
```

(5) Checking the WMI connection

Use the `wbemtest.exe` Windows tool to check whether the PFM - RM host and a monitored host are connected. Perform this procedure at the PFM - RM host.

To check the WMI connection:

1. At the command prompt, execute the following command:
   `runas /user:`*user-name* `wbemtest`
   The Windows Management Instrumentation Tester dialog box appears.
   For the user name, specify the values for `RMHost_User` and `RMHost_Domain`. If re-entry of the password is requested after the command executes, specify the value of `RMHost_Password`.
   For details about `RMHost_User`, `RMHost_Domain`, and `RMHost_Password`, see Table *3-20 Instance environment setting items and values for PFM - RM for Platform (for Windows)*.
   To use common account information, specify the respective values that are specified in `User`, `Domain`, and `Password` in the common account information (pfmhost) for the instance environment.

2. Click the **Connect** button.
   The Connect dialog box appears.

3. In **Namespace**, **User**, **Password**, and **Authority**, enter the appropriate information.
   If the WMI connection target is the local host, there is no need to enter values in **User**, **Password**, or **Authority**. If you enter values in these items, an error occurs and you will not be able to connect.
   To execute the tool (`wbemtest.exe`) on the local host, click the **Connect** button without entering values in **User**, **Password**, or **Authority**.
   The following describes each item.
   - **Namespace**
     Enter `\\`*monitored-host-name*`\root\cimv2`. For the name of the monitored host, specify the value of `Target Host`.
   - **User**
     Enter the user name used to log on to the monitored host. For the user name, specify the value of `User`. To use common account information, specify the value that is specified in `User` in the common account information (wmi).
   - **Password**
     Enter the user's password. For the user's password, specify the value of `Password`. To use common account information, specify the value that is specified in `Password` in the common account information (wmi).
   - **Authority**

Enter `ntlmdomain:`*domain-name-of-monitored-host*. If the monitored host is a workgroup, leave this field blank. For the domain name of the monitored host or the monitored host name, specify the value of `Domain`. To use common account information, specify the value that is specified in `Domain` in the common account information (wmi).

For details about `Target Host`, `User`, `Password`, and `Domain`, see Table *3-27 Setting items and values for a monitored host in PFM - RM for Platform*.

4. Click the **Connect** button.

   If connection is established successfully, the Connect dialog box closes and all buttons are enabled in the Windows Management Instrumentation Tester dialog box.

   If an error dialog box is displayed, check the settings based on the error number. The error numbers and causes are described below.

   Note that if you change the settings while running the `wbemtest.exe` tool, and then attempt to re-establish connection, an error might result. In such a case, restart the tool, and then check the connection.

   - `0x8001011c`

     DCOM is not set at the PFM - RM host.

   - `0x80070005`

     Possible cause of the error is one of the following:

     · DCOM is not set at the PFM - RM host.

     · DCOM is not set at the monitored host.

     · The user name, password, or domain name used to connect to the monitored host is invalid.

   - `0x80041003`

     At the monitored host, **Namespace** is not selected for WMI.

   - `0x80041008`

     The value specified in **Authority** does not begin with `ntlmdomain:`.

   - `0x800706`*xx*

     Possible cause of the error is one of the following:

     · The monitored host name is invalid.

     · The monitored host is not running.

     · The firewall was not set up at the monitored host.

     · The password for the user who logs on to the monitored host has expired.

5. Click the **Enum Instances** button.

   The Class Info dialog box appears.

6. To monitor processes, enter `Win32_Service` in **Enter superclass name**, or enter `Win32_PerfRawData_PerfOS_System` in all other cases, and then click the **OK** button.

   The Query Result dialog box appears.

   If you enter `Win32_Service` in **Enter superclass name**

   Check to see if objects are displayed in the list. If an error dialog box is displayed, the user name used to connect to the monitored host might not be a member of the Administrators group.

   If you enter `Win32_PerfRawData_PerfOS_System` in **Enter superclass name**

   Check to see if `Win32_PerfRawData_PerfOS_System=@` is displayed in the list. If an error dialog box is displayed or this value is not displayed in the list, the user who connects to the monitored host might not be a member of the Administrators, Performance Log Users, or Performance Monitor Users group.

Note that if you change the settings while running the `wbemtest.exe` tool, and then attempt to re-execute enumeration of instances, an error might result. In such a case, restart the tool, and then re-check the connection.

For details about PFM - Manager startup, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3.1.6 SSH connection setting method for Windows (when the PFM - RM host is running Windows and the monitored host is running UNIX)

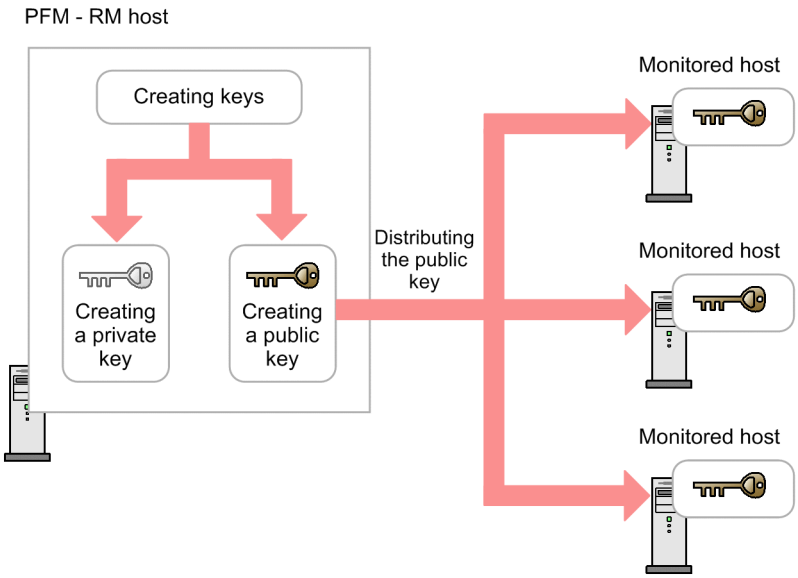
This subsection explains how to set up the SSH connection settings necessary for collecting performance data from a monitored host running UNIX. For SSH authentication, you use the public key authentication method.

To connect SSH, settings for the following are required:

- Enabling public key authentication for the SSH server
  Specify this on the monitored host.
- Creating a key
  Specify this on the PFM - RM host.
- Placing the private key on the PFM - RM host
  Specify this on the PFM - RM host.
- Placing the public key on the monitored host
  Specify this on the monitored host.

The following figure provides an overview of public key authentication.

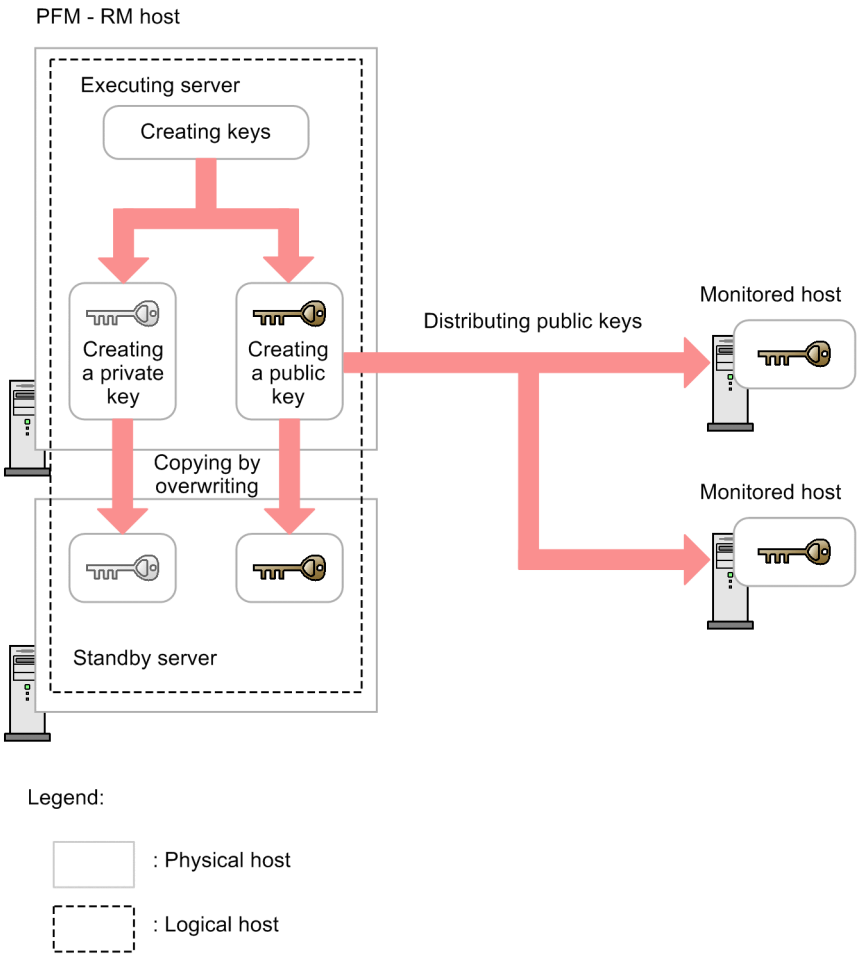
Figure 3–7: Concept of public key authentication



For public key authentication in a cluster system, you can either use a common key on both the active server node and the standby server node, or use different keys on these nodes.

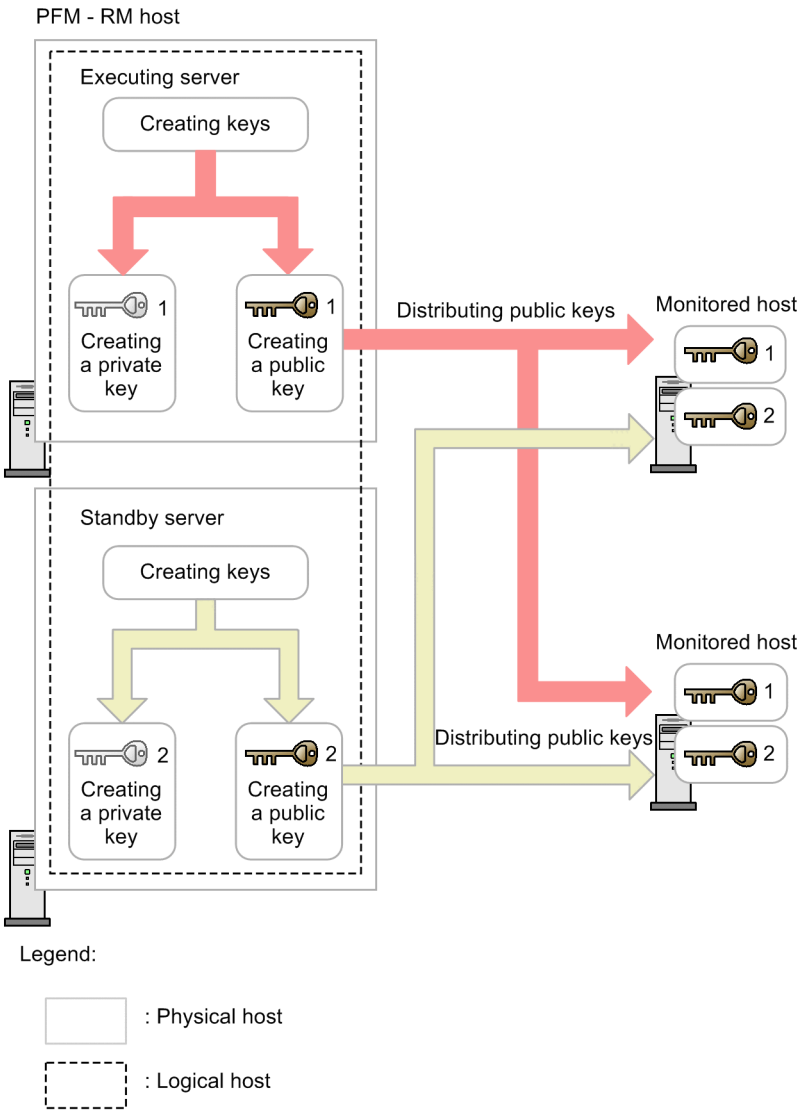
To use a common key on both the active server node and the standby server node, copy the key file from the active server node to the copy file of the standby server node, overwriting any existing key files. The following figure shows the concept of using a common key.

Figure 3–8: Concept of public key authentication (when a common key is used at both the active server node and the standby server node)



To use different keys on the active server node and the standby server node, register the key files of the active server node and the standby server node at the monitored host. The following figure shows the concept of using different keys.

Figure 3–9: Concept of public key authentication (when different keys are used at the active server node and the standby server node)



(1) Enabling the SSH server's public key authentication

To enable public key authentication:

1. Log on to the monitored host as a superuser.
2. Open `/etc/ssh/sshd_config`#.
3. Change `PubkeyAuthentication` to `yes`.
4. Save and close `/etc/ssh/sshd_config`#.
5. Execute the following command to start the sshd service:

```
[root@TargetHost.ssh]$ /etc/rc.d/init.d/sshd restart
```

Reference note

To log on as a superuser to collect information, open `/etc/ssh/sshd_config`# and change `PermitRootLogin` to `yes`. After that, restart the sshd service.

#

This will be `/opt/ssh/etc/sshd_config` when using HP-UX.

(2) Creating keys

This subsection explains the procedure for creating keys.

Log on to the PFM - RM host and create a key by executing PuTTY. You can select RSA or DSA encryption for the key type. The only difference between RSA and DSA encryption is the encryption algorithms; their operation methods are the same.

To create RSA keys:

1. From the Windows Start menu, choose **All Programs**, **PuTTY**, and then **PuTTYgen**.

   The PuTTY Key Generator window appears.

2. Under **Parameters**, make sure that **SSH-2 RSA** is selected for **Type of key to generate**, and then click the **Generate** button.

   A progress bar showing the key generation progress is displayed in **Key**.

   Because PuTTY uses version 2 of the SSH protocol as the default, **SSH-2 RSA** is selected. For details about how to change the default used to version 1 of the SSH protocol, see the documentation for PuTTY.

3. Until the progress bar reaches 100%, randomly move the mouse in the dialog box to generate random numbers necessary for creating a key.

   When the progress bar reaches 100%, the generated random numbers are displayed in **Key** and a key is generated.

4. Click the **Save private key** button to save the private key.

   If you did not enter any value in **Key passphrase** or **Confirm passphrase**, a dialog box still appears. Do not enter any value in **Key passphrase** or **Confirm passphrase** and click the Yes button.

5. Click the **Save public key** button to save the public key.

(3) Placing the public key on the monitored hosts

Place the created public key on the monitored host. If there are multiple monitored hosts, distribute the key to all of them.

(a) Transferring the public key to the monitored host

Transfer the public key created at the PFM - RM host to the monitored host.

To transfer the public key:

1. Log on to the monitored host by using the value that was specified in `User` during monitoring target setup.

   To use common account information, specify the value that is specified in `User` in common account information (ssh).

2. Execute the `cd` command to change the current directory to the `.ssh` directory under the home directory.

   If the `.ssh` directory does not exist under the home directory, create it. For the `.ssh` directory attribute, specify `700` or `755`. For the owner and group, specify the same as those specified for the user who was specified during the setup of the monitored host. If the attribute, owner, or group setting of the home directory or the `.ssh` directory is invalid, SSH connection might fail.

   For details about how to specify directory attributes, see the documentation for the OS.

3. Start the command prompt at the PFM - RM host, and then change the current directory to the folder in which PuTTY is installed.

4. Execute the `pscp` command provided by PuTTY.

   The following is an example of command execution when a public key is located in the PuTTY installation directory:

```
C:\Program Files\PuTTY>pscp.exe agt7.pub ClientUser@TargetHost:.ssh
 ClientUser@TargetHost's password: password
 agt7.pub     | 0 kB |   0.3 kB/s | ETA: 00:00:00 | 100%
```

   If a message appears asking if a fingerprint should be registered, enter `n`.

(b) Registering the public key at the monitored host

To register the public key at the monitored host:

1. Log on to the monitored host by using the value that was specified in `User` during monitoring target setup.

   To use common account information, specify the value that is specified in `User` in common account information (ssh).

2. Execute the `cd` command to change the current directory to the `.ssh` directory.

3. Execute the `ssh-keygen` command with both the `-i` and `-f` options specified.

   The public key created in PuTTY is converted into a format that can be used by OpenSSH.

4. Execute the `rm` command to delete the public key file received in *(a) Transferring the public key to the monitored host*.

5. Execute the `chmod` command to change the attribute of the authentication key file to `600`.

An example of performing steps 2 through 5 follows:

```
[ClientUser@TargetHost ~]$ cd .ssh
[ClientUser@TargetHost .ssh]$ ssh-keygen -i -f agt7.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm agt7.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

The name of the authentication key file is set by `AuthorizedKeysFile` of `/etc/ssh/sshd_config`. For HP-UX, it is `/opt/ssh/etc/sshd_config`.

By default, `~/.ssh/authorized_keys` is set.

(4) Checking the connection and registering a fingerprint

To check whether the PFM - RM host and a monitored host can connect to each other:

1. Log on to the PFM - RM host by using the value that was specified in `RMHost_User` during instance environment setup.

   To use common account information, log on to the PFM - RM host by using the value that is specified in `User` in common account information (pfmhost).

2. Start the command prompt.

3. Using the created private key, execute PuTTY's `plink` command on the monitored host.

   The connection process begins.

4. During the initial connection, register a fingerprint.

   Register the fingerprint of the public key on the monitored host. Here, enter `y`. When you enter `y`, the monitored host's command prompt appears.

5. From the monitored host's prompt, execute the `exit` command to log out from the monitored host.

6. From the PFM - RM host, execute PuTTY's `plink` command on the monitored host to reconnect to it.

   If the monitored host's prompt appears in subsequent connections without you having to enter any information, setup of the connection between the PFM - RM host and the monitored host is completed. From the monitored host's command prompt, execute the `exit` command to log out from the monitored host.

   If an error occurs or if you are asked to enter anything, check to see if you have correctly followed the procedure.

A setting example for checking connection follows:

```
C:\WINDOWS\system32>"C:\Program Files\PuTTY\plink.exe" -ssh -noagent -i "C:
\Program Files\PuTTY\agt7.ppk" -P 22 ClientUser@TargetHost
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
Using username "ClientUser".
Last login: Wed Aug  4 13:29:55 2010 from xxx.xxx.xxx.xxx
[ClientUser@TargetHost]$ exit
logout
C:\WINDOWS\system32>"C:\Program Files\PuTTY\plink.exe" -ssh -noagent -i "C:
\Program Files\PuTTY\agt7.ppk" -P 22 ClientUser@TargetHost
Using username "ClientUser".
Last login: Wed Aug  4 13:30:00 2010 from xxx.xxx.xxx.xxx
[ClientUser@TargetHost]$ exit
logout
C:\WINDOWS\system32>
```

Notes:

- PFM - RM for Platform assumes that fingerprint registration has already been completed. Because you can register a fingerprint during the initial SSH client connection, we recommend that you complete the procedure described here at that point.
- If you change the user account specified for `RMHost_User` during the instance environment setup, you need to re-register a fingerprint. If you are using common account information, you also need to re-register a fingerprint when updating the value of `User` in common account information (pfmhost).
- If you run PFM - RM for Platform in a cluster system, register a fingerprint on the standby node in the same way as on the executing node.
- Confirm that a response is returned in less than 10 seconds when you execute a command such as `uname` on the monitored host from the PFM - RM host.

For details about PFM - Manager startup, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3.1.7 Notes about installation and setup of the Windows edition

This subsection provides notes about installing and setting up Performance Management in a Windows environment.

(1) Notes about registry

PFM - RM for Platform supports operation in an environment that is set up by the OS-provided standard method. If you have customized the OS environment, such as by using a registry editor to directly edit registry information, performance data might no longer be collected correctly even if such customization is disclosed in the Microsoft technical support information.

(2) Notes about environment variables

Performance Management uses the `JPC_HOSTNAME` environment variable. Do not set a user-specific `JPC_HOSTNAME` environment variable. If such an environment variable is set, Performance Management will not function correctly.

(3) Notes about installing multiple Performance Management programs on the same host (for Windows)

In Performance Management, you can install PFM - Manager, PFM - Web Console, and PFM - RM for Platform on the same host. This subsection provides notes about installing multiple Performance Management programs on the same host.

To improve system performance and reliability, we recommend that you run PFM - Manager, PFM - Web Console, and PFM - RM for Platform on separate hosts.

- PFM - Manager and PFM - Base cannot be installed on the same host. If you need to install PFM - Manager on a host where PFM - Base and PFM - RM for Platform have been installed, perform the following procedure:
  1. Uninstall all Performance Management programs except PFM - Web Console.
  2. Install PFM - Manager.
  3. Install PFM - RM for Platform.

- If you need to install PFM - Base on a host where PFM - Manager and PFM - RM for Platform have been installed, perform the following procedure:
  1. Uninstall all Performance Management programs except PFM - Web Console.
  2. Install PFM - Base.
  3. Install PFM - RM for Platform.
- If you install PFM - Manager on the PFM - RM host, the connection-target PFM - Manager for the PFM - RM for Platform is reset to the local host name. If this is the case, check the common message log because the setting results are output to the log.
- If you are installing PFM - RM for Platform on the PFM - Web Console host, close all browser windows before you start the installation.
- If you install a new Performance Management program, the status management function is enabled by default.

(4) Notes about upgrading (for Windows)

This subsection provides notes about upgrading PFM - RM for Platform.

- When you install a Performance Management program, stop all Performance Management programs and services on the local host before you start installation. Stop all services on both physical and logical hosts. For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.
- If you install PFM - RM for Platform on a host where Performance Management programs have already been installed, the PFM - RM for Platform installation folder will be the same as for the installed Performance Management programs. To change the installation folder, you must first delete all Performance Management programs except PFM - Web Console, and then re-install the programs.
- When upgrading the data model version of the Store database, a space of twice the size of the Store database is temporarily required on the Store database storage disk because the existing Store database is upgraded automatically. Before you start upgrading, make sure that there is enough free space on the Store database storage disk. Determine the required free space based on the total size of the current Store database. For example, if the total size of the current Store database is 100 gigabytes, you need at least 200 gigabytes of free space for installing the upgraded version. If you change the storage destination disk for the Store database, take the disk size following the change into consideration.

(5) Notes about linking with other systems (for Windows)

This subsection provides notes about linking with other systems.

- If you install PFM - RM for Platform in an environment that is linked with NNM, stop the NNM linkage facility and `ovw` before you start the installation. For details about the NNM linkage facility, see the chapter that describes NNM linkage in the *Job Management Partner 1/Performance Management User's Guide*.

(6) Notes about installing PFM - RM for Platform in a Windows environment

This subsection provides notes about installing PFM - RM for Platform in a Windows environment.

- If you install PFM - RM for Platform in an environment where no Performance Management program has been installed, make sure that there are no folders or files in the installation folder.
- If you install PFM - RM for Platform while Performance Management programs and services or other programs that reference Performance Management files (such as Windows Event Viewer) are running, a message prompting

you to restart the system might be displayed. In such a case, restart the system according to the message to complete the installation.

- If you install PFM - RM for Platform in any of the statuses below, file expansion might fail:
  - Performance Management programs and services or other programs that reference Performance Management files (such as Windows Event Viewer) are running.
  - The disk capacity is insufficient.
  - The user does not have required folder permissions.

  If installation has failed, terminate the programs that reference Performance Management files or take appropriate action, such as by resolving the problem of insufficient disk capacity or of folder permissions, and then re-install PFM - RM for Platform.
- If you upgrade PFM - RM for Platform in a cluster environment, you must place the shared disk online in either the executing system or the standby system.
- If you perform new installation of PFM - RM for Platform, the system must be restarted. In the case of overwrite installation and upgrading, a message prompting the user to restart the system might be displayed. In such a case, restart the system according to the message to complete the installation.
- If the *installation-folder*`\setup` folder contains the setup file of PFM - RM for Platform, additional setup of a new PFM - RM for Platform will be executed.
- Before you install a Performance Management program, check to see if any of the security-related programs described below are installed. If such a program is installed, take appropriate action according to the information provided below.
  - Security monitoring program

    Either terminate the security monitoring program or change its settings so that installation of the Performance Management program will not be affected.
  - Virus detection program

    We recommend that you terminate any virus detection program before you install the Performance Management programs.

    If a virus detection program is running during installation of a Performance Management program, it might slow down the installation process, the installation might fail, or the program might not install correctly.
  - Process monitoring program

    Either terminate the process monitoring program or change its settings so that it does not monitor Performance Management services and processes or services and processes of common components.

    Installation of a Performance Management program might fail if these services and processes are started or stopped by the process monitoring program during the installation process.

3.2 Installation and setup of the UNIX edition

This section describes the procedures for installing and setting up PFM - RM for Platform in a UNIX environment.

3.2.1 Issues to consider before installing the UNIX edition

This subsection describes issues to be considered before you install PFM - RM for Platform.

(1) Prerequisite OS

PFM - RM for Platform can run on the following operating systems (OSs):

- Linux (x86)
- Linux (x64)

(2) Setting up a network environment

To use Performance Management to run PFM - RM for Platform, you must set up a network environment, such as IP addresses and port numbers.

(a) Setting IP addresses

You must set up the environment for PFM - RM for Platform in such a manner that an IP address can be determined from the host name. PFM - RM for Platform will not start in an environment in which IP addresses cannot be resolved.

You use one of the following methods to set host names and IP addresses:

- `jpchosts` file (Performance Management's host information configuration file)
- `hosts` file
- DNS

For the monitoring host name, use either the real host name or the alias name.

- Using the real host name
  In a UNIX environment, specify the name in such a manner that the IP address can be resolved from the host name that is obtained from the result of executing the `uname -n` command. You can also use the host name that is acquired by the `hostname` command.

  Note that Performance Management supports DNS, but not FQDN. This means that when you set the IP address, you must use the host name obtained by the `uname -n` command without the domain name.
- Using an alias name
  Set the environment in such a manner that the IP address can be resolved from the specified alias name.

For details about setting the name of the monitoring host, see the chapter that describes changing the system configuration in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note that the IP address specified in the `jpchosts` file is not used for IP address resolution with the monitored host.

Notes about setting IP addresses

- If you use Performance Management in multiple LAN environments, use the `jpchosts` file to set IP addresses. For details about using the `jpchosts` file to set IP addresses, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
- Performance Management will not run on a host where IP addresses are assigned dynamically by DHCP. You must set fixed IP addresses for all monitoring hosts.

(b) Settings for using IPv6

Performance Management supports both IPv4 and IPv6 network environments. Therefore, you can run Performance Management even in a network environment where IPv4 and IPv6 coexist.

PFM - RM for Platform can use IPv6 to communicate with PFM - Manager. However, this applies only when the OS of the host on which PFM - RM for Platform and PFM - Manager are installed is Windows Server 2008 R2, Windows Server 2012, or Linux. For details about the applicable scope of communication in the IPv4 and IPv6 environments, see *L. Communication in IPv4 and IPv6 Environments*.

To communicate using IPv6, you must enable the use of IPv6 on both the PFM - Manager host and the PFM - RM host. You specify this setting by executing the `jpcconf ipv6 enable` command. The following explains the conditions to use for determining whether you need to execute this command.

Cases in which you need to execute the `jpcconf ipv6 enable` command:

- All hosts are being changed from an IPv4 environment to an IPv6 environment.
- In an environment where IPv4 and IPv6 coexist and PFM - Manager is being changed from an IPv4 environment to an IPv6 environment

Cases in which you do not need to execute the `jpcconf ipv6 enable` command:

- All hosts are already in an IPv6 environment.
- In an environment where IPv4 and IPv6 coexist and PFM - Manager is already in an IPv6 environment.

An example of executing the `jpcconf ipv6 enable` command follows:

```
jpcconf ipv6 enable
```

For details about the `jpcconf ipv6 enable` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*. For details about the conditions and timing for executing the `jpcconf ipv6 enable` command, see the chapter that describes an example of a network configuration that includes an IPv6 environment in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

When PFM - RM for Platform will use IPv6 to communicate with monitored hosts, specify a monitored host name that can be resolved.

PFM - RM for Platform uses a resolvable IP address to communicate with a monitoring target. When PFM - RM for Platform communicates with a monitoring target in an environment where IPv4 and IPv6 coexist, PFM - RM for Platform will not try to communicate using another IP address if communication using a resolvable IP address fails.

For example, if a connection attempt using IPv4 fails, PFM - RM for Platform will not retry using IPv6. Conversely, if a connection attempt using IPv6 fails, PFM - RM for Platform will not retry using IPv4. Therefore, make sure that connection can be established beforehand.

(c) Setting port numbers

You must assign a port number to each service of the programs used in Performance Management. Set up the network in such a manner that the port numbers assigned to PFM - RM for Platform can be used for communication.

The table below lists and describes the default port numbers assigned to various services. For other services, an unused port number is assigned automatically each time the service starts.

Table 3–30: Default port numbers for services (for Windows)

No.	Supported function	Service name	Parameter	Port number	Description
1	Service configuration information management function	Name Server	`jp1pcnsvr`	`22285`	Port number used by PFM - Manager's Name Server service. This port number is set at all hosts of Performance Management.
2	NNM linkage facility	NNM Object Manager	`jp1pcovsvr`	`22292`	Port number used for communication between the map manager and the object manager when the NNM linkage facility is used with PFM - Manager and PFM - Base. This port number is set at the host where PFM - Manager and PFM - Base are installed.
3	Service status management function	Status Server	`jp1pcstatsvr`	`22350`	Port number used by the Status Server service of PFM - Manager and PFM - Base. This port number is set at the host where PFM - Manager and PFM - Base are installed.
4	Monitoring console communication function	View Server	`jp1pcvsvr`	`22286`	Port number used by the View Server service of PFM - Manager. This port number is set at the host where PFM - Manager is installed.
5	Web service function	Web Service	--	`20358`	Port number used by the Web Service service of PFM - Web Console.
6	Web container function	Web Console	--	`20359` `20360`	Port number used by the Web Console service of PFM - Web Console.
7	JP1/ITSLM linkage facility	JP1/ITSLM	--	`20905`	Default port number specified in JP1/ITSLM.

Legend:

--: Not applicable

When you use Performance Management in an environment that includes a firewall, you must use fixed port numbers. For details about how to use fixed port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(3) OS user permissions required for installation

When you install PFM - RM for Platform, make sure that you use an account that has Administrator permissions.

(4) Prerequisite programs

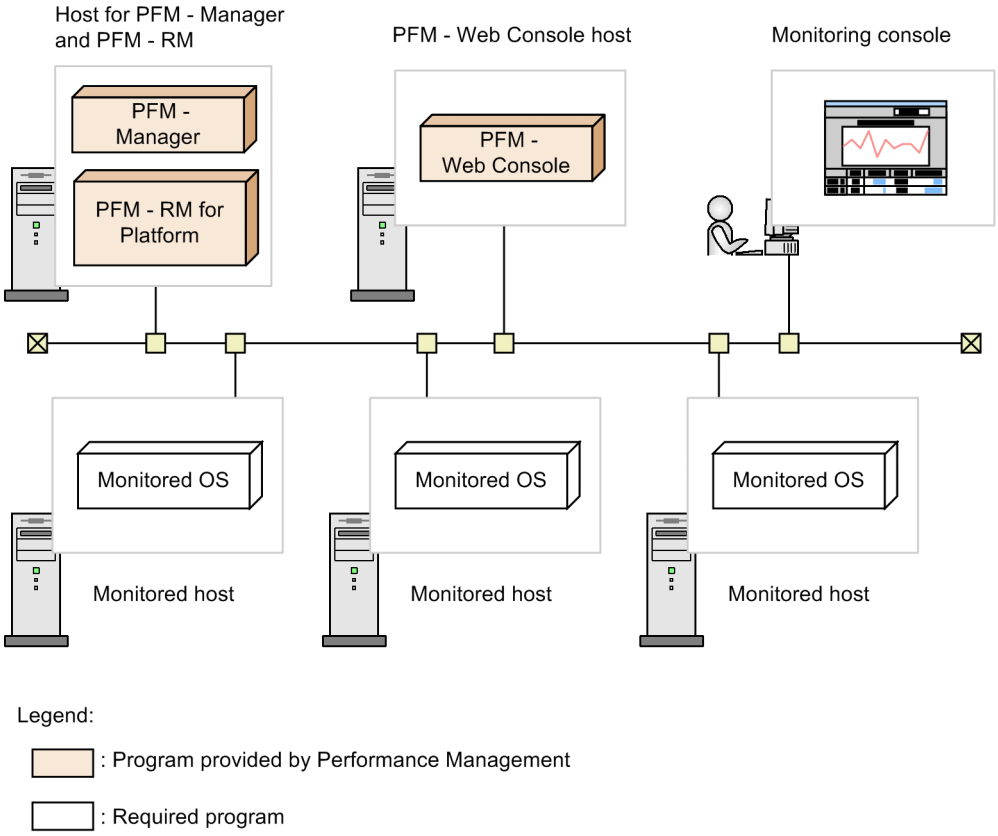
This subsection describes the configuration of programs required in order to install PFM - RM for Platform.

There are two major types of program configurations, as described below. Evaluate the program configurations from the perspective of your system environment.

When installing PFM - RM for Platform on the PFM - Manager host

With this program configuration, PFM - RM for Platform is installed on the same host as PFM - Manager. The following figure shows the program configuration.

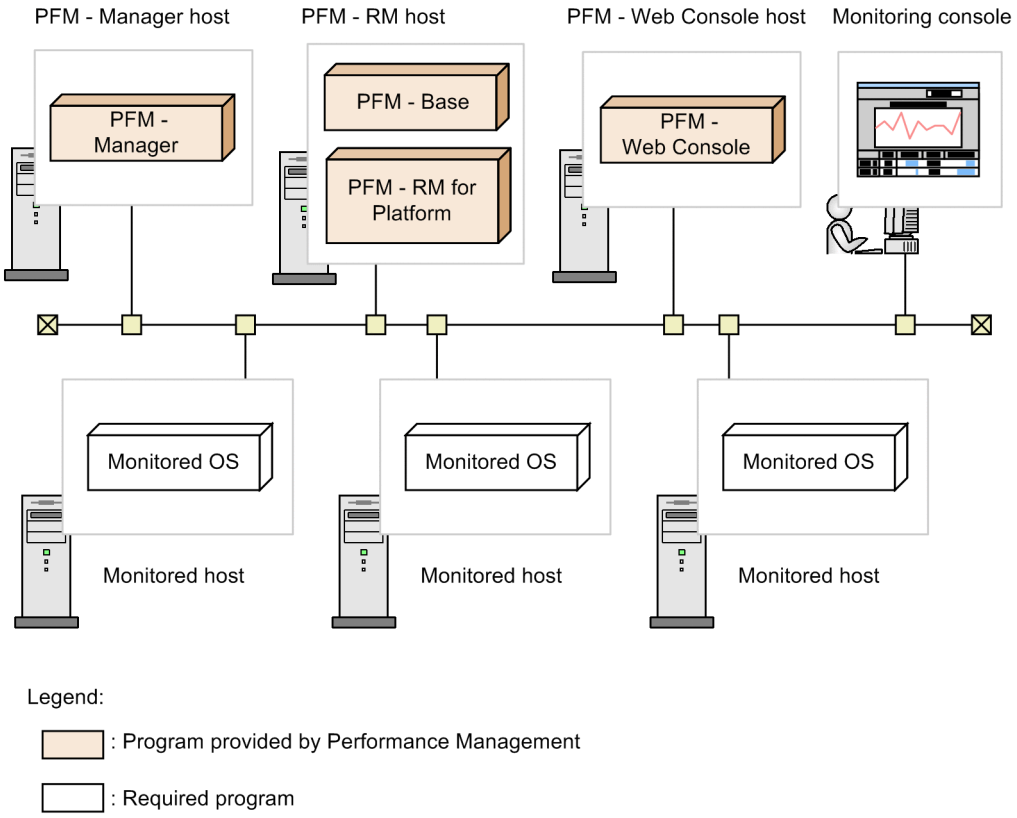
Figure 3–10: Program configuration (when PFM - RM for Platform and PFM - Manager are installed on the same host (for UNIX))



When installing PFM - RM for Platform on a host other than the PFM - Manager host

With this program configuration, PFM - RM for Platform is installed on a host other than the PFM - Manager host. If you use this program configuration, you must install PFM - Base on the same host as for PFM - RM for Platform. The following figure shows the program configuration.

Figure 3–11: Program configuration (when PFM - RM for Platform and PFM - Base are on the same host (for UNIX))



(a) Prerequisite OSs for monitored hosts

A monitored host must be using one of the following OSs:

- HP-UX
- Solaris
- AIX
- Linux

(b) Prerequisite programs for Performance Management

PFM - Manager or PFM - Base must be available on the host where PFM - RM for Platform is installed.

If you install PFM - RM for Platform on a host where PFM - Manager is available, PFM - Base is not required. If you install multiple PFM - RMs on a host where PFM - Base is available, you need only one PFM - Base.

You also need PFM - Web Console in order to use PFM - RM for Platform to monitor the operation of monitored hosts.

(5) Environment settings required for collecting performance data (for UNIX)

PFM - RM for Platform uses SSH to collect performance data from monitored hosts. Performance data cannot be collected if SSH connection settings have not been specified. Because SSH authentication uses the public key authentication method, you must specify public key authentication settings. You might need to install other appropriate packages because OS commands are used to collect performance data.

The following describes the required SSH settings.

(a) Installing packages

■ RPM packages required for the PFM - RM host

The table below lists the RPM packages required for the PFM - RM host. For details, see the *Release Notes* for this product.

Table 3–31: RPM packages required for the PFM - RM host

No.	Software name	OS	Default
1	OpenSSH	Linux 6 (x64)	Y
2		Linux 6 (x86)	Y
3	Perl	Linux 6 (x64)	Y
4		Linux 6 (x86)	Y

Legend:

Y: Installed by default.

■ Packages required for monitored hosts (SSH)

For details about the packages required for monitored hosts (SSH), see *3.1.1(6)(b) Installing software and packages*.

■ Packages required for monitored hosts (commands)

For details about the packages required for monitored hosts (commands), see *3.1.1(6)(b) Installing software and packages*.

(b) SSH connection settings

Specify the SSH connection settings at both the PFM - RM host and the monitored hosts. For details about the SSH connection settings, see *3.2.5 SSH (for UNIX) connection setting method*.

(c) User of a monitored host

If the OS of a monitored host is AIX and a user other than `root` is to collect information, that user must belong to both the `adm` group and the `system` group; otherwise, some information will not be collected.

To ensure that the user belongs to both groups (`adm` and `system`), execute the following command at the connection-target monitored host:

```
$ id
uid=xxx(xxx) gid=x(xxx) groups=0(system),4(adm)
```

For details about the information that will not be collected, see *7. Records*. If the OS of the monitored host is not AIX, this user limitation is not applicable.

(6) Prerequisite when setting the process operation monitoring condition to 4,096 bytes

When using version 10-00 or later of PFM - Manager and PFM - Web Console, you can set the monitoring condition to be used for monitoring performance to a maximum of 4,096 bytes.

When installing PFM - Base or PFM - Manager on the PFM - RM host, use version 10-00 or later.

(7) Preparing to collect information when an error occurs

If a problem occurs, you might have to collect core dump files as information to be used for investigating the problem. Because the output of core dump files depends on the user's environment settings, check the following settings:

Core dump file size setting

The maximum size of core dump files is limited by the root user's core dump file size setting (`ulimit -c`). Set up a script as follows:

```
ulimit -c unlimited
```

If this setting violates the security policy of the machine being used, turn the script setting into a comment line as shown in the following:

```
# ulimit -c unlimited
```

Important note

When you turn the script setting into a comment, the core dump will not be output when a trigger for outputting a core dump file occurs, such as when a segmentation error or bus error occurs in a process. Consequently, you might not be able to investigate the cause of the error.

Kernel parameter setting related to core dump (Linux only)

If you change the output destination for the core dump files and their file names from the default settings by using Linux kernel parameter (`kernel.core_pattern`), you might not be able to collect the core dump files. Therefore, we recommend that you do not change the Linux kernel parameter (`kernel.core_pattern`) settings.

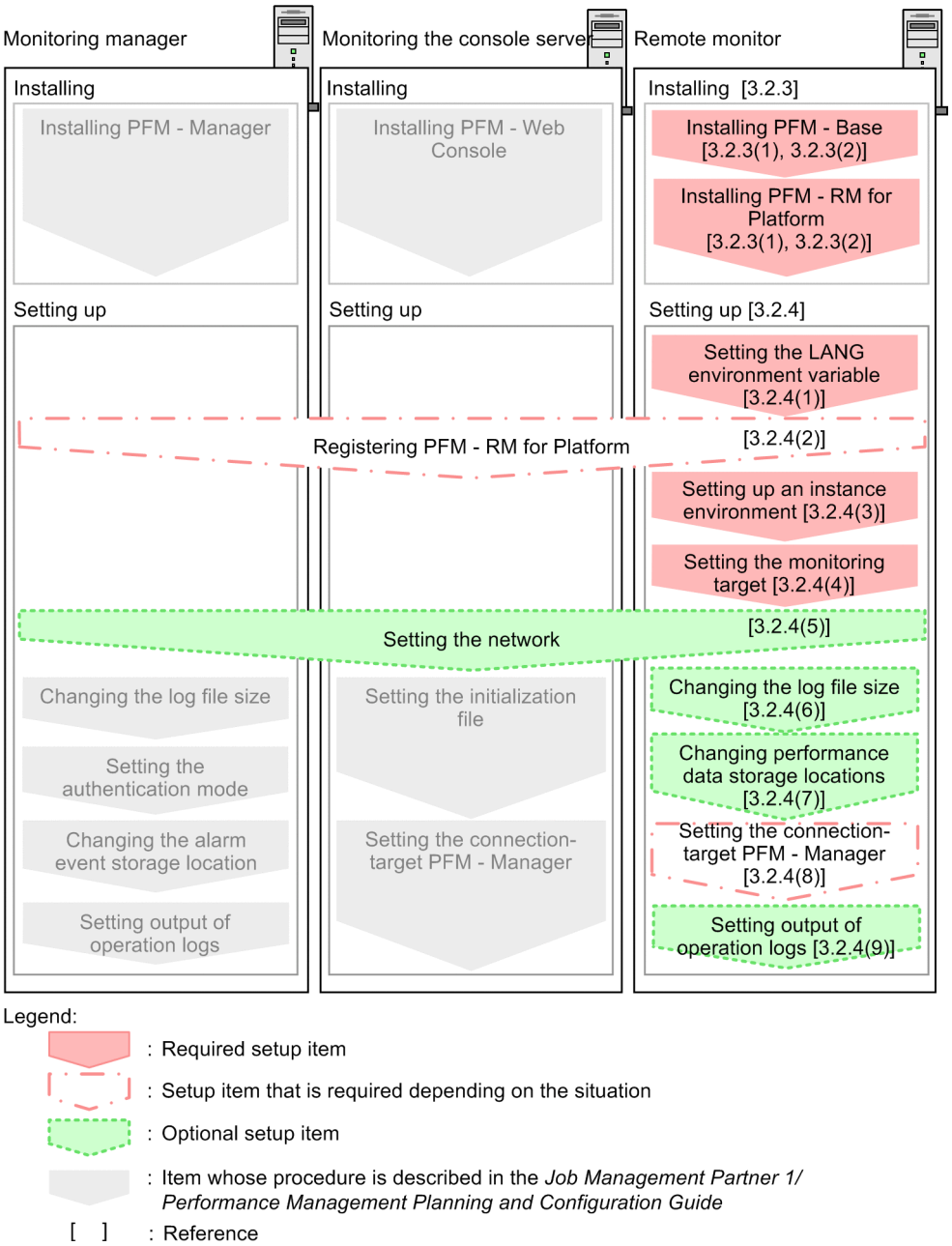
3.2.2 Flow of installation and setup for the UNIX edition

This subsection describes the procedures for installing and setting up PFM - RM for Platform.

For details about how to install and set up PFM - Manager and PFM - Web Console, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The following figure shows the procedures for installing and setting up PFM - RM for Platform.

Figure 3–12: Installation and setup procedures (for UNIX)



For setup commands that require a user input, you can select whether to execute the commands in the interactive or non-interactive mode.

When a command is executed in the interactive mode, the user must enter values by following the instruction displayed by the command.

When a command is executed in the non-interactive mode, no user input is required because option specifications or definition files replaces the input steps required during command execution. Furthermore, batch processing or remote execution can automate the setup procedure, thereby reducing the workload on the administrator and the cost of operations. Commands in the non-interactive mode are convenient in the following cases:

- You want to change the password used for connecting to monitoring targets on a regular basis.
- You want to improve the efficiency of the procedure for adding multiple monitoring targets.

For details about commands, see the manual *Job Management Partner 1/Performance Management Reference*.

3.2.3 Installation procedure for the UNIX edition

This subsection describes how to install PFM - RM for Platform in a UNIX environment.

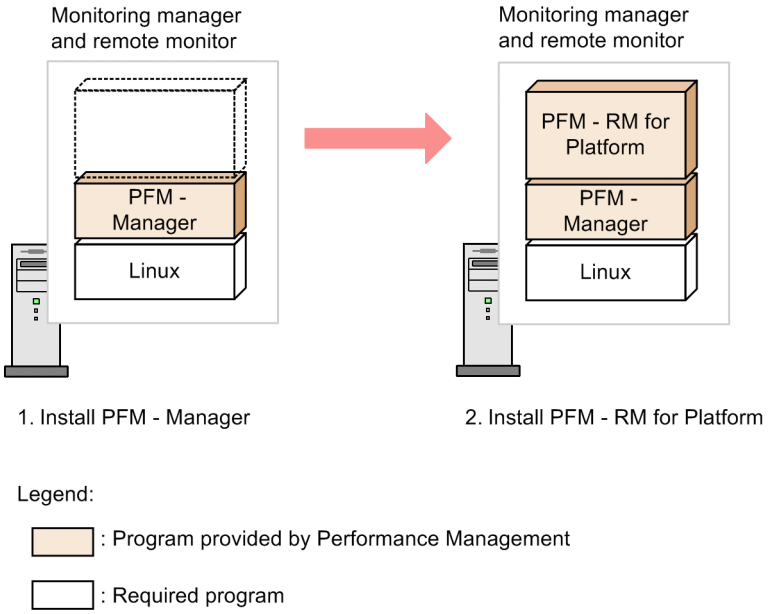
(1) Program installation sequence

This subsection describes the order in which PFM - RM for Platform and its prerequisite programs are to be installed.

When installing PFM - RM for Platform on the PFM - Manager host

Install PFM - Manager first, and then install PFM - RM for Platform.

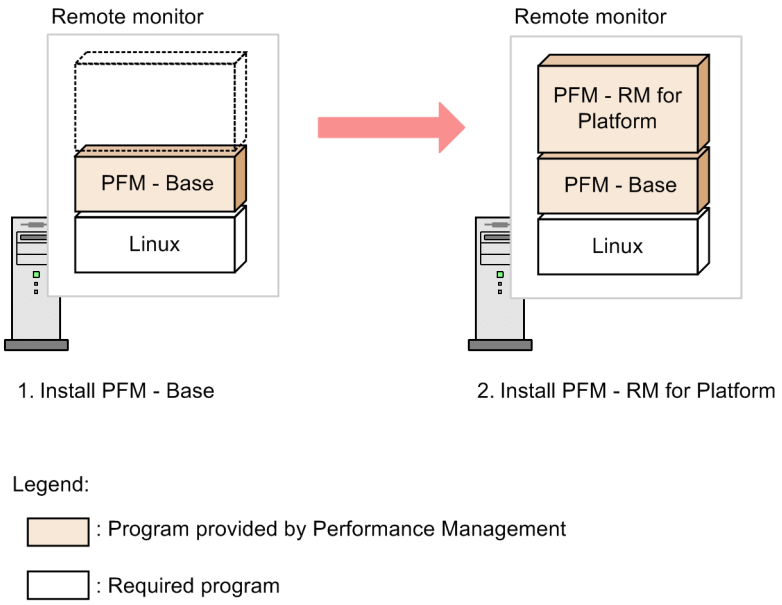
Figure 3–13: Program installation sequence (when PFM - RM for Platform and PFM - Manager are on the same host (for UNIX))



When installing PFM - RM for Platform on a host other than the PFM - Manager host

Install PFM - Base first, and then install PFM - RM for Platform.

Figure 3–14: Program installation sequence (when PFM - RM for Platform and PFM - Base are on the same host (for UNIX))



If you install multiple PFM - RMs on the same host, you can install the individual PFM - RMs in any order.

(2) Installation procedure

This subsection describes how to install PFM - RM for Platform.

There are two ways to install PFM - RM for Platform in a UNIX environment: by using the distribution media or by using JP1/Software Distribution for remote installation. For details about the method that uses JP1/Software Distribution, see the *Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide*, *Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide*, for UNIX systems, and *Job Management Partner 1/Software Distribution Client Description and User's Guide*, for UNIX systems.

To install from the distribution media:

1. At the host where PFM - RM for Platform is to be installed, log on as a superuser. Alternatively, use the `su` command to change to a superuser.

2. At the local host, stop all services of Performance Management programs that are running.
   If any services of Performance Management programs are running, stop all of them.

   Note concerning the services to be stopped

   You must stop all Performance Management services on physical and logical hosts. For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3. Insert the distribution media into the appropriate drive.

4. Execute the `mount` command to mount the distribution media.
   The following example mounts the distribution media in the mount directory:

   ```
   /bin/mount -r -o mode=0544 device-special-file-name mount-directory
   ```

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

```
mount-directory/LINUX/SETUP mount-directory
```

The Hitachi Program Product Installer starts and the initial window is displayed.

6. In the initial window, enter `l`.

   A list of the programs that can be installed is displayed.

7. Select PFM - RM for Platform, and then enter `I`.

   PFM - RM for Platform is installed. To select another program, move the cursor to the desired program, and then press the space key to select it.

8. When installation is completed successfully, enter `Q`.

   The initial window of the Hitachi Program Product Installer is displayed again.

3.2.4 Setup procedure for the UNIX edition

This subsection describes how to set up PFM - RM for Platform.

Optional indicates the following setup items:

- Setup item required depending on the environment in use
- Setup item for changing a default setting

(1) Setting the LANG environment variable

You must set the `LANG` environment variable.

The table below shows the `LANG` environment variable values supported by PFM - RM for Platform. Before you set a `LANG` environment variable value, check that the applicable language environment has been installed and configured correctly. Invalid installation and configuration of the language environment might result in encoding errors and illegal rewriting of definition data.

Table 3–32: LANG environment variable values supported by PFM - RM for Platform

No.	Language		LANG environment variable value
1	Japanese	UTF-8 code	• `ja_JP.UTF-8` • `ja_JP.utf8`
2	English (no Japanese)		`C`

Note;

If you specify a value not listed in this table, PFM - RM for Platform runs in `C`.

Notes regarding setting of the LANG environment variable

The language for the common message log is determined by the `LANG` environment variable that is specified during service startup or command execution. Therefore, character strings in multiple language codes, such as both Japanese and English, might be present.

(2) Registering PFM - RM for Platform

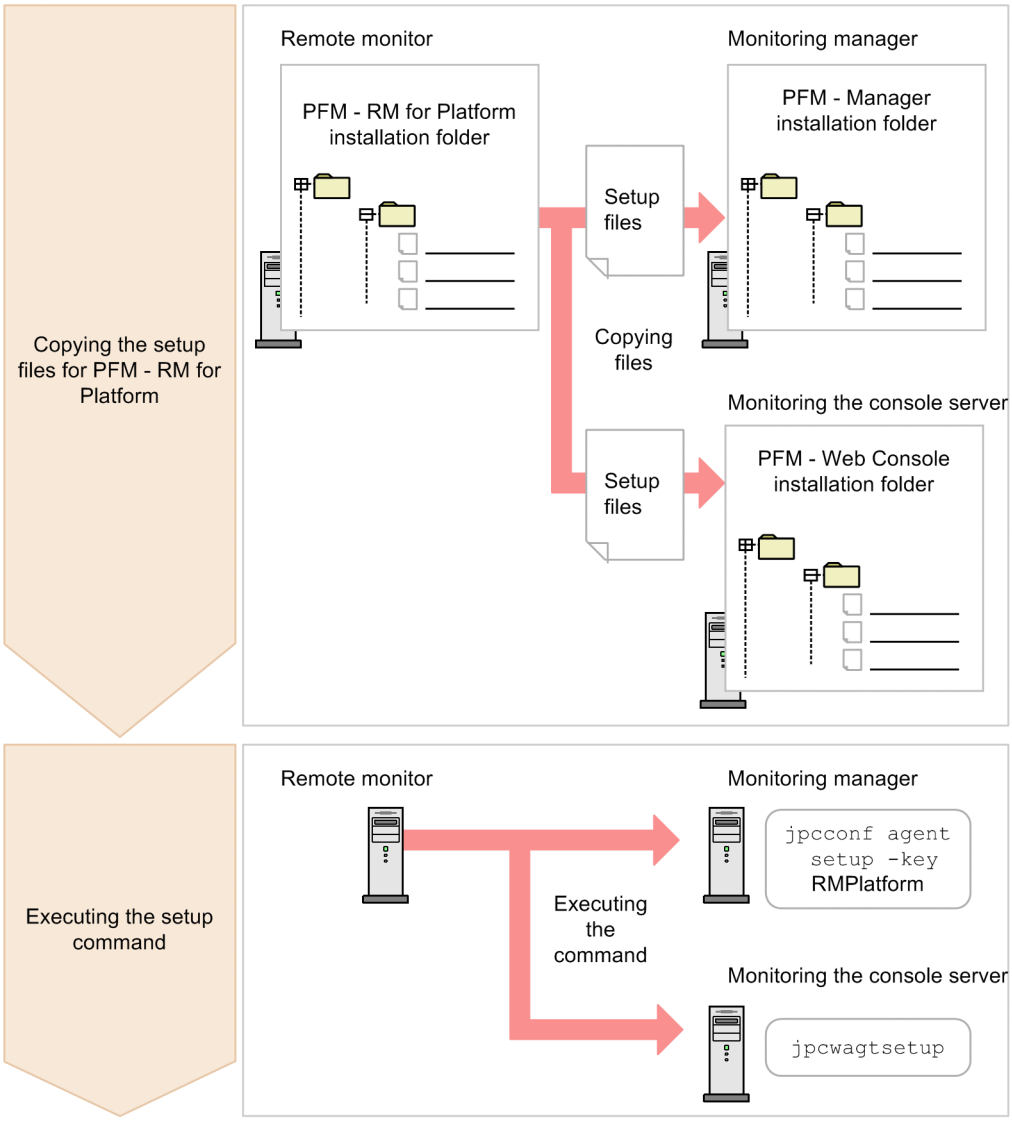
To achieve central management of PFM - RM for Platform in the Performance Management system, you must register PFM - RM for Platform into PFM - Manager and PFM - Web Console.

You must register PFM - RM for Platform at the following times:

- Whenever you add a new PFM - RM for Platform in the Performance Management system.
  Note: If a PFM - RM for Platform has already been registered and you are adding a new PFM - RM for Platform of the same version, there is no need to register the new PFM - RM for Platform.
- When you update the Data model version for the registered PFM - RM for Platform.

The following figure shows the procedure for registering PFM - RM for Platform.

Figure 3–15: Procedure for registering PFM - RM for Platform (for UNIX)



Notes about registering PFM - RM for Platform

- Register PFM - RM for Platform before you set up an instance environment.
- If you install different versions of PFM - RM for Platform on separate hosts, set up old versions before you set up new versions.

- If you install PFM - RM for Platform on the same host as where PFM - Manager is installed, the `jpcconf agent setup` command executes automatically.
- When PFM - RM for Platform is registered, folders named `RM Platform` are created on the **Reports** and **Alarms** pages of PFM - Web Console. If you have already created a folder or file named `RM Platform` on the **Reports** page, you must rename it before starting the registration procedure.

The following subsections describe how to register PFM - RM for Platform.

(a) Copying the setup files for PFM - RM for Platform

Copy the setup files from the PFM - RM host to the hosts where PFM - Manager and PFM - Web Console are installed.

To copy the setup files:

1. Stop PFM - Web Console.
   If PFM - Web Console is running, stop it.

2. Copy the setup files in binary mode.
   Copy the files from the PFM - RM host to the PFM - Manager and PFM - Web Console hosts.
   The following table lists the source file storage locations and the copy destination locations.

   Table 3–33: Setup files to be copied (for UNIX))

No.	Source (setup files for PFM - RM for Platform)	Target		
		Program name	OS	Target folder
1	`/opt/jp1pc/setup/jpcagt7w.EXE`	PFM - Manager	Windows	*PFM-Manager-installation-folder*`\setup`
2	`/opt/jp1pc/setup/jpcagt7u.Z`		UNIX	`/opt/jp1pc/setup/`
3	`/opt/jp1pc/setup/jpcagt7w.EXE`	PFM - Web Console	Windows	*PFM-Web-Console-installation-folder*`\setup`
4	`/opt/jp1pc/setup/jpcagt7u.Z`		UNIX	`/opt/jp1pcwebcon/setup/`

(b) Executing the setup command at the PFM - Manager host

At the PFM - Manager host, execute the setup command for PFM - RM for Platform.

Execute the following command:

```
jpcconf agent setup -key RMPlatform
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf agent setup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Notes about executing the command

Before you execute the command, stop all Performance Management programs and services at the local host. An error might occur if the `jpcconf agent setup` command is executed before all Performance Management programs and services have stopped completely. If an error has occurred, make sure that all Performance

Management programs and services have stopped completely, and then re-execute the `jpcconf agent setup` command.

After you have executed the setup command at the PFM - Manager host, you might delete the setup files for PFM - RM for Platform that were copied to the PFM - Manager.

(c) Executing the setup command at the PFM - Web Console host

At the PFM - Web Console host, execute the setup command for PFM - RM for Platform.

Execute the following command:

```
jpcwagtsetup
```

After you have executed the setup command at the PFM - Web Console host, you might delete the setup files for PFM - RM for Platform that were copied to the PFM - Web Console.

(3) Setting up an instance environment

Set up an instance environment for PFM - RM for Platform at the PFM - RM host. To set multiple instance environments, repeat this procedure. In PFM - RM for Platform, you can define a maximum of 50 monitoring targets in a single instance environment.

Notes about setting instance environments

Before you set instance environments, make sure that the procedure described in *3.2.1(5) Environment settings required for collecting performance data (for UNIX)* has been completed and the correct environment has been set up.

The table below lists and describes the instance environment setting items and values. Check this information before you start operations.

Use the `jpcconf inst setup` command to set up an instance environment. For details about how to execute the `jpcconf inst setup` command, see *(a) Execution in the interactive mode* and *(b) Execution in the non-interactive mode*.

Table 3–34: Instance environment setting items and values for PFM - RM for Platform (for UNIX)

No.	Item name#1	Description	Setting	Default
1	`Interval`	Specifies a collection interval for the collection process.	Specify a value in the range from 60 to 3,600 (seconds).	`300`
2	`Std_Category`#2	Specifies whether the collection process is to collect basic information (`PI` and `PI_CPU` records).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	`Y`
3	`Disk_Category`#2	Specifies whether the collection process is to collect disk information (`PI_PDSK` and `PI_LDSK` records).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	`Y`
4	`Network_Category`#2	Specifies whether the collection process is to collect network information (`PI_NET` record).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	`Y`

No.	Item name#1	Description	Setting	Default
5	Ps_Category#2	Specifies whether the collection process is to collect process information (PD_APS, PD_ASVC, PD_APP2, PD_APPC, and PD_APPD records).	Specify one of the following values: • Y: Collect • N: Do not collect	Y
6	Log_Size	Specifies the maximum size of one agent log file.#3	Specify a value in the range from 1 to 32 (megabytes).	3

#1

When the jpcconf inst setup command is executed in the non-interactive mode, this item name is used as a product-specific label in the definition file. For details about commands in the non-interactive mode, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

#2

The settings for Std_Category, Disk_Category, Network_Category, and Ps_Category are given higher priority than the collection settings for the individual records.

For example, if you set Std_Category to N (do not collect), a PI record is handled as follows:

- The PI record information is not recorded in the Store database.
- If an attempt is made to display a real-time report based on PI records, the KAVJS5001-I error message is displayed.
- If an alarm is bound to a PI record, that alarm will not function.

#3

The following formula can be used to estimate the agent log file size:

Agent log (megabytes) = $((a \times 24 \times 3600) \div b \times 4) \div (4 \times 1024)$

Legend:

a: Number of days agent logs are stored

b: Interval value of the instance

For agent logs, the maximum number of files collected for each instance is (8 + the number of monitoring targets × 4). If there is not enough free space on the hard disk, agent logs result in an output error. For details about agent logs, see *9.3 Log information to be collected for troubleshooting*.

(a) Execution in the interactive mode

1. Execute the jpcconf inst setup command.

   The command sets an instance environment with an instance name of inst1:

```
jpcconf inst setup -key RMPlatform -inst inst1
```

2. Set up an instance environment for PFM - RM for Platform.

   Enter each instance environment setting for PFM - RM for Platform according to the command's instructions. For details about each instance environment setting, see Table *3-34 Instance environment settings for PFM - RM for Platform (for UNIX)*. After you enter each setting, press the **Enter** key. To use a displayed default value, press the **Enter** key.

   The following example sets all instance environment settings to the default values:

```
/opt/jp1pc/tools>jpcconf inst setup -key RMPlatform -inst inst1
 Interval                [300]                :<Enter>
 Std_Category            [Y]                  :<Enter>
 Disk_Category           [Y]                  :<Enter>
 Network_Category        [Y]                  :<Enter>
 Ps_Category             [Y]                  :<Enter>
 Log_Size (MB)           [3]                  :<Enter>
KAVE05080-I The instance environment is now being created.
(servicekey#=RMPlatform, inst=inst1)
```

```
KAVE05081-I The instance environment has been created.
(servicekey#=RMPlatform, inst=inst1)
```

#

If PFM - Manager's product name display function is disabled, `agt7` is displayed for `servicekey`.

(b) Execution in the non-interactive mode

1. Execute the `jpcconf inst setup` command to create a definition file template.

   Execute the command as follows:

   ```
   jpcconf inst setup -key RMPlatform -noquery -template definition-file-name
   ```

   Sections and labels that correspond to the instance environment settings are output to a definition file. Note that the value for the label of the `Instance Definitions` section is left blank.

2. Edit the definition file template created in step 1.

   Edit the template setting values according to the instance environment.

   For details about the product-specific labels to be specified in the definition file, see Table *3-34 Instance environment settings for PFM - RM for Platform (for UNIX)*.

   Shown below is an example of coding a definition file. Specify values for the labels in the `Instance Definitions` section according to the instance environment.

   ```
   [Common Definitions]
   Definition File Version=0001

   [Product Information]
   Product ID=7

   [Instance Definitions]
   Interval=300
   Std_Category=Y
   Disk_Category=Y
   Network_Category=Y
   Ps_Category=Y
   Log_Size=3
   ```

3. Execute the `jpcconf inst setup` command to set up the instance environment for PFM - RM for Platform.

   Shown below is an example of executing a command for setting up an instance environment where `inst1` is the instance name. For the `-input` option, specify the definition file edited in step 2.

   ```
   jpcconf inst setup -key RMPlatform -inst inst1 -noquery -input definition-
   file-name
   ```

Note;

If the definition file contains confidential information such as passwords, save the definition file in a secure location, and delete it after you have used it. If you want to transfer the definition file between hosts, we recommend that you use a secure file transfer protocol, such as Secure File Transfer Protocol (SFTP), which is FTP over an SSH tunnel.

When all of the settings have been completed, an instance environment can be built. The following table shows the directory structure of an instance environment.

Table 3–35: Directory structure of an instance environment (for UNIX)

No.	Storage directory	File name	Description
1	`/opt`[#1]`/jp1pc/agt7/agent/`*instance-name*	`jpcagt.ini`	Service startup initialization file of Remote Monitor Collector
2		`jpcagt.ini.lck`	Lock file for the service startup initialization file of Remote Monitor Collector (for each instance)
3		`jpcagt.ini.model`[#2]	Sample of a service startup initialization file of Remote Monitor Collector
4		`status.dat`	Intermediate file for internal processing
5		`tstatuses.dat`	Virtual Agent status information[#3]
6		`targetlist.ini`	List of monitoring targets
7		`grouplist.ini`	List of groups
8		`GARULES.DAT`	Grouping rule description file
9		`targets`	Storage folder for remote agent
10		`groups`	Storage folder for group agent
11		`log`	Storage folder for log files
12	`/opt`[#1]`/jp1pc/agt7/store/`*instance-name*	`*.DB`	Performance data file
13		`*.IDX`	Index files for performance data files
14		`*.LCK`	Lock files for performance data files
15		`jpcsto.ini`	Service startup initialization file of Remote Monitor Store
16		`jpcsto.ini.model`[#2]	Model file for the service startup initialization file of Remote Monitor Store
17		`status.dat`	Intermediate file for internal processing
18		`*.DAT`	Definition file for a data model
19		`dump`	Export folder
20		`backup`	Backup folder
21		`partial`	Partial backup folder
22		`import`	Import folder
23		`log`	Storage folder for log files

#1

If you run a logical host, replace `opt` with *environment-directory*. An environment directory is a directory on the shared disk that is specified when the logical host is created.

#2

Use these sample files when you want to restore the settings to their initial values from when the instance environment was configured.

#3

Created when the health check function is enabled.

To change an instance environment, re-execute the `jpcconf inst setup` command, and then update each instance environment setting. For details about updating the instance environment settings, see *3.6.2 Updating an instance environment*.

You can change some settings by using PFM - Web Console to edit properties. For details about the information that can be changed by editing properties, see *E.2 List of properties of the Remote Monitor Collector service*.

In an instance environment, the service IDs are as follows:

Service IDs in an instance environment

- For the Remote Monitor Collector service
  `7A`*instance-number instance-name*`[`*host-name*`]`
- For the Remote Monitor Store service
  `7S`*instance-number instance-name*`[`*host-name*`]`
- For the Group Agent service
  `7A`*instance-number instance-name*`[All@`*host-name*`]`

In PFM - RM for Platform, the instance name specified in the `jpcconf inst setup` command is displayed.

If the host name of the PFM - RM host is `host1` and `inst1` is specified as the instance name, the service IDs will be as follows:

- For the Remote Monitor Collector service
  `7A1inst1[host1]`
- For the Remote Monitor Store service
  `7S1inst1[host1]`
- For the Group Agent service
  `7A1inst1[All@host1]`

For details about the service IDs, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

You cannot set up an instance environment by using PFM - Web Console's facility for distributing agent-specific properties.

(4) Setting the monitored host

Set information about the monitored host for the instance that was set up in *(3) Setting up an instance environment*. You can set a maximum of 50 monitored hosts for a single instance. To set multiple monitored hosts, repeat this procedure. However, if the number of monitored hosts is large, the desired performance might not be achieved depending on the system's performance and environment. In this case, reduce the number of monitored hosts. Carefully validate the performance before starting operation.

You must specify physical hosts as monitoring targets. PFM - RM for Platform does not support monitoring of logical hosts.

Using common account information for monitored hosts

If `Y` is set for `UseCommonAccount` in the setting items for the monitored host, common account information (ssh) that was created beforehand for the monitored host is used.

The following table lists the correspondence between the setting items for the monitored host and those for common account information.

Table 3–36: Correspondence between the setting items for the monitored host and those for common account information

Setting items for the monitored host	Setting items for common account information (ssh)	Description
`User`	`User`	User name
`Private_Key_File`	`Private_Key_File`	Private key file name

Note 1:

Common account information can only be used in an environment where both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

Note 2:

Common account information must be created on the PFM - RM host beforehand.

Use the `jpcconf acc setup` command to create common account information. For details about the `jpcconf acc setup` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Note 3:

The settings and precautions required for creating common account information (ssh) are the same as for the corresponding monitoring target setting items. See the corresponding monitoring target setting items in Table 3-37.

Important note

To use common account information, you need to unify the account information settings so that you can connect to multiple monitoring targets by using a single set of account information. For this reason, there is a risk of greater negative impact if common account information is leaked. To avoid such a risk, determine whether to use common account information after considering security measures and information management.

Notes about setting the monitored host

- Before you set a monitored host, make sure that the procedure described in *3.2.1(5) Environment settings required for collecting performance data (for UNIX)* has been completed and the environment has been set up.
- Even if an invalid value is specified when setting up the monitored host, the monitored host creation command terminates normally. However, if you start record collection with any invalid settings, performance data is not collected. For details about troubleshooting when performance data is not collected, see *9.2.5(3) PFM - RM for Platform was started, but no performance data is being collected*.

(a) Monitoring target setting items and values

The table below lists and describes the setting items and values for a monitored host. Check this information before you start operations.

Use the `jpcconf target setup` command to set up a monitored host.

For details about how to execute the `jpcconf target setup` command, see *(c) Execution in the interactive mode* and *(d) Execution in the non-interactive mode*.

For details about the `jpcconf target setup` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Table 3–37: Setting items and values for the monitored host in PFM - RM for Platform

No.	Item name#1	Description	Setting	Default
1	`Target Host`	Specifies the name of the monitored host. Specify a host name that can be resolved.#2 The specified monitored host name is used during performance data collection and health checking. If JP1/IM or NNM is linked, this name is also used as the event host name.	From 1 to 32 bytes of alphanumeric characters and the hyphen (-) are permitted. The name cannot begin with a hyphen (-). The specified value must be unique within the instance.#3	No monitored host name is specified.#4
2	`UseCommonAccount`	Specifies whether to use common account information.	Specify one of the following values: • `Y`: Use • `N`: Do not use	`N`
3	`User`#5	Specifies the user used to log on to the monitored host. PFM - RM for Platform uses this user to log on to the monitored host and collect performance data.	From 1 to 256 bytes of characters are permitted. The tab character is not permitted.	--
4	`Private_Key_File`	Specifies the name of the private key file#6 that is used with the SSH public key method.	From 1 to 256 bytes of characters are permitted. The tab character is not permitted.	`/opt/jp1pc/agt7/.ssh/agt7`
5	`Port`	Specifies the port number of the SSH server on the monitored host.	Specify a value in the range from 1 to 65,535.	`22`

Legend:

--: No default is set.

#1

When the `jpcconf target setup` command is executed in the non-interactive mode, this item name is used as a product-specific label in the definition file. For details about commands in the non-interactive mode, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

#2

To collect performance data and perform health checking, the name must be resolvable at least by the PFM - RM host.

If the JP1/IM linkage facility is used, the name must be resolvable by the JP1/IM host. If the NNM linkage facility is used, the name must be resolvable by the PFM - Manager host and the NNM host.

#3

`All` cannot be used because it is a reserved word for group agents.

#4

If the specification is omitted, the host name of the PFM - RM host is assumed.

#5

For the login shell for the user to be specified, specify `bash`, `bsh`, or `ksh`.

This also applies when `User` in common account information (ssh) is used.

#6

If a connection attempt using the specified private key fails, the private key set by the SSH server (IdentityFile) is used for connection.

This also applies when `Private_Key_File` in common account information (ssh) is used.

(b) Monitored host setting items that are not displayed

Monitored host setting items are usually displayed by executing a command, but some are not displayed depending on the contents of other setting items or for some other reason. The table below describes conditions that prevent monitored host setting items from being displayed. It also shows the input values that are used in such cases.

Table 3–38: Conditions that prevent monitored host setting items from being displayed, and input values that are used

Item name	Conditions that prevent monitored host setting items from being displayed, and input values that are used
`UseCommonAccount`	This item is not displayed in an environment where common account information cannot be used.
`User`	These items are not displayed when `Y` is specified for `UseCommonAccount` in an environment where common account information can be used. Input value: The value in the corresponding common account information is used as the input value. For details about the corresponding common account information, see Table 3-36.
`Private_Key_File`	

Note:

Here, *an environment where common account information can be used* refers to an environment where both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

(c) Execution in the interactive mode

1. Execute the `jpcconf target setup` command.

   In PFM - RM for Platform, we recommend that you specify the host name of the monitored host as the name of the monitoring target.

   The following example sets the monitored host `targethost1` with instance name `inst1` as the monitoring target:

```
jpcconf target setup -key RMPlatform -inst inst1 -target targethost1
```

2. Set up the monitoring target for PFM - RM for Platform.

   Enter setting items for the monitored host according to the instructions given by the command. For details about the setting items for the monitored host, see Table 3-37. After you input each setting item, press the **Enter** key to set it. To use a displayed default value, simply press the **Enter** key.

   The following shows an example of setting up a monitoring target:

   Conditions for the PFM - RM host to be set up

   - SSH client program: `:/usr/bin/ss`
   - Private key: `/opt/jp1pc/agt7/.ssh/agt7`

   Conditions for the monitored host to be set up

   - Host name: `targethost1`
   - User: `ssh-user`
   - Port number of SSH: `22`

```
/opt/jp1pc/tools>jpcconf target setup -key RMPlatform -inst inst1 -target
targethost1
 Target Host              []                      :targethost1<Enter>
 UseCommonAccount#1       [N]                     :<Enter>
 User#2                                           :ssh-user<Enter>
 Private_Key_File#2   [/opt/jp1pc/agt7/.ssh/agt7]:<Enter>
 Port                        [22#3]               :<Enter>
KAVE05361-I The monitoring target is now being added.
(servicekey#4=RMPlatform, inst=inst1, target=targethost1)
KAVE05362-I The monitoring target has been added.
(servicekey#4=RMPlatform, inst=inst1, target=targethost1)
```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

This item is not displayed when `Y` is specified for `UseCommonAccount`.

#3

If the port number used in SSH is not `22`, change the value of `Port` to the port number used in SSH.

#4

If PFM - Manager's product name display function is disabled, `agt7` is displayed for `servicekey`.

(d) Execution in the non-interactive mode

1. Execute the `jpcconf target setup` command to create a definition file template.

```
jpcconf target setup -key RMPlatform -noquery -template definition-file-
name
```

Sections and labels that correspond to the monitored host setting items are output to a definition file. Note that the value for the label of the `Target Definitions` section is left blank.

2. Edit the definition file template created in step 1.

Edit the template setting values as required for the monitored host.

For details about the product-specific labels to be specified in the definition file, see Table 3-37.

Shown below is an example of coding a definition file. Specify values for the labels in the `Target Definitions` section as required for the monitored host.

```
[Common Definitions]
Definition File Version=0001

[Product Information]
Product ID=7

[Target Definitions]
Target Host=targethost1
UseCommonAccount#1=
User#2=user1
Private_Key_File#2=/opt/jp1pc/agt7/.ssh/agt7
Port=22
```

#1

This item is not displayed in an environment where common account information cannot be used.

#2

There is no need to specify a value for this item when `Y` is specified for `UseCommonAccount`.

3. Execute the `jpcconf target setup` command to set up the monitoring target for PFM - RM for Platform.

Shown below is an example of executing a command for setting up a monitoring target where `inst1` is the instance name and `targethost1` is the monitored host. For the `-input` option, specify the definition file edited in step 2.

```
jpcconf target setup -key RMPlatform -inst inst1 -target targethost1 -
input definition-file-name -noquery
```

Note:

If the definition file contains confidential information such as passwords, save the definition file in a secure location, and delete it after you have used it. If you want to transfer the definition file between hosts, we recommend that you use a secure file transfer protocol, such as Secure File Transfer Protocol (SFTP), which is FTP over an SSH tunnel.

When all of the settings have been completed, a monitoring target environment can be built. The following table shows the directory structure of the monitoring target environment.

Table 3–39: Directory structure of the monitoring target environment

No.	Storage directory	File name	Description
1	`/opt`#`/jp1pc/agt7/agent/`*instance-name*`/targets`	*monitoring-target-name*`.ini`	Monitoring target settings file
2		*monitoring-target-name*`.ini.model`	Sample of a monitoring target settings file
3	`/opt`#`/jp1pc/agt7/agent/`*instance-name*`/targets/`*monitoring-target-name*	--	Work directory for the monitoring target

Legend:

--: Not applicable

#

If you run a logical host, replace `opt` with *environment-directory*.

The following service IDs are added by the monitoring target settings:

Service IDs to be added

- Remote Agent service

  `7A`*instance-number instance-name*`[`*monitoring-target-name*`@`*host-name*`]`

  The instance name and monitoring target name will be the values specified in the `jpcconf target setup` command.

  If you specify `host1` as the host name of the PFM - RM host, `inst1` as the instance name, and `targethost1` as the monitoring target name, then the service ID will be as follows:

  `7A1inst1[targethost1@host1]`

For details about the service IDs, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

If you want to change information about the monitoring target, re-execute the `jpcconf target setup` command and update the information. For details about updating a monitoring target, see *3.6.3 Updating a monitoring target*.

You can change some settings by using PFM - Web Console to edit properties. For details about the information that can be changed by editing properties, see *E.3 List of properties of remote agents and group agents*.

(5) Network settings Optional

You must specify network settings only if you need to change the network environment settings based on the network configuration specified where Performance Management is used.

There are two types of network environment settings, as described below. Change network settings as necessary.

- IP address setting

Set this information to use Performance Management in a network that is connected to multiple LANs. You set multiple IP addresses by defining the host names and IP addresses in the `jpchosts` file. Make sure that the specified `jpchosts` file is consistent throughout the entire Performance Management system.

For details about the IP address settings, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Port number setting

  Set the port numbers used by Performance Management. To avoid confusion during operation, make sure that the specified port numbers and service names are consistent throughout the entire Performance Management system.

  For details about the port number settings, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(6) Changing the log file size Optional

The operation status of Performance Management is output to log files unique to Performance Management. This setting is required in order to change the size of these log files.

For the common message log, two files with a size of 2,048 kilobytes each are used by default. For details about changing the common message log, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(7) Changing performance data storage locations Optional

These settings are required in order to change the following settings for the performance data that is managed by PFM - RM for Platform:

- Database storage location

  By default, `/opt/jp1pc/agt7/store/`*instance-name*`/` is set.
- Backup location

  By default, `/opt/jp1pc/agt7/store/`*instance-name*`/backup/` is set.
- Partial backup location

  By default, `/opt/jp1pc/agt7/store/`*instance-name*`/partial/` is set.
- Export location

  By default, `/opt/jp1pc/agt7/store/`*instance-name*`/dump/` is set.
- Import location

  By default, `/opt/jp1pc/agt7/store/`*instance-name*`/import/` is set.

Note

If you use a logical host for operation, replace `opt` with *environment-directory*.

For details about changing performance data storage locations, see *3.6.1 Changing performance data storage locations*.

(8) Setting the connection-target PFM - Manager

You must specify on the PFM - RM host information about the PFM - Manager that manages PFM - RM for Platform. The `jpcconf mgrhost define` command is used to make this setting.

Notes about setting the connection-target PFM - Manager

- Only one PFM - Manager can be set as the connection destination even when multiple PFM - RMs are installed on the same host. A different PFM - Manager cannot be specified for each PFM - RM.

- If PFM - RM for Platform and PFM - Manager are installed on the same host, then the PFM - Manager on the local host is the connection-target PFM - Manager. In this case, you cannot change the connection-target PFM - Manager to any other PFM - Manager. To connect to PFM - Manager on a remote host, install PFM - RM for Platform on a different host than for PFM - Manager.

To set the connection-target PFM - Manager:

1. Stop the Performance Management programs and services.

   If any Performance Management programs and services are running on the local host, stop all of them before starting the setup procedure. If Performance Management programs and services are running during execution of the `jpcconf mgrhost define` command, a message is displayed that asks you to terminate them.

   For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

2. Execute the `jpcconf mgrhost define` command with the host name of the connection-target PFM - Manager specified.

   The following shows an example of command execution when the connection-target PFM - Manager is located on the `host01` host:

   ```
   jpcconf mgrhost define -host host01
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf mgrhost define` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(9) Action log output settings Optional

These settings are required in order to output action logs at the following times:

- When a PFM service starts
- When a PFM service stops
- When the PFM - Manager connection status is changed

An action log contains log information about exceeded threshold values caused by factors such as system overloads; its output is linked with the alarm function. For details about the action log output settings, see *I. Outputting Action Log Data*.

3.2.5 SSH (for UNIX) connection setting method

This subsection describes how to set SSH connection. For SSH authentication, the public key authentication method is used.

To connect SSH, you need the following settings:

- Enabling the SSH server's public key authentication

  Specify this setting at the monitored hosts.
- Creating keys

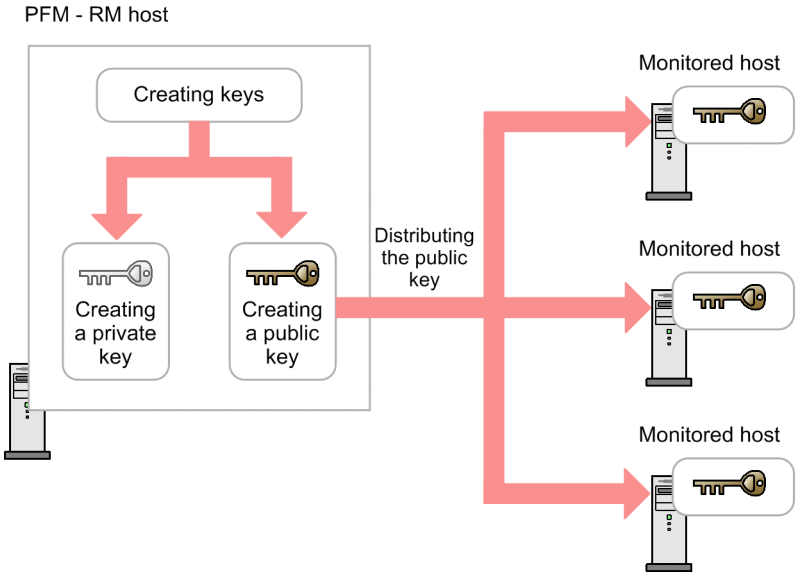
  Specify this setting at the PFM - RM host.
- Placing the private key on the PFM - RM host

  Specify this setting at the PFM - RM host.

- Placing the public key on the monitored hosts
  Specify this setting at the monitored hosts.

The following figure shows the concept of public key authentication.

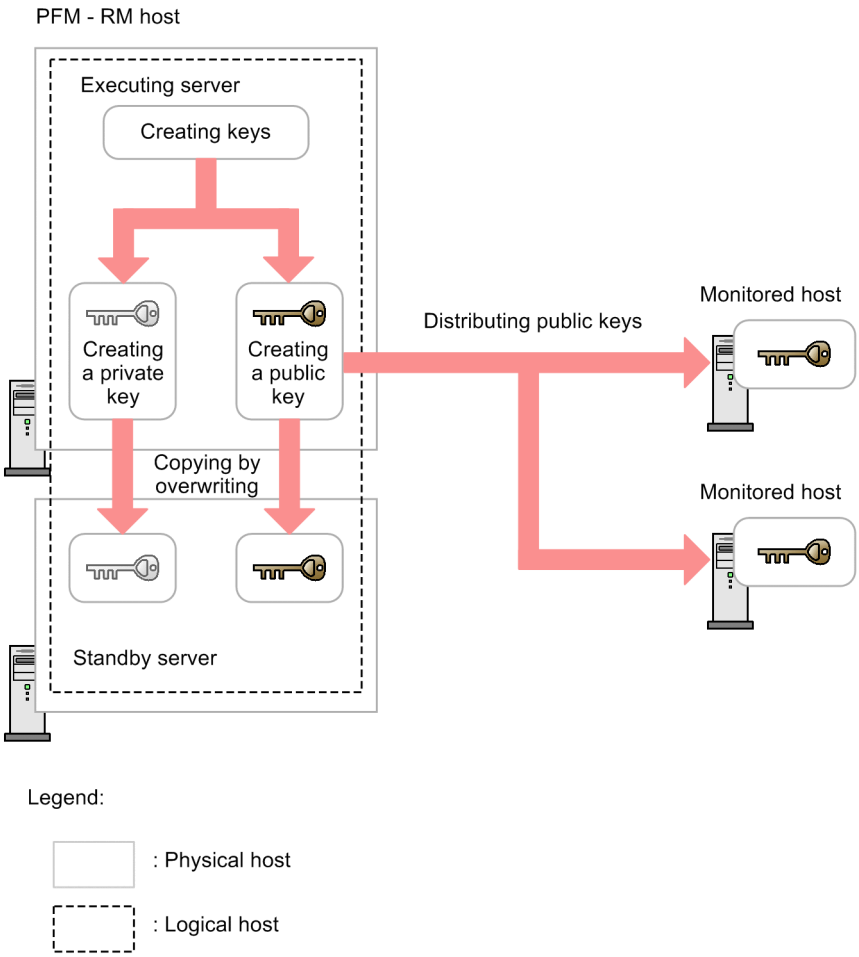
Figure 3–16: Concept of public key authentication



There are two ways to perform public key authentication in a cluster system. One is by using the same key for both executing and standby nodes, and the other is by using different keys.

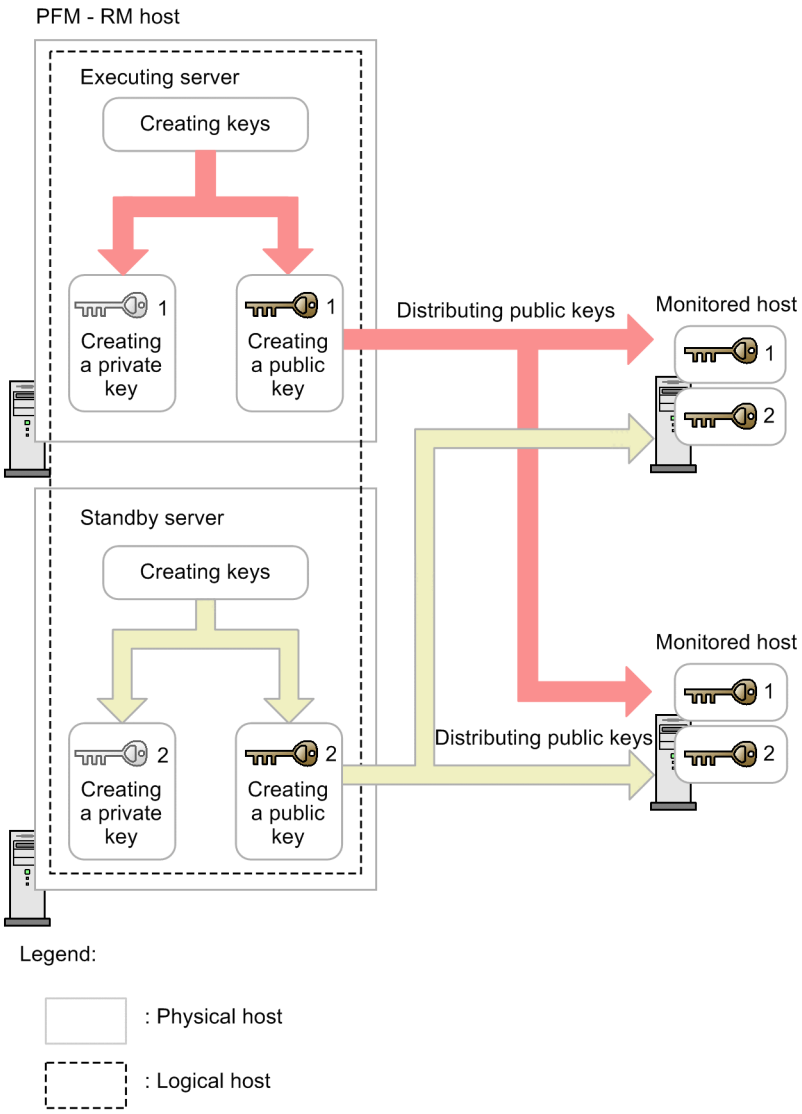
To use the same key for both executing and standby nodes, copy the standby node's key file to the executing node's key file by overwriting. The following figure shows the concept of public key authentication using the same key.

Figure 3–17: Concept of public key authentication (using the same key for both executing and standby nodes)



To use different keys for the executing and standby nodes, you must register the key files for both the executing node and the standby node into the monitored hosts. The following figure shows the concept of public key authentication using different keys.

Figure 3–18: Concept of public key authentication (using different keys for executing and standby nodes)



(1) Enabling the SSH server's public key authentication

To enable public key authentication:

1. Log on to the monitored host as a superuser.
2. Open `/etc/ssh/sshd_config`#.
3. Set `PubkeyAuthentication` to `yes`.
4. Save and close `/etc/ssh/sshd_config`#.
5. Execute the following command to restart the sshd service:

```
[root@TargetHost.ssh]$ /etc/rc.d/init.d/sshd restart
```

Reference note

To log on as a superuser to collect information, open `/etc/ssh/sshd_config`# and change `PermitRootLogin` to `yes`. After that, restart the sshd service.

#

This will be `/opt/ssh/etc/sshd_config` when using HP-UX.

(2) Creating keys

Keys are created automatically. Although you can create keys manually, we recommend that you use the keys that are created automatically unless otherwise necessary.

(a) Creating keys automatically

When you install PFM - RM for Platform, both private and public keys are created automatically in `/opt/jp1pc/agt7/.ssh/`.

The following table lists and describes the storage directory for the private and public keys, the file names, and the settings.

Table 3–40: Storage directory for the private and public keys, the file names, and settings

No.	Storage directory and file name		Attribute	Owner	Description
1	`/opt/jp1pc/agt7/.ssh/`	--	`700`	`root:root`	Hidden directory for storing private and public keys
2		`agt7`	`600`		Private key file
3		`agt7.pub`	`644`		Public key file

Legend:

--: Not applicable

Important note

When you use an automatically created key, do not delete the created key file. If you delete it, the key information will not match the monitored host when the key file is automatically re-created due to an overwrite installation or version upgrade. Consequently, you will no longer be able to connect to the monitored host. If you cannot connect the monitored host following an overwrite installation or version upgrade because the key file has been deleted, perform the procedure described in *(3) Placing the public key on the monitored hosts* and place the public key on all monitored hosts again.

(b) Creating keys manually

This subsection describes how to create keys manually.

You can create keys by logging on to the PFM - RM host as a superuser and then executing the `ssh-keygen` command. The only difference between RSA and DSA encryption is the encryption algorithms; their operation methods are the same.

To create RSA keys:

1. Log on to the PFM - RM host as a superuser.

2. Execute the `ssh-keygen -t rsa` command.

   This command creates an RSA key.

   To create a DSA key, specify the `-s dsa` option instead of the `-t rsa` option.

3. Determine the destination and name of the private key.

   By default, `~/.ssh/id_rsa(RSA)` is set.

4. Press the **Enter** key twice.

   When you are asked to enter a pass phrase for the private key, press the **Enter** key without entering anything. When re-entry is prompted, press the **Enter** key again without entering anything.

The following shows an example of `ssh-keygen -t rsa` command execution:

```
[root@RMHost]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): <Enter>
Enter passphrase (empty for no passphrase): <Enter>
Enter same passphrase again: <Enter>
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@RMHost
```

Notes about creating keys

- Securely manage information about private keys.
- Creation of keys (a pair of public and private keys) should not introduce any problem in any environment or tool because it does not depend on environments or tools. However, after creating keys, you must place the private and public keys appropriately.

(3) Placing the public key on the monitored hosts

Place the created public key on the monitored hosts. When there are multiple monitored hosts, be sure to perform this procedure on all of them.

To place the public key on a monitored host:

1. Log on to the monitored host by using the value that was specified in `User` during monitoring target setup.

   To use common account information, specify the value that is specified in `User` in common account information (ssh).

2. Execute the `cd` command to change the current directory to the `.ssh` directory under the home directory.

   If the `.ssh` directory does not exist under the home directory, create it. For the `.ssh` directory attribute, specify `700` or `755`. For the owner and group, specify the same as those specified for the user who was specified during the setup of the monitored host. If the attribute, owner, or group setting of the home directory or the `.ssh` directory is invalid, SSH connection might fail.

3. Execute the `scp` command.

   The public key file that has already been created is received.

4. Execute the `cat` command.

The contents of the public key file are redirected to the authentication key file. Also, the contents of the received public key file are added to the authentication key file.

The name of the authentication key file is set by `AuthorizedKeysFile` of `/etc/ssh/sshd_config`. For HP-UX, it is `/opt/ssh/etc/sshd_config`.

By default, `~/.ssh/ authorized_keys` is set.

5. Execute the `rm` command to delete the received public key file.

6. Execute the `chmod` command to change the attribute of the authentication key file to `600`.

An example of performing steps 2 through 6 follows:

```
[ClientUser@TargetHost ]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp root@RMHost:/opt/jp1pc/agt7/.ssh/
agt7.pub .
root@RMHost's password: password
agt7.pub                                  100%  233     0.2KB/s   00:00
[ClientUser@TargetHost .ssh]$ cat agt7.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm agt7.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

You can also execute the `ssh-copy-id` command on the PFM - RM host to place the public key on the monitored hosts. When you use the `ssh-copy-id` command, there is no need to change the specification of the `.ssh` directory in which to place the public key, or the name and attribute of the public key.

To use the `ssh-copy-id` command to place the public key:

1. Log on to the PFM - RM host as a superuser.

2. Execute the `ssh-copy-id` command.

   The public key is copied.

   For details about the `ssh-copy-id` command, see the OpenSSH documentation.

An example of performing steps 1 and 2 follows:

```
[root@RMHost ]$ /usr/bin/ssh-copy-id -i /opt/jp1pc/agt7/.ssh/agt7.pub
ClientUser@TargetHost
29
The authenticity of host 'TargetHost (xxx.xxx.xxx.xxx)' can't be
established.
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'TargetHost,xxx.xxx.xxx.xxx' (RSA) to the list
of known hosts.
ClientUser@TargetHost's password: password
Now try logging into the machine, with "ssh 'ClientUser@TargetHost'", and
check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

(4) Checking the connection and registering a fingerprint

To check whether the PFM - RM host and a monitored host can connect to each other:

1. Log on to the PFM - RM host as a superuser.
2. Using the created private key, execute the `ssh` client command on the monitored host.
   The connection process begins.
3. During the initial connection, register a fingerprint.
   Register the fingerprint of the public key of the monitored host. Here, enter `yes`. When you enter `yes`, the monitored host's command prompt appears.
4. From the monitored host's command prompt, execute the `exit` command to log out from the monitored host.
5. From the PFM - RM host, execute the `ssh` client command on the monitored host to reconnect to it.
   If the monitored host's prompt appears in subsequent connections without you having to enter any information, setup of the connection between the PFM - RM host and the monitored host is completed. From the monitored host's command prompt, execute the `exit` command to log out from the monitored host.
   If an error occurs or an entry is requested, check if the procedure was executed correctly.

The following shows an example of the settings for checking the connection:

```
[root@RMHost]$ /usr/bin/ssh -i /opt/jp1pc/agt7/.ssh/agt7 -p 22
ClientUser@TargetHost
The authenticity of host 'TargetHost (xxx.xxx.xxx.xxx)' can't be
established.
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'TargetHost,xxx.xxx.xxx.xxx' (RSA) to the list
of known hosts.
Last login: Mon Mar 23 17:17:52 2009 from xxx.xxx.xxx.xxx
[ClientUser@TargetHost ~]$ exit
logout

Connection to TargetHost closed.
[root@RMHost]$ /usr/bin/ssh -i /opt/jp1pc/agt7/.ssh/agt7 -p 22
ClientUser@TargetHost
Last login: Mon Mar 23 17:18:00 2009 from xxx.xxx.xxx.xxx
[ClientUser@TargetHost ~]$ exit
logout

Connection to TargetHost closed.
[root@RMHost]$
```

Notes:

- PFM - RM for Platform assumes that fingerprint authentication has already been completed. Because you can register a fingerprint during the initial SSH client connection, we recommend that you complete the procedure described here at that point.
- Confirm that a response is returned in less than 10 seconds when you execute a command such as `uname` on the monitored host from the PFM - RM host.

For details about PFM - Manager startup, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3.2.6 Notes about installation and setup of the UNIX edition

(1) Notes about environment variables

Performance Management uses the `JPC_HOSTNAME` environment variable. Do not set a user-specific `JPC_HOSTNAME` environment variable. If such an environment variable is set, Performance Management will not function correctly.

(2) Notes about installing multiple Performance Management programs on the same host (for UNIX)

The notes about installing multiple Performance Management programs on the same host are the same as for the Windows environment.

See *3.1.7(3) Notes about installing multiple Performance Management programs on the same host (for Windows)*.

(3) Notes about upgrading (for UNIX)

The notes about upgrading are the same as for the Windows environment.

See *3.1.7(4) Notes about upgrading (for Windows)*.

(4) Notes about linking with other systems (for UNIX)

The notes about linking with other systems are the same as for the Windows environment.

See *3.1.7(5) Notes about linking with other systems (for Windows)*.

(5) Notes about installing PFM - RM for Platform in a UNIX environment

This subsection provides notes about installing PFM - RM for Platform in a UNIX environment.

- If you install PFM - RM for Platform in an environment where no Performance Management program has been installed, make sure that there are no folders or files in the installation folder.
- If `Install failed` is displayed on the status bar during installation and the installation fails, collect the `/etc/.hitachi/.hitachi.log` log file. This log file will be overwritten during the next installation process. Make a backup of this file, as required.
- If you install Performance Management programs by adding a link to the installation directory, some files and directories might remain in the linked directory even if you delete all Performance Management programs. You must delete these files and directories manually. Note that during installation, if a linked directory contains files and directories with the same names as source files and directories, those files and directories will be overwritten.
- If the `/opt/jp1pc/setup` directory contains the setup file of PFM - RM for Platform, additional setup of a new PFM - RM for Platform will be executed.
- To run PFM - RM for Platform as services, use an account with superuser permissions.

- Before you install a Performance Management program, check to see if any of the security-related programs described below are installed. If such a program is installed, take appropriate action according to the information provided below.
  - Security monitoring program

    Either terminate the security monitoring program or change its settings so that installation of the Performance Management program will not be affected.
  - Virus detection program

    We recommend that you terminate any virus detection program before you install the Performance Management programs.

    If a virus detection program is running during installation of a Performance Management program, it might slow down the installation process, the installation might fail, or the program might not install correctly.
  - Process monitoring program

    Either terminate the process monitoring program or change its settings so that it does not monitor Performance Management services and processes as well as services and processes of common components.

    Installation of a Performance Management program might fail if these services and processes are started or stopped by the process monitoring program during the installation process.

3.3 Uninstallation and unsetup of the Windows edition

This section describes how to uninstall PFM - RM for Platform and cancel its setup in a Windows environment.

3.3.1 Issues to consider before uninstalling and canceling the setup for the Windows edition

This subsection provides notes about uninstalling PFM - RM for Platform and canceling its setup.

(1) Notes about OS user permissions required for uninstallation

When you uninstall PFM - RM for Platform, make sure that you use an account that has Administrator permissions.

(2) Notes about network

Uninstalling a Performance Management program does not delete the port numbers defined in the `services` file.

(3) Notes about programs

- If you uninstall PFM - RM for Platform while Performance Management programs and services or other programs that reference Performance Management files (such as Windows Event Viewer) are running, some files and folders might remain in the system. In such a case, you must manually delete all files and folders under the installation folder.
- If you uninstall PFM - RM for Platform in the states described below, files or folders might remain. In this case, you must manually delete all files and folders from *installation-folder*`\agt7`. If you are using PFM - RM for Platform in a logical host environment, delete files and folders from *environment-folder*`\jp1pc\agt7` in the same way.
  - A Performance Management program or service is running.
  - Another program (such as Windows Event Viewer) that references a Performance Management file is running.
  - A file or folder under *installation-folder*`\agt7` is being referenced.
- If you attempt to uninstall PFM - RM for Platform while Performance Management programs and services or other programs that reference Performance Management files (such as Windows Event Viewer) are running, a message prompting system restart might be displayed. If this occurs, restart the system to complete the uninstallation procedure.
- If PFM - Base and PFM - RM for Platform are both installed on the same host, PFM - Base cannot be uninstalled unless you uninstall PFM - RM for Platform. In such a case, uninstall PFM - RM for Platform, and then uninstall PFM - Base. Similarly, if PFM - Manager and PFM - RM for Platform are installed on the same host, PFM - Manager cannot be uninstalled unless you uninstall PFM - RM for Platform. In this case, uninstall PFM - RM for Platform, and then uninstall PFM - Manager.

(4) Notes about services

Uninstalling PFM - RM for Platform might not delete the service information that is displayed by the `jpctool service list` command. In such a case, use the `jpctool service delete` command at the host where PFM - Manager is installed to delete the service information. To have the deletion of service information apply to the PFM - Web Console host, you must execute the `jpctool service sync` command to synchronize the agent information between the PFM - Manager host and the PFM - Web Console host.

(5) Other notes

To uninstall Performance Management programs from a host on which PFM - Web Console is installed, close all browser windows before you start the uninstallation.

3.3.2 Procedure for canceling the setup for the Windows edition

This subsection describes how to cancel the setup of PFM - RM for Platform.

(1) Canceling the setup for a monitoring target

To cancel the setup for a monitoring target, first check the name of the monitoring target, and then use the PFM - RM host to delete the monitoring target.

To check the name of a monitoring target, use the `jpcconf target list` command. To delete a configured monitoring target, use the `jpcconf target unsetup` command.

Reference note

There is no need to stop PFM - RM for Platform services while you are deleting a monitoring target.

To delete a monitoring target:

1. Check the name of the monitoring target.

   Execute the `jpcconf target list` command with the service key that indicates PFM - RM for Platform and the instance name specified:

   ```
   jpcconf target list -key RMPlatform -inst inst1
   ```

   The names of all monitoring targets are displayed:

   ```
   Targets:
   targethost1
   targethost2
   Groups:
   All
   ```

2. Delete the desired monitoring target.

   Execute the `jpcconf target unsetup` command with the service key that indicates PFM - RM for Platform, the instance name, and the name of the monitoring target specified:

   ```
   jpcconf target unsetup -key RMPlatform -inst inst1 -target targethost1
   ```

   When the `jpcconf target unsetup` command in this example terminates normally, `targethost1` will no longer be a monitoring target.

   Important note

   If you delete the monitoring targets by executing the `jpcconf target unsetup` command, the service information is automatically deleted from PFM - Manager; therefore, there is no need to execute the

`jpctool service delete` command. The service information is deleted from PFM - Manager at the following times:

- If you execute the `jpcconf target unsetup` command while both PFM - Manager and the PFM - RM service to be deleted are running, PFM - RM requests PFM - Manager to delete the service information, and PFM - Manager deletes the service information.
- If you execute the `jpcconf target unsetup` command while both PFM - Manager and the PFM - RM service to be deleted are stopped, PFM - Manager deletes the service information when the PFM - RM service starts and connects to PFM - Manager.

To apply the deletion of the monitoring target to the PFM - Web Console host, you must execute the `jpctool service sync` command to synchronize the agent information between the PFM - Manager host and the PFM - Web Console host.

Canceling the setup for a monitoring target does not delete the folders and files listed below. You must delete these folders and files manually.

- *installation-folder*#`\agt7\agent\`*instance-name*`\targets\`*monitoring-target-name*
- *installation-folder*#`\agt7\agent\`*instance-name*`\log\target_`*monitoring-target-name*`_`*nn*

#
If you use a logical host for operation, replace *installation-folder* with *environment-folder*`\jp1pc`.

(2) Canceling an instance environment setup

To cancel the setup for an instance environment, first check the name of the instance, and then delete the instance environment. Execute deletion of an instance environment at the PFM - RM host. To check the name of an instance, use the `jpcconf inst list` command. To delete a configured instance environment, use the `jpcconf inst unsetup` command.

To delete an instance environment:

1. Check the name of the instance.
   Execute the `jpcconf inst list` command with the service key that indicates PFM - RM for Platform specified:
   ```
   jpcconf inst list -key RMPlatform
   ```
   For example, if the set instance name is `inst1`, the command displays `inst1`.
2. If any services of PFM - RM for Platform are running in the instance environment, stop all of them.
   For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.
3. Delete the instance environment.
   Execute the `jpcconf inst unsetup` command with the service key that indicates PFM - RM for Platform and the instance name specified.
   For example, if the set instance name is `inst1`, specify the command as follows:
   ```
   jpcconf inst unsetup -key RMPlatform -inst inst1
   ```

This example shows execution in the interactive mode, but you can also execute the `jpcconf inst unsetup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

When the `jpcconf inst unsetup` command terminates normally, the folders configured as the instance environment, the service ID, and the Windows services are deleted.

Important note

Canceling the setup of an instance environment might not delete the service information that is displayed by the `jpctool service list` command. In such a case, use the `jpctool service delete` command at the host where PFM - Manager is installed to delete the service information.

To apply the deletion of the instance environment to the PFM - Web Console host, you must execute the `jpctool service sync` command to synchronize the agent information between the PFM - Manager host and the PFM - Web Console host.

- Instance name: `inst1`
- Host name: `lhost1`
- Service ID of the Remote Monitor Collector service: `7A1inst1[lhost1]`
- Service ID of the Remote Monitor Store service: `7S1inst1[lhost1]`
- Service ID of the Group Agent service: `7S1inst1[All@lhost1]`

```
jpctool service delete -id 7?1inst1[lhost1] -host lhost1
```

```
jpctool service delete -id 7?1inst1[*@lhost1] -host lhost1
```

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

3.3.3 Procedure for uninstalling the Windows edition

To uninstall PFM - RM for Platform:

1. At the host where PFM - RM for Platform is to be uninstalled, log on as a user with Administrator permissions.

2. At the local host, stop the Performance Management programs and services.

   Display the service information to make sure that no services are running. If any Performance Management programs and services are running on the local host, stop all the active programs and services. You must stop all services on both physical and logical hosts.

   For details about how to display service information and how to stop services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3. Select the Performance Management program to be uninstalled.

   From the Windows **Control Panel**, choose **Add/Remove Programs**, and then select the Performance Management program to be uninstalled.

4. Select **Remove**, and then click the **OK** button.

   The selected program is uninstalled.

Notes on uninstalling PFM - RM for Platform from a Windows Server 2008 or Windows Server 2012 environment

If the user account control functionality (UAC) is enabled in the operating system, the User Account Control dialog box might be displayed during uninstallation. If it is displayed, click the **Continue** button to continue uninstallation, or click the **Cancel** button to cancel uninstallation.

Important note

If you changed the WMI connection settings in *3.1.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows)* but the change is no longer necessary, return the settings to their original values. If you specified a private key and a public key to be used for setting up SSH public key authentication in *3.1.6 SSH connection setting method for Windows (when the PFM - RM host is running Windows and the monitored host is running UNIX)*, delete these keys as necessary. Furthermore, if PuTTY and ActivePerl are not needed, uninstall them.

3.4 Uninstallation and unsetup of the UNIX edition

This section describes how to uninstall PFM - RM for Platform and cancel its setup in a UNIX environment.

3.4.1 Issues to consider before uninstalling and canceling the setup for the UNIX edition

This subsection provides notes about uninstalling PFM - RM for Platform and canceling its setup.

(1) Notes about OS user permissions required for uninstallation

When you uninstall PFM - RM for Platform, make sure that you use an account that has the superuser permissions.

(2) Notes about network

Uninstalling a Performance Management program does not delete the port numbers defined in the `services` file.

(3) Notes about programs

- If you uninstall PFM - RM for Platform while Performance Management programs and services or other programs that reference Performance Management files are running, some files and directories might remain in the system. In such a case, you must manually delete all files and directories under the installation directory.
- If PFM - Base and PFM - RM for Platform are both installed on the same host, PFM - Base cannot be uninstalled unless you uninstall PFM - RM for Platform. In such a case, uninstall PFM - RM for Platform, and then uninstall PFM - Base. Similarly, if PFM - Manager and PFM - RM for Platform are installed on the same host, PFM - Manager cannot be uninstalled unless you uninstall PFM - RM for Platform. In this case, uninstall PFM - RM for Platform, and then uninstall PFM - Manager.

(4) Notes about services

- When you uninstall PFM - Manager, make sure that all Performance Management programs and services are stopped throughout the entire Performance Management system.
- Uninstalling PFM - RM for Platform might not delete the service information that is displayed by the `jpctool service list` command. In such a case, use the `jpctool service delete` command at the host where PFM - Manager is installed to delete the service information. To apply the deletion of service information to the PFM - Web Console host, you must execute the `jpctool service sync` command to synchronize the agent information between the PFM - Manager host and the PFM - Web Console host.

3.4.2 Procedure for canceling the setup for the UNIX edition

This subsection describes how to cancel the setup of PFM - RM for Platform.

(1) Canceling the setup for a monitoring target

To cancel the setup for a monitoring target, first check the name of the monitoring target, and then use the PFM - RM host to delete the monitoring target.

To check the name of a monitoring target, use the `jpcconf target list` command. To delete a configured monitoring target, use the `jpcconf target unsetup` command.

Reference note

There is no need to stop PFM - RM for Platform services while you are deleting a monitoring target.

To delete a monitoring target:

1. Check the name of the monitoring target.
   Execute the `jpcconf target list` command with the service key that indicates PFM - RM for Platform and the instance name specified.

   ```
   jpcconf target list -key RMPlatform -inst inst1
   ```

   The names of all monitoring targets are displayed:

   ```
   Targets:
   targethost1
   targethost2
   Groups:
   All
   ```

2. Delete the desired monitoring target.
   Execute the `jpcconf target unsetup` command with the service key that indicates PFM - RM for Platform, the instance name, and the name of the monitoring target specified:

   ```
   jpcconf target unsetup -key RMPlatform -inst inst1 -target targethost1
   ```

   When the `jpcconf target unsetup` command in this example terminates normally, `targethost1` will no longer be a monitoring target.

   ### Important note

   If you delete the monitoring targets by executing the `jpcconf target unsetup` command, the service information is automatically deleted from PFM - Manager; therefore, there is no need to execute the `jpctool service delete` command. The service information is deleted from PFM - Manager at the following times:

   - If you execute the `jpcconf target unsetup` command while both PFM - Manager and the PFM - RM service to be deleted are running, PFM - RM requests PFM - Manager to delete the service information, and PFM - Manager deletes the service information.
   - If you execute the `jpcconf target unsetup` command while both PFM - Manager and the PFM - RM service to be deleted are stopped, PFM - Manager deletes the service information when the PFM - RM service starts and connects to PFM - Manager.

   To apply the deletion of the monitoring target to the PFM - Web Console host, you must execute the `jpctool service sync` command to synchronize the agent information between the PFM - Manager host and the PFM - Web Console host.

   For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Canceling the setup for a monitoring target does not delete the directories and files listed below. You must delete these directories and files manually.

- `/opt`#`/jp1pc/agt7/agent/`*instance-name*`/targets/`*monitoring-target-name*
- `/opt`#`/jp1pc/agt7/agent/`*instance-name*`/log/target_`*monitoring-target-name*`_`*nn*

#
If you use a logical host for operation, replace `opt` with *environment-directory*.

(2) Canceling an instance environment setup

To cancel the setup for an instance environment, first check the name of the instance, and then delete the instance environment. Execute deletion of an instance environment at the PFM - RM host. To check the name of an instance, use the `jpcconf inst list` command. To delete a configured instance environment, use the `jpcconf inst unsetup` command.

To delete an instance environment:

1. Check the name of the instance.
   Execute the `jpcconf inst list` command with the service key that indicates PFM - RM for Platform specified.

   ```
   jpcconf inst list -key RMPlatform
   ```

   For example, if the set instance name is `inst1`, the command displays `inst1`.

2. If any services of PFM - RM for Platform are running in the instance environment, stop all of them.
   For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

3. Delete the instance environment.
   Execute the `jpcconf inst unsetup` command with the service key that indicates PFM - RM for Platform and the instance name specified.
   For example, if the set instance name is `inst1`, specify the command as follows:

   ```
   jpcconf inst unsetup -key RMPlatform -inst inst1
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf inst unsetup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.
   When the `jpcconf inst unsetup` command terminates normally, the directories configured as the instance environment and the service ID are deleted.

Important note

Canceling the setup of an instance environment might not delete the service information that is displayed by the `jpctool service list` command. In this case, use the `jpctool service delete` command on the host where PFM - Manager is installed to delete the service information.

To apply the deletion of the instance environment to the PFM - Web Console host, you must execute the `jpctool service sync` command to synchronize the agent information between the PFM - Manager host and the PFM - Web Console host.

In such a case, use the `jpctool service delete` command at the host where PFM - Manager is installed to delete the service information. After the command executes, restart the PFM - Manager service. The following shows a specification example:

- Instance name: `inst1`
- Host name: `lhost1`
- Service ID of the Remote Monitor Collector service: `7A1inst1[lhost1]`
- Service ID of the Remote Monitor Store service: `7S1inst1[lhost1]`
- Service ID of the Group Agent service: `7S1inst1[All@lhost1]`

```
jpctool service delete -id 7?1inst1[lhost1] -host lhost1
```

```
jpctool service delete -id 7?1inst1[*@lhost1] -host lhost1
```

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

3.4.3 Procedure for uninstalling the UNIX edition

To uninstall PFM - RM for Platform:

1. At the host where a Performance Management program is to be uninstalled, log on as superuser. Alternatively, use the `su` command to change the user to a superuser.

2. At the local host, stop the Performance Management programs and services.

   Display the service information to make sure that no services are running. If any Performance Management programs and services are running on the local host, stop all the active programs and services. You must stop all services on both physical and logical hosts.

   For details about how to display service information and how to stop services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

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

   ```
   /etc/hitachi_setup
   ```

   The Hitachi Program Product Installer starts and the initial window is displayed.

4. In the initial window, enter `D`.

   A list of programs that can be uninstalled is displayed.

5. Select the Performance Management program that you want to uninstall, and then enter `D`.

   The selected program is uninstalled. To select another program, move the cursor to the desired program, and then press the space key to select it.

6. When uninstallation is completed successfully, enter `Q`.

   The initial window of the Hitachi Program Product Installer is displayed again.

Important note

If you specified a private key and a public key to be used for setting up SSH public key authentication in *3.2.5 SSH (for UNIX) connection setting method*, delete these keys as necessary.

3.5 Changing the PFM - RM for Platform system configuration

When a change occurs, such as the monitoring target system's network configuration and host names, you must change the system configuration for PFM - RM for Platform.

When you change the system configuration for PFM - RM for Platform, you must also change the settings for PFM - Manager and PFM - Web Console. For details about how to change the system configuration for Performance Management, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

3.6 Changing the PFM - RM for Platform operation method

It might be necessary to change the operation method for PFM - RM for Platform for a reason such as a change made to the method for handling the collected operation monitoring data. This section describes how to change the operation method for PFM - RM for Platform.

For details about how to change the operation method for the entire Performance Management system, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

3.6.1 Changing performance data storage locations

The performance data collected by PFM - RM for Platform is managed in the Store database of the Remote Monitor Store service of PFM - RM for Platform. This subsection describes how to change performance data storage locations.

You use the `jpcconf db define` command to change the storage directories listed below for performance data managed in the Store database. For details about the `jpcconf db define` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

- Storage directory
- Backup directory
- Export directory
- Partial backup directory
- Import directory

(1) In Windows

The following table lists and describes the option names set by the `jpcconf db define` command and their permitted values.

Table 3–41: Items set by the jpcconf db define command (for Windows)

No.	Option name	Description	Permitted value (Store version 2.0)	Default
1	`bd`	Sets the performance data backup folder[#1]	Path name of 1 to 211 bytes	*installation-folder*[#2]`\agt7\store\`*instance-name*`\backup`
2	`bs`	Sets the maximum generation number when performance data is backed up	From 1 to 9	`5`
3	`id`	Sets the performance data import folder[#1]	Path name of 1 to 222 bytes	*installation-folder*[#2]`\agt7\store\`*instance-name*`\import`
4	`pbd`	Sets the performance data partial backup folder[#1]	Path name of 1 to 214 bytes	installation-folder[#2]`\agt7\store\`*instance-name*`\partial`
5	`dd`	Sets the performance data export folder[#1]	Path name of 1 to 127 bytes	*installation-folder*[#2]`\agt7\store\`*instance-name*`\dump`
6	`sd`	Sets the performance data creation folder[#1]	Path name of 1 to 214 bytes	*installation-folder*[#2]`\agt7\store\`*instance-name*

#1

Specify either the folder name relative to the default Store database storage folder (*installation-folder*`\agt7\store`) or the absolute path.

#2

For the default values for logical host operation, replace *installation-folder* with *environment-folder*`\jp1pc`.

(2) In UNIX

The following table lists and describes the option names set by the `jpcconf db define` command and their permitted values.

Table 3–42: Items set by the jpcconf db define command (for UNIX)

No.	Option name	Description	Permitted value (Store version 2.0)	Default
1	`bd`	Sets the performance data backup directory#1	Path name of 1 to 211 bytes	`/opt`#2`/jp1pc/agt7/store/`*instance-name*`/backup`
2	`bs`	Sets the maximum generation number when performance data is backed up	From 1 to 9	`5`
3	`id`	Sets the performance data import directory#1	Path name of 1 to 222 bytes	`/opt`#2`/jp1pc/agt7/store/`*instance-name*`/import`
4	`pbd`	Sets the performance data partial backup directory#1	Path name of 1 to 214 bytes	`/opt`#2`/jp1pc/agt7/store/`*instance-name*`/partial`
5	`dd`	Sets the performance data export directory#1	Path name of 1 to 127 bytes	`/opt`#2`/jp1pc/agt7/store/`*instance-name*`/dump`
6	`sd`	Sets the performance data creation directory#1	Path name of 1 to 214 bytes	`/opt`#2`/jp1pc/agt7/store/`*instance-name*

#1

Specify either the directory name relative to the default Store database storage directory (`/opt/jp1pc/agt7/store`) or the absolute path.

#2

For the default values for logical host operation, replace `opt` with *environment-directory*.

3.6.2 Updating an instance environment

This subsection describes how to change an instance environment of PFM - RM for Platform while the Performance Management system is running.

(1) In Windows

To update an instance environment, check the instance name, and then update individual instance environment settings. Use the PFM - RM host to set individual instance environment settings.

Use the following table to check the information to be updated beforehand.

Table 3–43: Instance environment settings for PFM - RM for Platform (for Windows)

No.	Item name	Description	Setting	Default
1	`UseCommonAccount`#	Specifies whether to use common account information.	Specify one of the following values:	Previous setting

No.	Item name	Description	Setting	Default
1	UseCommonAccount#	Specifies whether to use common account information.	• Y: Use • N: Do not use	Previous setting
2	Interval	Specifies the collection interval for the collection process.	Specify a value in the range from 60 to 3,600 (seconds).	
3	Std_Category	Specifies whether the collection process is to collect basic information (PI and PI_CPU records).	Specify one of the following values: • Y: Collect • N: Do not collect	
4	Disk_Category	Specifies whether the collection process is to collect disk information (PI_PDSK and PI_LDSK records).	Specify one of the following values: • Y: Collect • N: Do not collect	
5	Network_Category	Specifies whether the collection process is to collect network information (PI_NET record).	Specify one of the following values: • Y: Collect • N: Do not collect	
6	Ps_Category	Specifies whether the collection process is to collect process information (PD_APS, PD_ASVC, PD_APP2, PD_APPC, and PD_APPD records).	Specify one of the following values: • Y: Collect • N: Do not collect	
7	RMHost_User#	Specifies the user account used at the PFM - RM host.	From 1 to 256 bytes of characters are permitted. The tab character is not permitted.	
8	RMHost_Password#	Specifies the password for the account used at the PFM - RM host. The characters entered in this item are not displayed on the screen. If you enter this password, you are prompted to re-enter the same password.	From 1 to 256 bytes of characters are permitted. The tab character is not permitted.	
9	RMHost_Domain#	Specifies the domain name to which the account used at the PFM - RM host belongs. There is no need to specify this item if the account belongs to a work group.	From 0 to 256 bytes of characters are permitted. The tab character is not permitted.	
10	SSH_Client	Specifies an absolute path for the execution module (plink.exe) of the SSH client (PuTTY). Even if the file path contains a space, there is no need to enclose the file path in double quotation marks ("). There is no need to specify this item if all of the monitored hosts in the instance are running Windows.	From 0 to 256 bytes of characters are permitted. The tab character is not permitted.	
11	Perl_Module	Specifies an absolute path for the execution module (perl.exe) of Perl (ActivePerl). Even if the file path contains a space, there is no need to enclose the file path in double quotation marks ("). There is no need to specify this item if all of the monitored hosts in the instance are running Windows.	From 0 to 256 bytes of characters are permitted. The tab character is not permitted.	

No.	Item name	Description	Setting	Default
12	`Log_Size`	Specifies the maximum size of one agent log file.	Specify a value in the range from 1 to 32 (megabytes).	Previous setting

#

These items are not displayed, depending on the environment or settings. For details about the conditions and input values that prevent these items from being displayed, see Table 3-21.

To check the name of an instance, use the `jpcconf inst list` command. To update an instance environment, use the `jpcconf inst setup` command.

To update multiple instance environments, repeat the procedure described below.

To update an instance environment:

1. Check the name of the instance.

   Execute the `jpcconf inst list` command with the service key that indicates PFM - RM for Platform specified.

   ```
   jpcconf inst list -key RMPlatform
   ```

   For example, if the set instance name is `inst1`, the command displays `inst1`.

2. If any services of PFM - RM for Platform are running in the instance environment that you want to update, stop all of them.

   For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

   If a service of the instance environment that is to be updated is running during execution of the `jpcconf inst setup` command, a confirmation message is displayed to enable you to stop the service. When you stop the service, the update processing resumes. If you do not stop the service, the update processing is canceled.

3. Execute the `jpcconf inst setup` command with the service key that indicates PFM - RM for Platform and the instance name specified.

   For example, to update an instance environment whose instance name is `inst1`, execute the following command:

   ```
   jpcconf inst setup -key RMPlatform -inst inst1
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf inst setup` command in the non-interactive mode.

   For details about how to execute this command in the non-interactive mode, see *3.1.4(2) Setting up an instance environment*.

   If you execute the `jpcconf inst setup` command in the non-interactive mode, the procedure in step 4 is not required.

4. Update the instance environment for PFM - RM for Platform.

   Enter the applicable items listed in Table *3-43 Instance environment settings for PFM - RM for Platform (for Windows)* according to the command's instructions. The current settings are displayed. To not change a displayed value, press the **Enter** key. When all entries have been made, the instance environment is updated.

5. Restart the services for the updated instance environment.

   For details about how to start services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(2) In UNIX

To update an instance environment, check the instance name, and then update individual instance environment settings. Use the PFM - RM host to set individual instance environment settings.

Use the following table to check the information to be updated beforehand.

Table 3–44: Instance environment settings for PFM - RM for Platform (for UNIX)

No.	Item name	Description	Setting	Default
1	`Interval`	Specifies the collection interval for the collection process.	Specify a value in the range from 60 to 3,600 (seconds).	Previous setting
2	`Std_Category`	Specifies whether the collection process is to collect basic information (`PI` and `PI_CPU` records).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	
3	`Disk_Category`	Specifies whether the collection process is to collect disk information (`PI_PDSK` and `PI_LDSK` records).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	
4	`Network_Category`	Specifies whether the collection process is to collect network information (`PI_NET` record).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	
5	`Ps_Category`	Specifies whether the collection process is to collect process information (`PD_APS`, `PD_ASVC`, `PD_APP2`, `PD_APPC`, and `PD_APPD` records).	Specify one of the following values: • `Y`: Collect • `N`: Do not collect	
6	`Log_Size`	Specifies the maximum size of one agent log file.	Specify a value in the range from 1 to 32 (megabytes).	

To check the name of an instance, use the `jpcconf inst list` command. To update an instance environment, use the `jpcconf inst setup` command.

To update multiple instance environments, repeat the procedure described below.

To update an instance environment:

1. Check the name of the instance.

   Execute the `jpcconf inst list` command with the service key that indicates PFM - RM for Platform specified.

   ```
   jpcconf inst list -key RMPlatform
   ```

   For example, if the set instance name is `inst1`, the command displays `inst1`.

2. If any services of PFM - RM for Platform are running in the instance environment that you want to update, stop all of them.

   For details about how to stop services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

   If a service of the instance environment that is to be updated is running during execution of the `jpcconf inst setup` command, a confirmation message is displayed to enable you to stop the service. When you stop the service, the update processing resumes. If you do not stop the service, the update processing is canceled.

3. Execute the `jpcconf inst setup` command with the service key that indicates PFM - RM for Platform and the instance name specified.

   For example, to update an instance environment whose instance name is `inst1`, execute the following command:

   ```
   jpcconf inst setup -key RMPlatform -inst inst1
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf inst setup` command in the non-interactive mode.

   For details about how to execute this command in the non-interactive mode, see *3.2.4(3) Setting up an instance environment*.

   If you execute the `jpcconf inst setup` command in the non-interactive mode, the procedure in step 4 is not required.

4. Update the instance environment for PFM - RM for Platform.

   Enter the applicable items listed in Table *3-44 Instance environment settings for PFM - RM for Platform (for UNIX)* according to the command's instructions. The current settings are displayed. To not change a displayed value, press the **Enter** key. When all entries have been made, the instance environment is updated.

5. Restart the services for the updated instance environment.

   For details about how to start services, see the chapter that describes starting and stopping Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

3.6.3 Updating a monitoring target

This subsection describes how to update a monitoring target of PFM - RM for Platform while the Performance Management system is running.

(1) In Windows

To update a set monitoring target, you must first check the name of the monitoring target, and then update the monitoring target. Use the PFM - RM host to set the monitoring target.

Before you perform this operation, check the information to be updated. The following table lists and describes the information that can be updated.

Table 3–45: Monitoring target settings for PFM - RM for Platform (for Windows)

No.	Item	Description	Setting	Default value
1	`Target Host`	Specifies the resolvable host name where the monitoring target is run. This information is used for collection of performance data and health checking. It is also used as the event host name when JP1/IM or NNM is linked.	From 1 to 32 bytes of alphanumeric characters and the hyphen (-) are permitted. A name beginning with a hyphen (-) is not permitted. The host name must be unique within the instance.	Previous setting
2	`UseCommonAccount`#	Specifies whether to use common account information.	Specify one of the following values: • `Y`: Use • `N`: Do not use	

No.	Item	Description	Setting	Default value
3	`TargetType`	Specifies the method to use when connecting to the monitored host. The setting differs depending on whether the monitored host is running Windows or UNIX.	The values listed below can be set. You cannot change these settings. • `wmi`: WMI (when the monitored host is running Windows) • `ssh`: SSH (when the monitored host is running UNIX)	Initial setting
4	`User`#	Specifies the user who connects to the monitored host.	From 1 to 256 bytes of characters are permitted. The following character is not permitted: • Tab	Previous setting
5	`Password`#	Specifies the password needed to connect to the monitored host. The password is not displayed on the screen. If you set a password, you must enter it twice. There is no need to specify this item if the monitored host is running UNIX.	From 0 to 256 bytes of characters are permitted. The following character is not permitted: • Tab	
6	`Domain`#	Specifies the domain name to which the monitored host belongs. There is no need to specify this item if the monitored host belongs to a work group. There is no need to specify this item if the monitored host is running UNIX.	From 0 to 256 bytes of characters are permitted. The following character is not permitted: • Tab	
7	`Private_Key_File`#	Specifies an absolute path for the name of the private key file used in the SSH public key method. Even if the file path contains a space, there is no need to enclose the file path in double quotation marks (`"`). There is no need to specify this item if the monitored host is running Windows.	From 0 to 256 bytes of characters are permitted. The following character is not permitted: • Tab	
8	`Port`#	Specifies the port number of the SSH server on the monitored host. This item is not used if the monitored host is running Windows. In this case, leave the default value.	1 to 65,535	

#
These items are not displayed, depending on the environment or settings. For details about the conditions and input values that prevent these items from being displayed, see Table 3-28.

To check the name of a monitoring target, use the `jpcconf target list` command. To check the settings for a monitoring target, use the `jpcconf target display` command. To update a monitoring target, use the `jpcconf target setup` command.

Reference note

There is no need to stop services of PFM - RM for Platform while you are updating a monitoring target.

To update multiple monitoring targets, repeat the procedure described below.

To update a monitoring target:

1. To check the name of the monitoring target, execute the `jpcconf target list` command with the service key that indicates PFM - RM for Platform and the instance name specified:

```
jpcconf target list -key RMPlatform -inst inst1
Targets:
targethost1
targethost2
Groups:
All
```

2. To check the settings for the monitoring target, execute the `jpcconf target display` command with the service key that indicates PFM - RM for Platform, the instance name, and the monitoring target name specified.

   For example, if you want to check the settings for the monitoring target whose name is `targethost1`, execute the following command:

```
jpcconf target display -key RMPlatform -inst inst1 -target targethost1
```

3. Execute the `jpcconf target setup` command with the service key that indicates PFM - RM for Platform, the instance name, and the monitoring target name specified.

   For example, if you want to update the monitoring target whose name is `targethost1`, execute the following command:

```
jpcconf target setup -key RMPlatform -inst inst1 -target targethost1
```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf target setup` command in the non-interactive mode.

   For details about how to execute this command in the non-interactive mode, see *3.1.4(3) Setting the monitored host*.

   If you execute the `jpcconf target setup` command in the non-interactive mode, the procedure in step 4 is not required.

4. To update the PFM - RM for Platform monitoring target, enter the applicable items listed in Table *3-45 Monitoring target settings for PFM - RM for Platform (for Windows)* according to the command's instructions.

   The current settings are displayed. To not change a displayed value, press the **Enter** key. When all entries have been made, the monitoring target is updated.

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(2) In UNIX

To update a set monitoring target, you must first check the name of the monitoring target, and then update the monitoring target. Use the PFM - RM host to set the monitoring target.

Before you perform this operation, check the information to be updated. The following table lists and describes the information that can be updated.

Table 3–46: Monitoring target settings for PFM - RM for Platform (for UNIX)

No.	Item	Description	Setting	Default value
1	`Target Host`	Specifies the resolvable host name where the monitoring target is run.	From 1 to 32 bytes of alphanumeric characters and the hyphen (-) are permitted. A name beginning with a hyphen (-) is not permitted. The host name must be unique within the instance.	Previous setting
2	`UseCommonAccount`#	Specifies whether to use common account information.	Specify one of the following values: • `Y`: Use • `N`: Do not use	
3	`User`#	Specifies the user who logs on to the monitoring target. PFM - RM for Platform uses this user to log on to the monitored host and perform information collection.	From 1 to 256 bytes of characters are permitted. The following character is not permitted: • Tab	
4	`Private_Key_File`#	Specifies the name of the private key file that is used in the SSH public key method.	From 1 to 256 bytes of characters are permitted. The following character is not permitted: • Tab	
5	`Port`	Specifies the port number of the SSH server on the monitored host.	From 1 to 65,535	

#
These items are not displayed, depending on the environment or settings. For details about the conditions and input values that prevent these items from being displayed, see Table 3-38.

To check the name of a monitoring target, use the `jpcconf target list` command. To check the settings for a monitoring target, use the `jpcconf target display` command. To update a monitoring target, use the `jpcconf target setup` command.

Reference note

There is no need to stop services of PFM - RM for Platform while you are updating a monitoring target.

To update multiple monitoring targets, repeat the procedure described below.

To update a monitoring target:

1. To check the name of the monitoring target, execute the `jpcconf target list` command with the service key that indicates PFM - RM for Platform and the instance name specified:

```
jpcconf target list -key RMPlatform -inst inst1
Targets:
targethost1
targethost2
Groups:
All
```

2. To check the settings for the monitoring target, execute the `jpcconf target display` command with the service key that indicates PFM - RM for Platform, the instance name, and the monitoring target name specified.
   For example, if you want to check the settings for the monitoring target whose name is `targethost1`, execute the following command:

```
jpcconf target display -key RMPlatform -inst inst1 -target targethost1
```

3. Execute the `jpcconf target setup` command with the service key that indicates PFM - RM for Platform, the instance name, and the monitoring target name specified.

   For example, if you want to update the monitoring target whose name is `targethost1`, execute the following command:

   ```
   jpcconf target setup -key RMPlatform -inst inst1 -target targethost1
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf target setup` command in the non-interactive mode.

   For details about how to execute this command in the non-interactive mode, see *3.2.4(4) Setting the monitored host*.

   If you execute the `jpcconf target setup` command in the non-interactive mode, the procedure in step 4 is not required.

4. To update the PFM - RM for Platform monitoring target, enter the applicable items listed in Table *3-46 Monitoring target settings for PFM - RM for Platform (for UNIX)* according to the command's instructions.

   The current settings are displayed. To not change a displayed value, press the **Enter** key. When all entries have been made, the monitoring target is updated.

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

3.7 Backing up and restoring PFM - RM for Platform

This section describes backing up and restoring PFM - RM for Platform.

To provide for recovery of the system in the event of a failure, you should back up the settings for PFM - RM for Platform periodically. You should also back up the settings whenever a change has been made to the system, such as whenever PFM - RM for Platform setup is performed.

For details about backup and restoration of the entire Performance Management system, see the chapter that describes backup and restoration in the *Job Management Partner 1/Performance Management User's Guide*.

3.7.1 Backing up

You can use any method to make a backup, such as by copying files. Always perform the backup operation while the services of PFM - RM for Platform are stopped.

(1) Files to be backed up for PFM - RM for Platform (for Windows)

The following table lists the settings files for PFM - RM for Platform that must be backed up.

Table 3–47: Files to be backed up for PFM - RM for Platform (for Windows)

No.	File name	Description
1	*installation-folder*#1`\agt7\agent\*.ini` file	Settings files for the Remote Monitor Collector service
2	*installation-folder*#1`\agt7\agent\`*instance-name*#2`\*.ini` file	
3	*installation-folder*#1`\agt7\agent\`*instance-name*#2`\groups\*.ini` file	
4	*installation-folder*#1`\agt7\agent\`*instance-name*#2`\targets\*.ini` file	
5	*installation-folder*#1`\agt7\agent\`*instance-name*#2`\targets\*_jpcapp` file#3	Application definition file
6	*installation-folder*#1`\agt7\store\*.ini` file	Settings files for the Remote Monitor Store service
7	*installation-folder*#1`\agt7\store\`*instance-name*#2`\*.ini` file	

#1

If you use a logical host for operation, replace *PFM-RM-for-Platform-installation-folder* with *environment-folder*`\jp1pc`. An environment folder is a folder on the shared disk that is specified when the local host is created.

#2

These are folders used for operation in an instance environment. In the case of an instance configuration, as many folders as there are instances are created.

#3

This file exists only if application monitoring is specified.

Important note

When you back up PFM - RM for Platform, you must manage the environment's product version numbers. For details about the product version numbers, see the *Release Notes*.

Before you back up PFM - RM for Platform, you must record the instances and the configuration of the monitoring targets (including the logical host environment).

(2) Files to be backed up for PFM - RM for Platform (for UNIX)

The following table lists the settings files for PFM - RM for Platform that must be backed up.

Table 3–48: Files to be backed up for PFM - RM for Platform (for UNIX)

No.	File name	Description
1	`/opt`[#1]`/jp1pc/agt7/agent/*.ini` file	Settings files for the Remote Monitor Collector service
2	`/opt`[#1]`/jp1pc/agt7/agent/`*instance-name*[#2]`/*.ini` file	
3	`/opt`[#1]`/jp1pc/agt7/agent/`*instance-name*[#2]`/groups/*.ini` file	
4	`/opt`[#1]`/jp1pc/agt7/agent/`*instance-name*[#2]`/targets/*.ini` file	
5	`/opt`[#1]`/jp1pc/agt7/agent/`*instance-name*[#2]`/targets/*_jpcapp` file[#3]	Application definition file
6	`/opt`[#1]`/jp1pc/agt7/store/*.ini` file[#2]	Settings files for the Remote Monitor Store service
7	`/opt`[#1]`/jp1pc/agt7/store/`*instance-name*[#2]`/*.ini` file	

#1

If you use a *logical* host for operation, replace `opt` with *environment-directory*. An environment directory is a directory on the shared disk that is specified when the logical host is created.

#2

These are directories used for operation in an instance environment. In the case of an instance configuration, as many directories as there are instances are created.

#3

This file exists only if application monitoring is specified.

Important note

When you back up PFM - RM for Platform, you must manage the environment's product version numbers. For details about the product version numbers, see the *Release Notes*.

3.7.2 Restoring

To restore PFM - RM for Platform settings, make sure that the prerequisites listed below are satisfied, and then copy the backup files to their original locations. The settings files on the host will be overwritten by the backup settings files.

Prerequisites

- PFM - RM for Platform has already been installed.
- All services of PFM - RM for Platform have stopped.
- Instances and monitoring targets (including the logical host environment) had been set up before they were backed up.

Important note

To restore settings for PFM - RM for Platform, the product version numbers must match between the environment from which the backup was made and the environment into which the backup is restored. For details about the product version numbers, see the *Release Notes*.

3.8 Settings for using a Web browser to reference manuals

You can use a Web browser to reference the Performance Management manuals. To do this, you must copy the manuals from the manuals distribution media provided with the program product to the host where PFM - Web Console is installed.

If you are running PFM - Web Console in a cluster environment, copy the manuals onto the physical hosts of both the executing and the standby systems.

3.8.1 Setup for referencing manuals

This subsection describes the setup procedure that enables you to reference manuals from Help of PFM - Web Console or from your machine's hard disk.

(1) Referencing manuals from Help of PFM - Web Console

To reference manuals from Help of PFM - Web Console:

1. Register PFM - RM in PFM - Web Console according to the PFM - Web Console setup procedure.
   Perform additional setup of PFM - RM.

2. On the host where PFM - Web Console is installed, create a directory for the copies of manuals.
   The following shows the directory to be created:

   In Windows

   PFM-Web-Console-installation-folder`\doc\`*language-code*`\`*Help-ID-of-PFM - RM-for-Platform*

   In UNIX

   `/opt/jp1pcwebcon/doc/`*language-code*`/`*Help-ID-of-PFM - RM-for-Platform*

   For details about the help ID of PFM - RM for Platform, see *B. List of Identifiers*.

3. From the manuals distribution media, copy the files and directories into the directory that was created in step 2.
   The following shows the files and directories to be copied:

   For HTML manuals

   In Windows

   All HTML files, CSS files, and `GRAPHICS` folders under *applicable-drive*`\MAN\3021\`*manual-number* (such as `03004A0D`)

   In UNIX

   All HTML files, CSS files, and `GRAPHICS` directories under `/`*distribution-media -mount-point*`/MAN/3021/`*manual-number* (such as `03004A0D`)

   For PDF manuals

   In Windows

   PDF files under *applicable-drive*`\MAN\3021\`*manual-number* (such as `03004A0D`)

   In UNIX

   PDF files under `/`*distribution-media -mount-point*`/MAN/3021/`*manual-number* (such as `03004A0D`)

   Directly under the created directory, place `INDEX.HTM` for the HTML manuals and the PDF files themselves for the PDF manuals.

4. Restart PFM - Web Console.

(2) Referencing manuals from your machine's hard disk

Use one of the following methods to reference manuals from your machine's hard disk:

- Use `setup.exe` on the distribution media to install the manuals (in Windows only).
- Copy the HTML, CSS, PDF, and GIF files directly into a directory of your choice.

When you reference HTML manuals, use the following directory structure:

`html` (stores HTML and CSS files)

`+-- GRAPHICS` (stores GIF files)

3.8.2 How to view manuals

To view a manual:

1. In the Main window of PFM - Web Console, click the **Help** menu in the menu bar frame.
   The Help window appears.
2. Click a manual name or the **PDF** link that follows a manual name.
   Clicking a manual name displays the HTML version of that manual.
   Clicking a **PDF** link displays that manual in PDF format.

Notes about displaying manuals in a Web browser

In Windows, if you display an online manual from the **Start** menu, the HTML manual might be displayed in the Web browser that is already open.

4 Collecting Process Operation Status Information

This chapter explains how to use PFM - RM for Platform to collect process operation status information and monitor it on PFM - Web Console. It also provides examples of actions to take when alarms are issued.

4.1 Setup for collecting process operation status information

This section explains the setup necessary for using PFM - RM for Platform to collect process operation status information.

You set up the collection of process operation status information by using the Agents tree window of PFM - Web Console or by using commands.

If you want to collect process operation status information by using the same procedure as that used by earlier versions (earlier than 10-00) of PFM - RM for Platform, you can set it up in the Services tree window of PFM - Web Console.

4.1.1 Setup using the Agents tree

You can set up the collection of process operation status information in the Agents tree window of PFM - Web Console.

To simplify the setup operation, you can also use an application definition template.

Setup using the Agents tree is available in PFM - Web Console version 10-00 or a later version.

4.1.2 Setting up monitoring targets in the Agents tree

To set up a monitoring targets in the Agents tree:

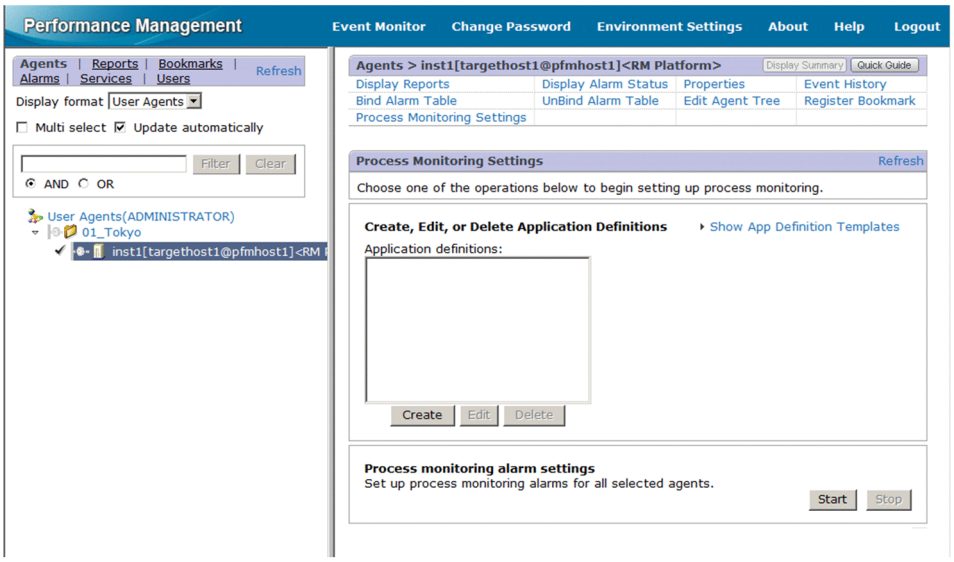
1. Create an application.
2. Bind an alarm table to the monitoring agent.

To collect operation status information on a per-process or per-service basis, specify only a single process or service in the application when creating it. To collect operation status information on a per-application basis, specify multiple processes or services in the application when creating it.

The following subsections provide a detailed description of how to set up a monitoring target.

(1) Creating an application

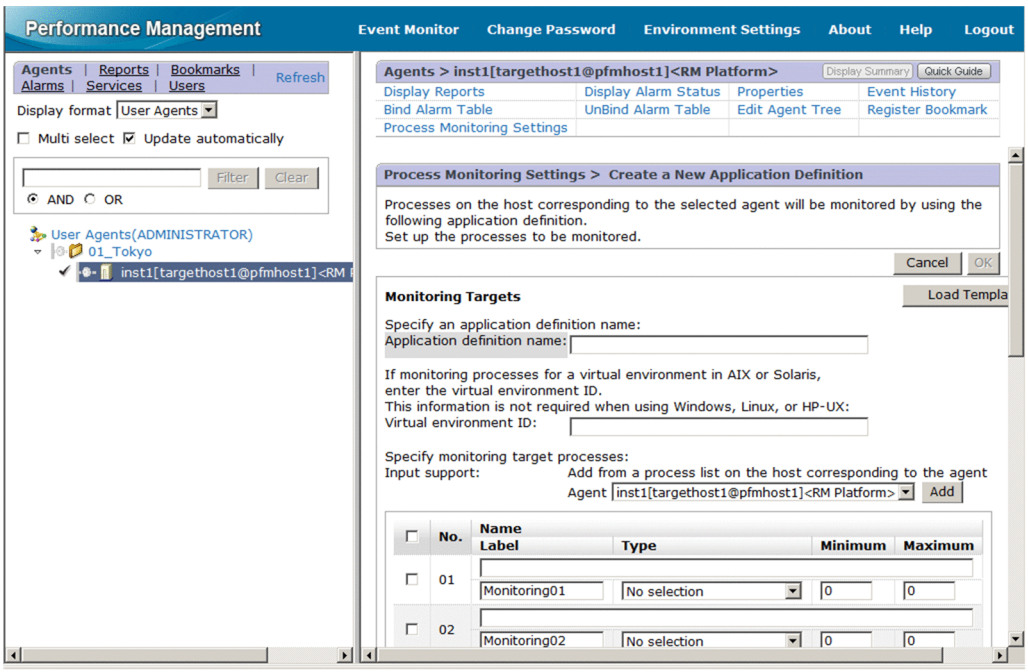
1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.
3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select the **Process Monitoring Settings** method.
   The Process Monitoring Settings window appears.



5. To create a new application, click the **Create** button. To modify an existing application, from **Application Definitions**, select the application definition you want to modify, and then click the **Edit** button.

   You cannot select a group of application definitions.

   The Process Monitoring Settings > Create a New Application Definition window or the Process Monitoring Settings > Edit an Application Definition window appears.



6. To create a new application, specify an application definition name in **Application definition name**.

   Application definition names and the character strings that can be specified must obey the following rules:

   - The user specifies a desired application definition name. The specified application definition name is stored in the `Application Name` fields of the `PD_APP2`, `PD_APPC`, and `PD_APPD` records, and is used as the identifier for identifying a specific application. Therefore, specify a unique name for the application definition name.
   - You can specify from 1 to 63 bytes of single-byte alphanumeric characters and symbols, excluding the following:

     Tab (`\t`) `\ : ; , * ? " ' <> |`

- You can specify a maximum of 64 applications.

7. If you are operating in a virtual system, specify a virtual environment identifier in **Virtual environment ID**.

   If you are operating in a virtual system, enter an identifier for identifying a specific virtual environment. By specifying an identifier, you can limit the monitoring targets to processes in a specific environment.

   You can specify from 1 to 63 bytes of single-byte alphanumeric characters and symbols, excluding the tab character (`\t`). The identifier you specify is compared to the value of the `Virtual Env ID` field of the `PD_APS` record.

   Note:

   Make sure that the character string you enter in **Virtual environment ID** matches what is entered in the `Virtual Env ID` field of the `PD_APS` record.

   Any character in the information to be acquired that is not in the ASCII character set range of `0x20` to `0x7E` will be converted to a hash mark (`#`: `0x23`) before it is stored in the `Virtual Env ID` field of the `PD_APS` record. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter `A` is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	`8260`	`2360`	`#`
EUC	`A3C1`	`2323`	`##`
UTF-8	`EFBCA1`	`232323`	`###`

8. Specify detailed information for the application.

   The following table shows the detailed information that you can specify in the Process Monitoring Settings > Create a New Application Definition window or the Process Monitoring Settings > Edit an Application Definition window.

Table 4–1: Detailed application information that can be specified

Setting	Description	Field name in the corresponding record
Name[#1]	Enter a condition for identifying a specific monitoring target. You can specify a maximum of 4,096 bytes of single-byte alphanumeric characters and symbols, excluding the tab character (`\t`).	`Monitoring Condition` field of the `PD_APPD` record
Label	Specify a label for identifying a specific monitoring condition. You can specify a maximum of 31 bytes of single-byte alphanumeric characters and symbols, excluding the tab character (`\t`). The default is `Monitoring`*XX*[#2]. If you do not enter any value, the default `Monitoring`*XX*[#2] is set. Specify a unique name for the monitoring label.	`Monitoring Label` field of the `PD_APPC` and `PD_APPD` records
Type	Select **Program**, **Command Line**, **Service**, or **No selection**. • **Program** The specified value is evaluated using the value of the `Program Name` field of the `PD_APS` record. • **Command Line** The specified value is evaluated using the value of the `Command Line` field of the `PD_APS` record. • **Service** The specified value is evaluated using the value of the `Service Name` field of the `PD_ASVC` record. • **No selection**	`Monitoring Field` field of the `PD_APPD` record

Setting	Description	Field name in the corresponding record
Type	No evaluation.	`Monitoring Field` field of the `PD_APPD` record
Minimum#3	Enter the lower threshold value for the number of applications to be monitored. You can specify a value from `0` to `65535`. The default is `0`.	`Monitoring Min` field of the `PD_APPD` record
Maximum	Enter the upper threshold value for the number of applications to be monitored. You can specify a value from `0` to `65535`. However, you must specify a value that is greater than or equal to the value specified for **Minimum**. The default is `0`.	`Monitoring Max` field of the `PD_APPD` record

#1

- You can use the wildcard characters `*` and `?` when specifying a name.

  An asterisk (`*`) represents zero or more instances of any character, and a question mark (`?`) represents any single character.

  If the monitoring target process' command line itself contains characters such as an asterisk (`*`) or a question mark (`?`), you cannot specify a monitoring condition based on complete matching.

  For example, suppose that the three processes listed below exist. If you enter `/bin/sample "*"` as the monitoring condition, the `*` in the monitoring condition is treated as a wildcard, and as a result all three processes are considered to match the monitoring condition.

  · `/bin/sample "*"`

  · `/bin/sample "abc"`

  · `/bin/sample "def"`

- Note the following if you specify a **Name** of 128 bytes or more as a monitoring condition when setting up collection of process operation status information: The `Monitoring Condition` field of the `PD_APPD` record will display only the first 127 bytes of the specified monitoring condition. However, monitoring will occur using the complete specified monitoring condition.

- When the OS of the monitored host is Windows, the monitoring condition specified for **Name** is not case-sensitive when used to identify monitoring targets in the default setting. When the OS of the monitored host is UNIX, on the other hand, the monitoring condition specified in **Name** is case-sensitive when used to identify monitoring targets in the default setting. For details about how to specify whether the monitoring condition will be case-sensitive when identifying monitoring targets, see *4.1.12 Specifying whether process or service names to be used as monitoring targets will be case-sensitive*.

- When the OS of the monitored host is Windows, if you select **Program** for **Type**, specify the Windows program extension (such as `.exe`) for **Name**.

- Make sure that the character string you enter in **Name** matches what is entered in the Program Name field of the `PD_APS` record, the Command Line field of the `PD_APS` record, and the Service Name field of the `PD_ASVC` record.

  Any character in the information to be acquired that is not in the ASCII character set range of `0x20` to `0x7E` will be converted to a hash mark (`#`: `0x23`) before it is stored in the Program Name field of the `PD_APS` record, the Command Line field of the `PD_APS` record, and the Service Name field of the `PD_ASVC` record. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter `A` is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

#2

A value from 01 to 15 is set for *XX*. A numeric value corresponding to the Monitoring Number field of the PD_APPC and PD_APPD records is set.

#3

To monitor a process that generates child processes, specify an appropriate numeric value by referring to *9.2.5(4) Alarms related to process monitoring are not reported as intended*.

Reference note

From the **Input support** > **Agent** pull-down menu, select a remote agent for a monitored host and click the **Add** button. The Process Monitoring Settings > Create a New Application Definition > Add from *monitoring-targets* window# or the Process Monitoring Settings > Edit an Application Definition > Add from *monitoring-target* window# appears. You can then select a process and set up its properties.

#

For *monitoring-targets*, **Running Process**, **Running Command Lines**, or **Services** is displayed depending on what is specified for **Type** in the Process Monitoring Settings > Create a New Application Definition window or the Process Monitoring Settings > Edit an Application Definition window.

If you selected **Program** for **Type** in these windows, **Running Processes** is displayed. If you selected **Command Line**, **Running Command Lines** is displayed. If you selected **Service**, **Services** is displayed. By default, **Running Processes** is displayed.

9. Click the **OK** button.

   The settings you specified take effect.

   Shown below is the procedure for setting up properties from the Process Monitoring Settings > Create a New Application Definition > Add from *monitoring-target* window# or the Process Monitoring Settings > Edit an Application Definition > Add from *monitoring-target* window# in steps 8 and beyond under *(1) Creating an application*.

   #

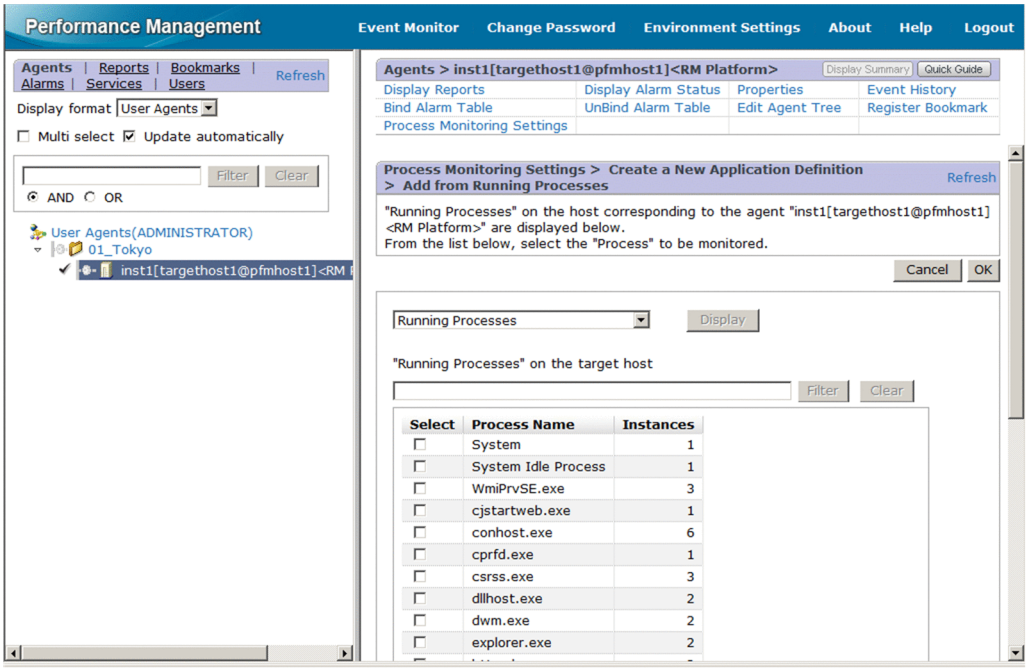
   For the monitoring target type, **Running Processes**, **Running Command Lines**, or **Services** is displayed depending on what is specified for **Type** in the Process Monitoring Settings > Create a New Application Definition window or the Process Monitoring Settings > Edit an Application Definition window.

   If you selected **Program** for **Type** in these windows, **Running Processes** is displayed. If you selected **Command Line**, **Running Command Lines** is displayed. If you selected **Service**, **Services** is displayed. By default, **Running Processes** is displayed.

10. Execute steps 1 through 7 in *(1) Creating an application*.

11. From **Input support** > **Agent** pull-down menu, select a remote agent for the monitored host and click the **Add** button.

The Process Monitoring Settings > Create a New Application Definition > Add from *monitoring-target* window or the Process Monitoring Settings > Edit an Application Definition > Add from *monitoring-target* window appears.



12. From the pull-down menu on the left side of the **Display** button, select a monitoring target type (**Running Processes**, **Running Command Lines**, or **Services**) and click the **Display** button.

    A process list is displayed at the bottom of the Process Monitoring Settings > Create a New Application Definition > Add from *monitoring-target* window or the Process Monitoring Settings > Edit an Application Definition > Add from *monitoring-target* window.

    In the process list, by specifying a keyword in **Filter** and clicking the **Search** button, you can display only those processes that include the keyword in their process names. Clicking the **Clear** button will take you back to the original process list.

13. From the process list, select the process you want to monitor and click the **OK** button.

    The Process Monitoring Settings > Create a New Application Definition > Add from *monitoring-target* window or the Process Monitoring Settings > Edit an Application Definition > Add from *monitoring-target* window closes, and the display will return to the Process Monitoring Settings > Create a New Application Definition window or the Process Monitoring Settings > Edit an Application Definition window.

14. Modify the necessary items in the displayed window.

    For details about the settings, see Table *4-1 Detailed application information that can be specified*.

15. Click the **OK** button.

    The new settings take effect.

(2) Binding an alarm table to the monitoring agent

Bind an alarm table for monitoring the operation status information to the monitoring agent. The alarm for monitoring the operation status information is called the Application Status alarm. Edit it as needed. For details about this alarm, see *Application Status* in *6. Monitoring Template*. If you monitor a process that generates child processes, specify an alarm-reporting method by referring to *9.2.5(4) Alarms related to process monitoring are not reported as intended*.

You can use one of the following two methods to bind an alarm table:

- Binding the alarm table PFM RM Platform Template Alarms [APP] 09.10
- Binding a user-created alarm table

To bind the alarm of PFM RM Platform Template Alarms [APP] 09.10:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.
3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select the **Process Monitoring Settings** method.
   The Process Monitoring Settings window appears.
5. Click the **Start** button for **Process monitoring alarm settings**.
   The alarm table is bound to the monitoring agent.

To bind a user-created alarm table:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.
3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select **Bind Alarm Table**.
   The Bind Alarm Table [Select Alarm Table] window appears.
5. Select an alarm table displayed under the **RM Platform** folder and click the **OK** button.
   The alarm table is bound to the monitoring agent.

If you want to monitor the status of a specific process only, you can create an alarm based on one of the following conditional expressions for monitoring.

Table 4–2: Conditional expression for monitoring a specific process only

Item	Conditional expression
Record	`Application Process Count (PD_APPC)`

Field	`Application Name`
	`Monitoring Label`
	`Monitoring Status`

Abnormal and warning conditions[#1]	`Application Name =` *Name*[#2] `AND Monitoring Label =` *Label*[#2] `AND Monitoring Status = ABNORMAL`

#1

For the abnormal and warning conditions, specify the same condition.

#2

Specify the application name to be monitored and a monitoring label.

4.1.3 Deleting monitoring target settings in Agents tree

To delete a monitoring target in the Agents tree:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.
3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select the **Process Monitoring Settings** method.
   The Process Monitoring Settings window appears.
5. From **Application Definitions**, select the application definition you want to delete and click the **Delete** button.
   The Process Monitoring Settings > Delete an Application Definition window appears.
6. Click the **OK** button.
   The setting is deleted.

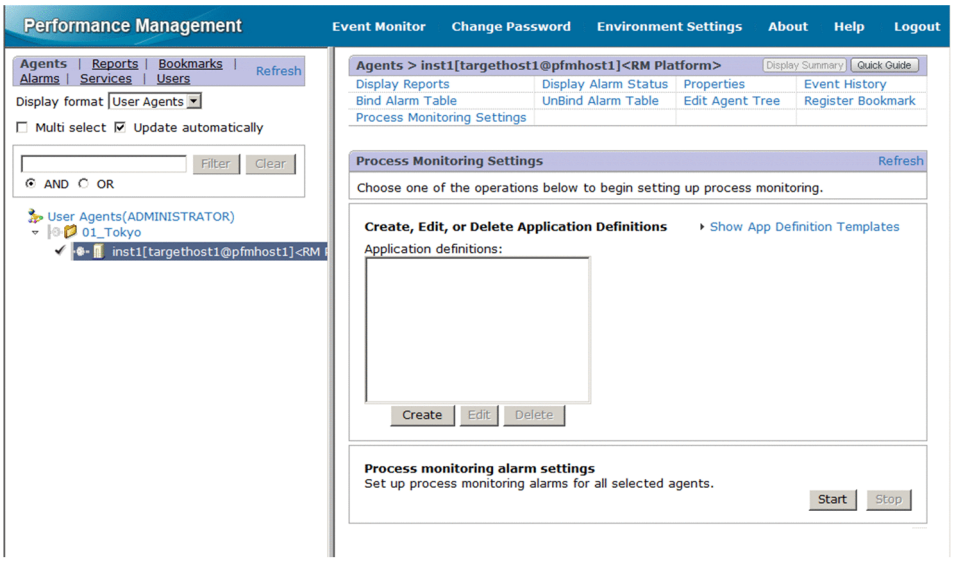
4.1.4 Using an application definition template in the Agents tree

You can save the setting for collecting process operation status information (application definition) that was specified in the Agents tree window of PFM - Web Console as a template and use it in multiple machines.

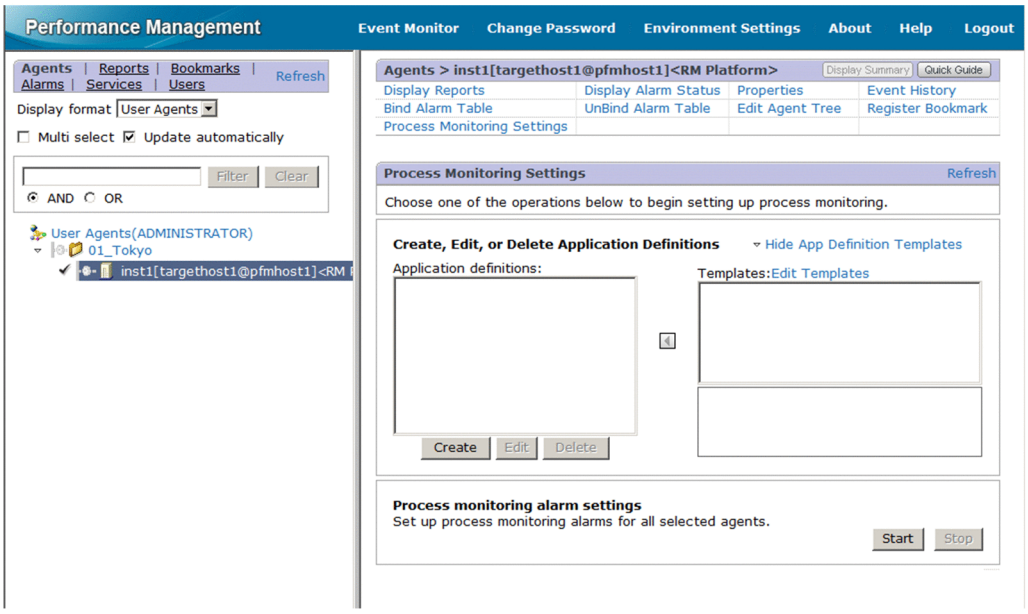
This subsection explains how to create, delete, and load an application definition template.

(1) Creating an application definition template

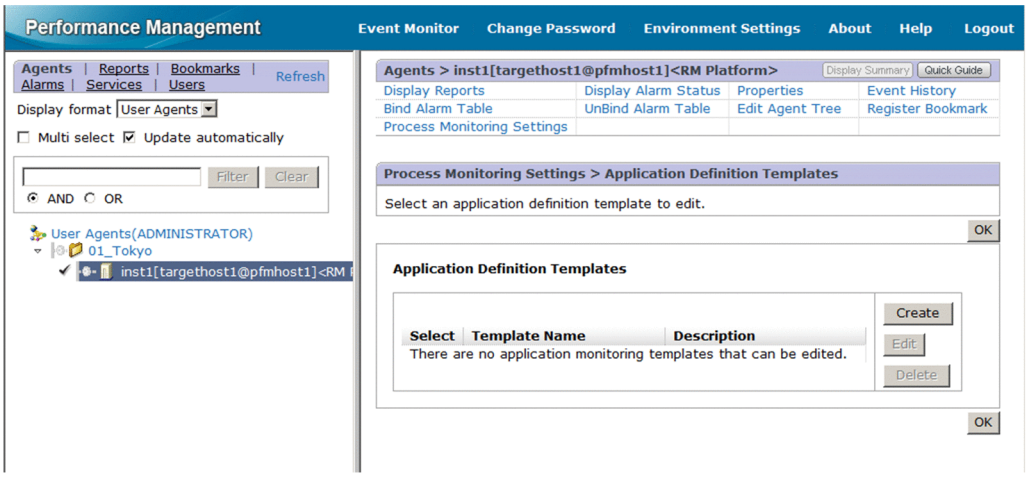
1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.
3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select the **Process Monitoring Settings** method.
   The Process Monitoring Settings window appears.



5. Select the **Show App Definition Templates** menu.
   The **Edit Templates** menu appears.

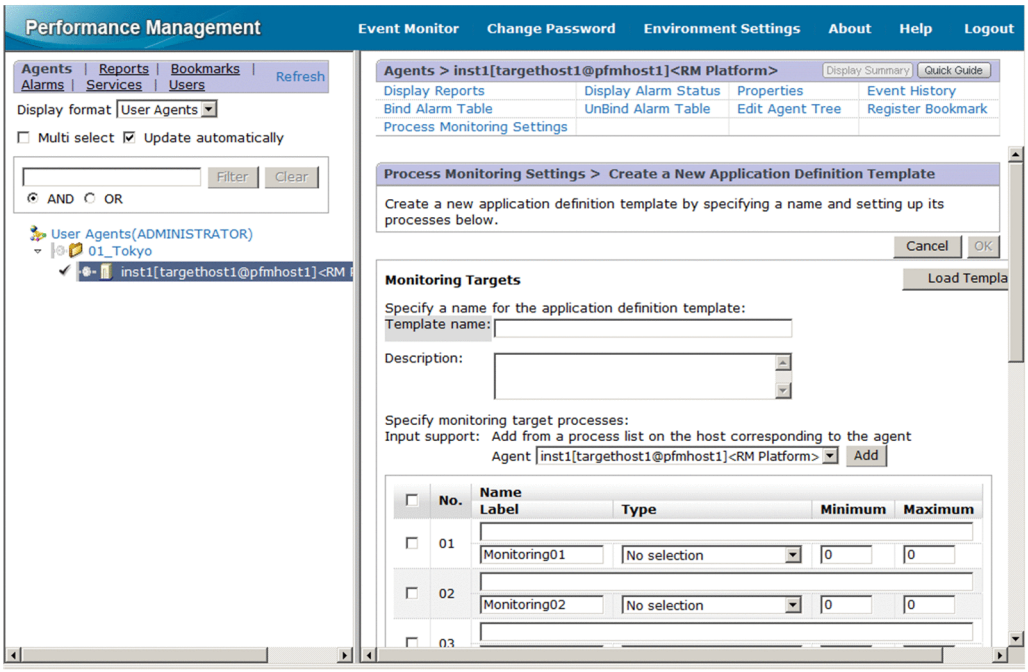


6. Select the **Edit Templates** menu.
   The Process Monitoring Settings > Application Definition Templates window appears.



7. To create a new template, click the **Create** button. To modify settings, select the template you want to modify from **Application Definition Templates** and click the **Edit** button.

   The Process Monitoring Settings > Create a New Application Definition Template window or the Process Monitoring Settings > Edit an Application Definition Template window appears.



8. Enter a template name in **Template name**.

9. Enter a template description in **Description**.

10. Specify detailed information for the application.

    For details about the settings, see Table *4-1 Detailed application information that can be specified* in *4.1.2(1) Creating an application*.

11. Click the **OK** button.

    An application definition template is created.

(2) Deleting an application definition template

1. From the browser of the monitoring console, log in to PFM - Web Console.

The Main window appears.

2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.

3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.

4. In the method frame, select the **Process Monitoring Settings** method.
   The Process Monitoring Settings window appears.

5. Select the **Show App Definition Templates** menu.
   The **Edit Templates** menu appears.

6. Select the **Edit Templates** menu.
   The Process Monitoring Settings > Application Definition Templates window appears.

7. From **Application Definition Templates**, select the template you want to delete and click the **Delete** button.
   The Process Monitoring Settings > Delete an Application Definition Template window appears.

8. Click the **OK** button.
   The application definition template is deleted.

(3) Loading an application definition template

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.

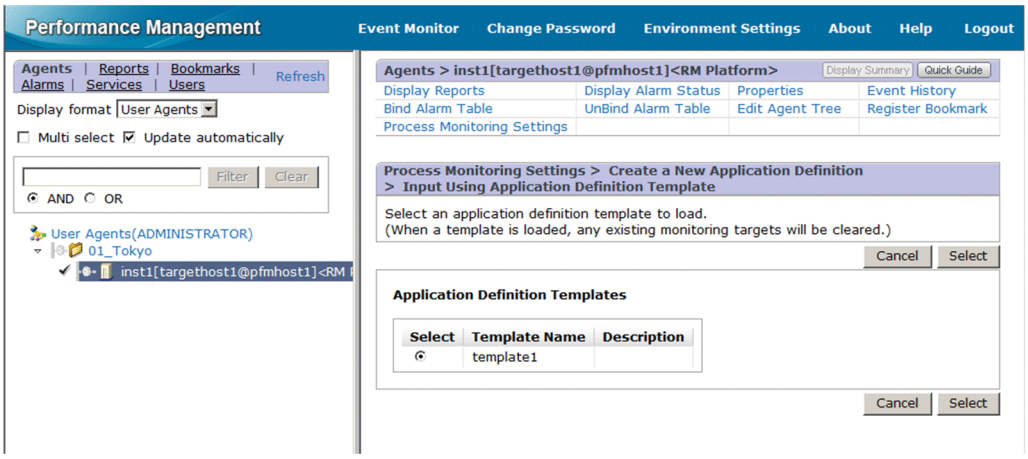
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.

3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.

4. In the method frame, select the **Process Monitoring Settings** method.
   The Process Monitoring Settings window appears.

5. Click the **Create** button.
   The Process Monitoring Settings > Create a New Application Definition window appears.

6. Click the **Load Template** button.
   The Process Monitoring Settings > Create a New Application Definition > Input Using Application Definition Template window appears.



7. Select the template you want to load from **Application Definition Templates** and click the **Select** button.
   The application definition template is loaded.

4.1.5 Setting up collection in Services

If you want to specify the collection of process operation status information using the same procedure that was used in an earlier versions of PFM - RM for Platform (earlier than 10-00), you can do so in the Services window of PFM - Web Console.

4.1.6 Setting up a monitoring target in Services

To set up a monitoring target in Services:

1. Create an application.
2. Specify application properties (the name of the application to be monitored and a threshold value).
3. Bind an alarm table to the monitoring agent.#

#
To bind an alarm table, use the Agents tree window of PFM - Web Console.

To collect operation status information on a per-process or per-service basis, specify only a single process or service when creating the application. To collect operation status information on a per-application basis, specify multiple processes or services when creating the application.

The following subsections provide a detailed description of how to set up a monitoring target.

(1) Creating an application

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, select the **Services** tab.
   The Services window appears.
3. From the navigation frame, expand the hierarchy under the **Machines** folder.

A folder with the name of the host on which Performance Management service is installed appears. When you expand the folder with the host name, the services installed on this host appear.

The name of each service is displayed as a service ID. For details about service IDs, see *B. List of Identifiers* and the section that describes service-naming rules in the appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The service ID format differs depending on whether the product name display function is enabled. For details about this function, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4. Expand the hierarchy under the monitoring agent host's folder and select a remote agent (*device-ID<product-name>*).

   A check mark is displayed for the selected remote agent.

5. In the method frame, select the **Properties** method.

   The Service Properties window appears.

6. Under the **Remote Monitor Configuration** tree, select the **ADDITION OR DELETION A SETTING** tree.

7. On the bottom of the information frame, specify an application name in **ADD AN APPLICATION MONITORING SETTING**.

   The following rules apply to application names and the character string that can be specified:

   - The user specifies a desired application name. The specified application name is stored in the `Application Name` fields of the `PD_APP2`, `PD_APPC`, and `PD_APPD` records, and is used as the identifier for identifying a specific application. Therefore, specify a unique name for the application name.
   - You can specify from 1 to 63 bytes of single-byte alphanumeric characters and symbols, excluding the following:

     Tab (`\t`) `\ : ; , * ? " ' <> |`
   - You can specify a maximum of 64 applications.

8. Click the **OK** button.

   In the Service Properties window, under the **Remote Monitor Configuration - Application monitoring setting** tree, an application name tree is generated.

(2) Specifying application properties

1. After you have performed the procedure in *(1) Creating an application*, open the Service Properties window again and select an application name generated under the **Remote Monitor Configuration - Application monitoring setting** tree.

   A window for entering property information appears at the bottom of the information frame.

2. Specify properties.

   Specify a virtual environment identifier, a monitoring label, a monitoring field, a monitoring condition, and the minimum and maximum threshold values for the number of monitoring targets. You can specify multiple pieces of process information. The following table lists and describes the properties.

   Table 4–3: Application property settings

Item	Property name	Description	Field name in the corresponding record
Virtual environment identifier	`Virtual Environment ID`[#1]	If you are operating on a virtual system, enter an ID for identifying a specific virtual environment. By specifying this item, you can restrict the operation to processes in a specific environment.	`Virtual Env ID` field of the `PD_APP2` record

Item	Property name	Description	Field name in the corresponding record
Virtual environment identifier	`Virtual Environment ID`#1	You can specify from 1 to 63 bytes of single-byte alphanumeric characters and symbols, excluding the tab character (`\t`). The identifier you specify is compared to the value of the `Virtual Env ID` field of the `PD_APS` record.	`Virtual Env ID` field of the `PD_APP2` record
Monitoring label	`Monitoring`*XX* `Label`	Specify a label for identifying a specific monitoring condition. You can specify a maximum of 31 bytes of single-byte alphanumeric characters and symbols, excluding the tab character (`\t`). The default is `Monitoring`*XX*#2. If you do not enter any value, the default `Monitoring`*XX*#2 is set. Specify a unique name for the monitoring label.	`Monitoring Label` field of the `PD_APPC` and `PD_APPD` records
Monitoring field	`Monitoring`*XX* `Field`	Select **Program Name**, **Command Line**, **Service Name**, or **None**. • **Program Name** The specified value is compared to the value of the Program Name field of the `PD_APS` record. • **Command Line** The specified value is compare to the value of the Command Line field of the `PD_APS` record. • **Service Name** The specified value is compared to the value of the Service Name field of the `PD_ASVC` record. • **None** No evaluation. The default is **None**.	`Monitoring Field` field of the `PD_APPD` record
Monitoring condition#3	`Monitoring`*XX* `Condition`	Enter a condition for identifying a specific monitoring target. You can specify a maximum of 4,096 bytes of single-byte alphanumeric characters and symbols, excluding the tab character (`\t`). The default is one space.	`Monitoring Condition` field of the `PD_APPD` record
Minimum and maximum threshold values for the number of monitoring targets#4	Monitoring*XX* Range	Enter the lower and upper threshold values for the number of monitoring targets by connecting the two values with a hyphen (`-`), such as `1-2`. You can specify from 0 to 65535. The default is `0-0`.	• Minimum value `Monitoring Min` field of the `PD_APPD` record • Maximum value `Monitoring Max` field of the `PD_APPD` record

#1

For the Virtual Environment ID property, you must check the `Virtual Env ID` field of the `PD_APS` record and enter the same character string as that specified in this field.

#2

A value from 01 to 15 is set for *XX*. A numeric value corresponding to the Monitoring Number field of the PD_APPC and PD_APPD records is set.

#3

- You can use the wildcard characters * and ? when specifying a condition.

  An asterisk (*) represents zero or more instances of any character, and a question mark (?) represents any single character.

  If the monitoring target process' command line itself contains characters such as an asterisk (*) or a question mark (?), you cannot specify a monitoring condition based on complete matching.

  For example, suppose that the three processes listed below exist. If you enter /bin/sample "*" as the monitoring condition, the * in the monitoring condition is treated as a wildcard, and as a result all three processes are considered to match the monitoring condition.

  · /bin/sample "*"

  · /bin/sample "abc"

  · /bin/sample "def"

- Note the following if you specify 128 bytes or more characters for the monitoring condition (Monitoring*XX* Condition) when setting up collection of process operation status information: The Monitoring Condition field of the PD_APPD record will display only the first 127 bytes of the specified monitoring condition. However, monitoring will occur using the complete specified monitoring condition.
- When the OS of the monitored host is Windows, the monitoring condition is not case-sensitive when identifying monitoring targets in the default setting. In contrast, when the OS of the monitored host is UNIX, the monitoring condition is case-sensitive when identifying monitoring targets in the default setting. For details about how to specify whether the monitoring condition will be case-sensitive when identifying monitoring targets, see *4.1.12 Specifying whether process or service names to be used as monitoring targets will be case-sensitive*.
- When the OS of the monitored host is Windows, if you specify **Program Name** for the Monitoring*XX* Field property, specify the Windows program extension (such as .exe) for the Monitoring*XX* Condition property.
- Make sure that the character string you enter in the Monitoring*XX* Condition property matches what is entered in the Program Name field of the PD_APS record, the Command Line field of the PD_APS record, and the Service Name field of the PD_ASVC record.

  Any character in the information to be acquired that is not in the ASCII character set range of 0x20 to 0x7E will be converted to a hash mark (#: 0x23) before it is stored in the Program Name field of the PD_APS record, the Command Line field of the PD_APS record, the Service Name field of the PD_ASVC record, and the Virtual Env ID field of the PD_APS record. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter Ａ is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

#4

To monitor a process that generates child processes, specify a maximum value by referring to *9.2.5(4) Alarms related to process monitoring are not reported as intended*.

3. Click the **OK** button.
   The settings you specified take effect.

(3) Binding an alarm table to the monitoring agent

Bind an alarm table for monitoring the operation status information to the monitoring agent.

The alarm for monitoring the operation status information is called the Application Status alarm. Edit it as needed.

For details about this alarm, see *Application Status* in *6. Monitoring Template*.

If you monitor a process that generates child processes, specify an alarm-reporting method by referring to *9.2.5(4) Alarms related to process monitoring are not reported as intended*.

To bind an alarm table:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, click **Agents**.
   The Agents tree window appears.
3. In the Agents tree of the navigation frame, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select **Bind Alarm Table**.
   The Bind Alarm Table [Select Alarm Table] window appears.
5. Select an alarm table displayed under the **RM Platform** folder and click the **OK** button.

If you want to monitor the status of one specific process only, you can create an alarm based on one of the following conditional expressions for monitoring.

Table 4–4: Conditional expression for monitoring a specific process only

Item	Conditional expression
Record	`Application Process Count (PD_APPC)`

Field	`Application Name`
	`Monitoring Label`
	`Monitoring Status`

Abnormal and warning conditions[#1]	`Application Name` = *Name*[#2] `AND Monitoring Label` = *Label*[#2] `AND Monitoring Status = ABNORMAL`

#1
For the abnormal and warning conditions, specify the same condition.

#2
Specify the application name to be monitored and a monitoring label.

4.1.7 Checking or modifying the settings for monitoring targets in Services

To check or modify the settings for monitoring targets in Services:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, select the **Services** tab.
   The Services window appears.
3. From the navigation frame, expand the hierarchy under the **Machines** folder.
   A folder with the name of the host on which Performance Management service is installed appears. When you expand the folder with the host name, the services installed on this host appear.
   The name of each service is displayed as a service ID. For details about service IDs, see *B. List of Identifiers* and the section that describes service-naming rules in the appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
   The service ID format differs depending on whether the product name display function is enabled. For details about this function, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
4. Expand the hierarchy under the monitoring agent host's folder and select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
5. In the method frame, select the **Properties** method.
   The Service Properties window appears.
6. Expand the **Remote Monitor Configuration - Application monitoring setting** tree and select the tree with the application name you want to check.
7. Check the setting content.
8. To update the setting content, follow step 2 in *4.1.6(2) Specifying application properties*.
9. Click the **OK** button.
   If you update the setting details in step 8, the new content goes into effect.

4.1.8 Deleting the settings for monitoring targets in Services

To delete the settings for monitoring targets in Services:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, select the **Services** tab.
   The Services window appears.
3. From the navigation frame, expand the hierarchy under the **Machines** folder.
   A folder with the name of the host on which Performance Management service is installed appears. When you expand the folder with the host name, the services installed on this host appear.

The name of each service is displayed as a service ID. For details about service IDs, see *B. List of Identifiers* and the section that describes service-naming rules in the appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The service ID format differs depending on whether the product name display function is enabled. For details about this function, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4. Expand the hierarchy under the monitoring agent host's folder and select a remote agent (*device-ID<product-name>*).

   A check mark is displayed for the selected remote agent.

5. In the method frame, select the **Properties** method.

   The Service Properties window appears.

6. Under the **Remote Monitor Configuration** tree, select the **ADDITION OR DELETION A SETTING** tree.

7. On the bottom of the information frame, from **DELETE AN APPLICATION MONITORING SETTING**, select the application name of the monitoring target you want to delete and click the **OK** button.

   The setting content is deleted.

4.1.9 Setup using non-interactive commands

You can set up the collection of process operation status information by executing commands.

You can also set up the collection of process operation status information in the Agents tree window of PFM - Web Console. However, when you use commands, batch processing can automate the setup tasks during maintenance, for example.

4.1.10 Using commands to set up monitoring targets

To use commands to set up monitoring targets:

1. Create an application definition file.
2. Create an application.
3. Bind an alarm table to the monitoring agent.

To collect operation status information on a per-process or per-service basis, specify only a single process or service when creating the application. To collect operation status information on a per-application basis, specify multiple processes or services when creating the application.

The subsections below provide a detailed description of how to set up a monitoring target.

For details about the `jpcmkkey`, `jpcprocdef create`, `jpcprocdef output`, and `jpctool alarm bind` commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

The service ID differs depending on various conditions such as the instance name, monitoring target name, and PFM - RM host name. For example, if the instance name is `inst1`, the monitoring target is `targethost1`, and the PFM - RM host name is `lhost1`, the service ID becomes `7A1inst1[targethost1@lhost1]`. For details about service IDs, see the section that describes service-naming rules in the appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(1) Creating an authentication key file

On the host on which PFM - Web Console is installed, create an authentication key file by executing the `jpcmkkey` command.

This step is not necessary if an authentication key file has already been created.

The following is an example of command execution that creates an authentication key file when `ADMINISTRATOR` is the user name to be used for login authentication and `xxxxx` is the password used during execution:

```
jpcmkkey -user "ADMINISTRATOR" -password "xxxxx"
```

(2) Creating an application definition file

Describe the conditions necessary for collecting the process operation status information in an application definition file (XML format). The application definition file is used as the parameter file for the `jpcprocdef create` command during application creation.

Execute this command by logging in to the host on which PFM - Web Console is installed.

If you are creating a new application definition file, you can use the sample shown below as a template.

When PFM - Web Console is running under Windows

PFM - Web-Console-installation-folder`\sample\processmonitoringcommand\jpcprocdef-parameters-windows.xml`

When PFM - Web Console is running under UNIX

`/opt/jp1pcwebcon/sample/processmonitoringcommand/jpcprocdef-parameters-unix.xml`

If an application definition already exists and you want to edit its content to create a new application definition, output it by executing the `jpcprocdef output` command.

Execute this command by logging in to the host on which PFM - Web Console is installed.

Examples of how to specify the `jpcprocdef output` command are shown below.

To output the application definition to `c:\sample.xml` when PFM - Web Console is running under Windows:

`jpcprocdef output -agent` *service-ID* `-name application1 -f c:\sample.xml`

To output the application definition to `/tmp/sample.xml` when PFM - Web Console is running under UNIX:

`jpcprocdef output -agent` *service-ID* `-name application1 -f /tmp/sample.xml`

(3) Creating an application

Specify an application definition file for the `-f` option and execute the `jpcprocdef create` command to create an application.

Execute the `jpcprocdef create` command by logging in to the host on which PFM - Web Console is installed. The `jpcprocdef create` command creates an application for a single agent. To create an application for multiple agents, repeatedly execute the command using a batch process. Examples of how to specify the `jpcprocdef create` command are shown below.

When PFM - Web Console is running under Windows and the application definition setting information file is `c:\sample.xml`

```
jpcprocdef create -agent service-ID -f c:\sample.xml
```

When PFM - Web Console is running under UNIX and the application definition setting information file is `/tmp/sample.xml`

```
jpcprocdef create -agent service-ID -f /tmp/sample.xml
```

(4) Binding an alarm table to the monitoring agent

Bind an alarm table for monitoring the operation status information to the monitoring agent by executing the `jpctool alarm bind` command.

Execute this command by logging in to the host on which PFM - Manager is installed.

The alarm for monitoring the operation status information is called the Application Status alarm. Edit it as needed. For details about this alarm, see *Application Status* in *6. Monitoring Template*.

If an alarm table has already been bound, there is no need to bind it every time you set up a monitoring target.

You can use one of the following two methods to bind an alarm table:

- Binding the alarm table PFM RM Platform Template Alarms [APP] 09.10
- Binding a user-created alarm table

An example of specifying the `jpctool alarm bind` command for binding the alarm table PFM RM Platform Template Alarms [APP] 09.10 follows:

```
jpctool alarm bind -key RMPlatform -table "PFM RM Platform Template Alarms
[APP] 09.10" -id service-ID -add
```

An example of specifying the `jpctool alarm bind` command for binding for binding a user-created alarm table follows:

```
jpctool alarm bind -key RMPlatform -table user-created-alarm-table-name# -id
service-ID -add
```

#

For *user-created-alarm-table-name*, you can specify the name of any user-created alarm table.

If you want to monitor the status of a specific process only, you can create an alarm based on conditional expressions. For details about the conditional expression for monitoring only one specific process, see Table *4-2 Conditional expression for monitoring a specific process only* in *4.1.2(2) Binding an alarm table to the monitoring agent*.

4.1.11 Using commands to delete settings for a monitoring target

To use commands to delete settings for a monitoring target:

1. Check the definition name of the application definition you want to delete.
2. Unbind the alarm table.

3. Delete the application definition.

For details about the `jpcmkkey`, `jpcprocdef list`, `jpctool alarm unbind`, and `jpcprocdef delete` commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

The service ID differs depending on various conditions such as the instance name, monitoring target name, and PFM - RM host name. For example, if the instance name is `inst1`, the monitoring target is `targethost1`, and the PFM - RM host name is `lhost1`, the service ID becomes `7A1inst1[targethost1@lhost1]`. For details about service IDs, see the section that describes service-naming rules in the appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(1) Creating an authentication key file

On the host on which PFM - Web Console is installed, create an authentication key file by executing the `jpcmkkey` command.

This step is not necessary if an authentication key file has already been created.

The following example shows a command execution that creates an authentication key file when `ADMINISTRATOR` is the user name to be used for login authentication and `xxxxx` is the password used during execution:

```
jpcmkkey -user "ADMINISTRATOR" -password "xxxxx"
```

(2) Checking the definition name of the application definition to be deleted

You can check the definition name of the application definition you want to delete from the list of application definitions defined in the monitoring agent by executing the `jpcprocdef list` command.

Execute the `jpcprocdef list` command by logging in to the host on which PFM - Web Console is installed. An example of how to specify this command follows:

```
jpcprocdef list -agent service-ID
```

(3) Unbinding the alarm table

Unbind the alarm table that is bound to the monitoring agent and stop any monitoring by executing the `jpctool alarm unbind` command.

Execute this command by logging in to the host on which PFM - Web Console is installed.

If the alarm table has already been unbound, there is no need to unbind it every time you delete a setting of a monitoring target.

An example of how to specify the `jpctool alarm unbind` command for unbinding the alarm table PFM RM Platform Template Alarms [APP] 09.10 follows:

```
jpctool alarm unbind -key RMPlatform -table "PFM RM Platform Template
Alarms [APP] 09.10" -id service-ID
```

(4) Deleting the application definition

Delete the application definition by executing the `jpcprocdef delete` command.

Execute this command by logging in to the host on which PFM - Web Console is installed.

The `jpcprocdef delete` command deletes an application definition for a single agent. To delete application definitions for multiple agents, repeatedly execute the command using a batch process.

An example of how to specify the `jpcprocdef delete` command for deleting application definition `application5` follows:

```
jpcprocdef delete -agent service-ID -name "application5"
```

4.1.12 Specifying whether process or service names to be used as monitoring targets will be case-sensitive

You can specify whether process or service names to be used as monitoring targets will be case-sensitive.

If the OS of the monitored host is Windows, the names are not case-sensitive by default. If the OS of the monitored host is UNIX, the names are case-sensitive by default.

To specify whether the process or service names to be used as monitoring targets will be case-sensitive:

1. From the browser of the monitoring console, log in to PFM - Web Console.
   The Main window appears.
2. In the navigation frame of the Main window, select the **Services** tab.
   The Services window appears.
3. In the Services window, select a remote agent (*device-ID<product-name>*).
   A check mark is displayed for the selected remote agent.
4. In the method frame, select the **Properties** method.
   The Service Properties window appears.
5. Select the **Remote Monitor Configuration - Application monitoring setting** tree.
   The window for entering property information appears at the bottom of the information frame.
6. Change the value of the **Case Sensitive** property.
   Select either of the following:
   - **Yes**: Case-sensitive
   - **No**: Not case-sensitive
7. Click the **OK** button.
   The setting is applied.

The following table shows the differences in actions based on the value of the **Case Sensitive** property.

Table 4–5: Differences in actions based on the value of the Case Sensitive property

Name of the process that is running	MonitoringXX Condition property setting	Case Sensitive property setting	Number of processes
• ProcessA • PROCESSA	ProcessA	Yes	1
		No	2
	PROCESSA	Yes	1
		No	2
	processa	Yes	0
		No	2

Legend:

Yes: Case-sensitive

No: Not case-sensitive

The above table shows differences in the number of processes that are judged to be running based on the settings of the `Monitoring`*XX*`Condition` and `Case Sensitive` properties in an environment in which two kinds of processes (`ProcessA` and `PROCESSA`) are running on the monitored host.

Note:

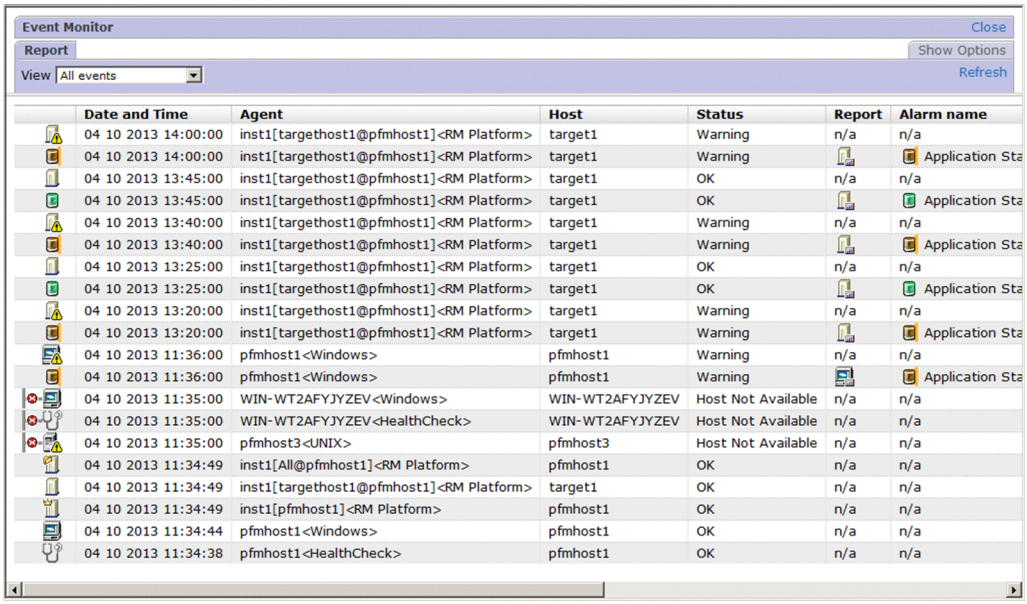
The setting of the `Case Sensitive` property affects all application definitions. Therefore, if you change the setting of the `Case Sensitive` property, check, and if necessary, revise the existing application definitions.

4.2 Example of the procedure to follow when an alarm is issued during the collection of process operation status information

This section shows an example of the procedure to identify the process that resulted in a warning if an alarm is issued when the collection of process operation status information is set.

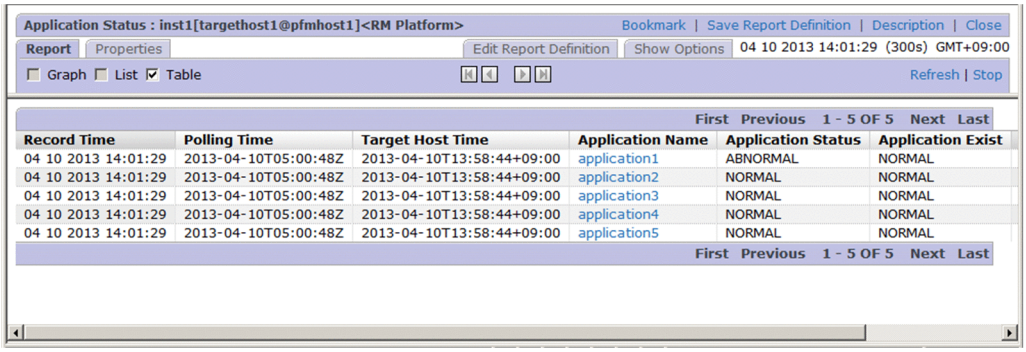
For details about alarms and reports, see *6. Monitoring Template*.

1. In the menu bar frame of the Main window, select the **Event Monitor** menu.
   The Event Monitor window appears.



	Date and Time	Agent	Host	Status	Report	Alarm name
	04 10 2013 14:00:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	Warning	n/a	n/a
	04 10 2013 14:00:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	Warning		Application Sta
	04 10 2013 13:45:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	OK	n/a	n/a
	04 10 2013 13:45:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	OK		Application Sta
	04 10 2013 13:40:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	Warning	n/a	n/a
	04 10 2013 13:40:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	Warning		Application Sta
	04 10 2013 13:25:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	OK	n/a	n/a
	04 10 2013 13:25:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	OK		Application Sta
	04 10 2013 13:20:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	Warning	n/a	n/a
	04 10 2013 13:20:00	inst1[targethost1@pfmhost1]<RM Platform>	target1	Warning		Application Sta
	04 10 2013 11:36:00	pfmhost1<Windows>	pfmhost1	Warning	n/a	n/a
	04 10 2013 11:36:00	pfmhost1<Windows>	pfmhost1	Warning		Application Sta
	04 10 2013 11:35:00	WIN-WT2AFYJYZEV<Windows>	WIN-WT2AFYJYZEV	Host Not Available	n/a	n/a
	04 10 2013 11:35:00	WIN-WT2AFYJYZEV<HealthCheck>	WIN-WT2AFYJYZEV	Host Not Available	n/a	n/a
	04 10 2013 11:35:00	pfmhost3<UNIX>	pfmhost3	Host Not Available	n/a	n/a
	04 10 2013 11:34:49	inst1[All@pfmhost1]<RM Platform>	pfmhost1	OK	n/a	n/a
	04 10 2013 11:34:49	inst1[targethost1@pfmhost1]<RM Platform>	target1	OK	n/a	n/a
	04 10 2013 11:34:49	inst1[pfmhost1]<RM Platform>	pfmhost1	OK	n/a	n/a
	04 10 2013 11:34:44	pfmhost1<Windows>	pfmhost1	OK	n/a	n/a
	04 10 2013 11:34:38	pfmhost1<HealthCheck>	pfmhost1	OK	n/a	n/a

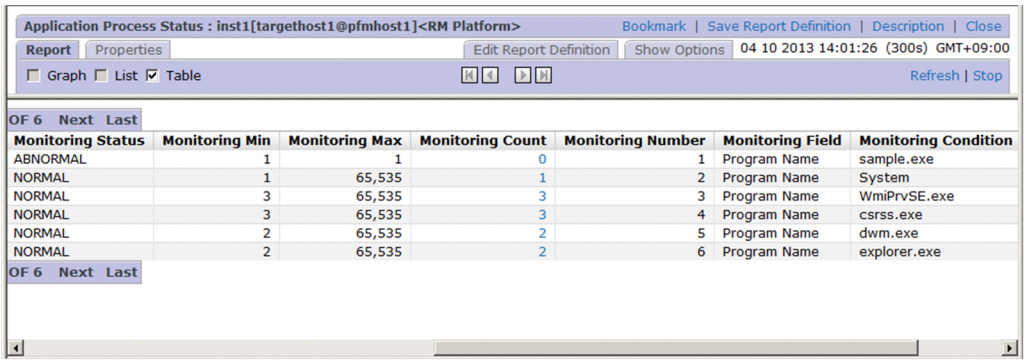
2. Click the report icon of the alarm for which a warning has been issued.
   An Application Status report appears.



Record Time	Polling Time	Target Host Time	Application Name	Application Status	Application Exist
04 10 2013 14:01:29	2013-04-10T05:00:48Z	2013-04-10T13:58:44+09:00	application1	ABNORMAL	NORMAL
04 10 2013 14:01:29	2013-04-10T05:00:48Z	2013-04-10T13:58:44+09:00	application2	NORMAL	NORMAL
04 10 2013 14:01:29	2013-04-10T05:00:48Z	2013-04-10T13:58:44+09:00	application3	NORMAL	NORMAL
04 10 2013 14:01:29	2013-04-10T05:00:48Z	2013-04-10T13:58:44+09:00	application4	NORMAL	NORMAL
04 10 2013 14:01:29	2013-04-10T05:00:48Z	2013-04-10T13:58:44+09:00	application5	NORMAL	NORMAL

3. Look for the lines where **ABNORMAL** is shown for **Application Status** or **Application Exist** to identify the application for which a warning was issued.

4. Under **Application Name**, select the application for which a warning was issued.
   Here, `application1` is selected.
   An Application Process Status report appears.



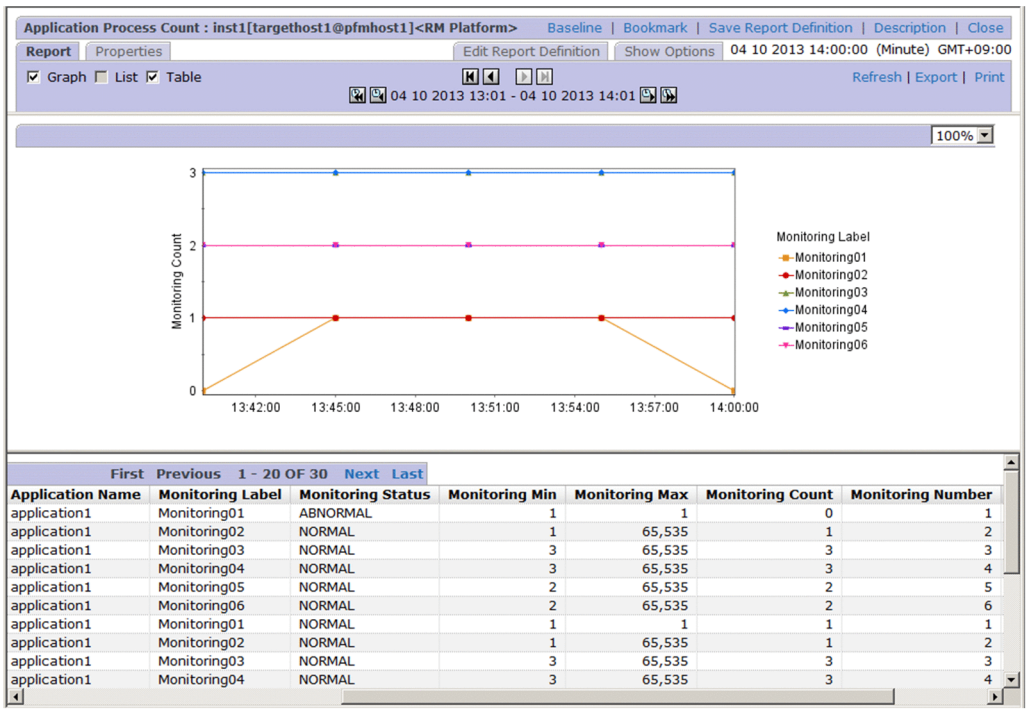
Monitoring Status	Monitoring Min	Monitoring Max	Monitoring Count	Monitoring Number	Monitoring Field	Monitoring Condition
ABNORMAL	1	1	0	1	Program Name	sample.exe
NORMAL	1	65,535	1	2	Program Name	System
NORMAL	3	65,535	3	3	Program Name	WmiPrvSE.exe
NORMAL	3	65,535	3	4	Program Name	csrss.exe
NORMAL	2	65,535	2	5	Program Name	dwm.exe
NORMAL	2	65,535	2	6	Program Name	explorer.exe

5. Look for the lines where **ABNORMAL** is shown for **Monitoring Status** to identify the process for which a warning was issued.

   Here, you can see that a warning was issued for `sample.exe`.

6. If you have collected the log data for the `PD_APPC` record, select a **Monitoring Count** value as needed.

   An Application Process Count report appears. You can check the status of each process and whether the log related to the process count has increased or decreased.



Application Name	Monitoring Label	Monitoring Status	Monitoring Min	Monitoring Max	Monitoring Count	Monitoring Number
application1	Monitoring01	ABNORMAL	1	1	0	1
application1	Monitoring02	NORMAL	1	65,535	1	2
application1	Monitoring03	NORMAL	3	65,535	3	3
application1	Monitoring04	NORMAL	3	65,535	3	4
application1	Monitoring05	NORMAL	2	65,535	2	5
application1	Monitoring06	NORMAL	2	65,535	2	6
application1	Monitoring01	NORMAL	1	1	1	1
application1	Monitoring02	NORMAL	1	65,535	1	2
application1	Monitoring03	NORMAL	3	65,535	3	3
application1	Monitoring04	NORMAL	3	65,535	3	4

Note:

If the alarm status is cancelled while a real-time report is being displayed, you cannot use the report to identify the process or service for which a warning was issued. An example of a real-time report is an Application Status report displayed by the event monitor, or an Application Process Status report displayed from an Application Status report. In this case, view the event monitor or an Application Process Count report (log report) to check the status transition that has occurred since the alarm was issued.

5 Operation in a Cluster System

This chapter describes the installation and setup of PFM - RM for Platform in a cluster system and the operating procedures when PFM - RM for Platform is run in a cluster system.

5.1 Configuration of PFM - RM for Platform in a cluster system

This section describes the configuration in which PFM - RM for Platform is run in a cluster system. For an overview of cluster systems and details about the system configuration for running the Performance Management system in a cluster system, see the chapter that describes system construction and operations in a cluster system in the *Job Management Partner 1/Performance Management User's Guide*.

If you run PFM - RM for Platform in a cluster system, you can improve availability because the system operation can be maintained by failover in the event of a problem.

To run PFM - RM for Platform in a cluster system, you must configure an environment in which the same instance of PFM - RM for Platform can be run in both the executing node and the standby node. Also you must store all data, such as data files, configuration files, and log files, on a shared disk.

When PFM - RM for Platform is run in a cluster system, it is configured as shown below.

Figure 5–1: Example of the configuration of PFM - RM for Platform in a cluster system (when PFM - RM for Platform is installed on the PFM - Manager host)

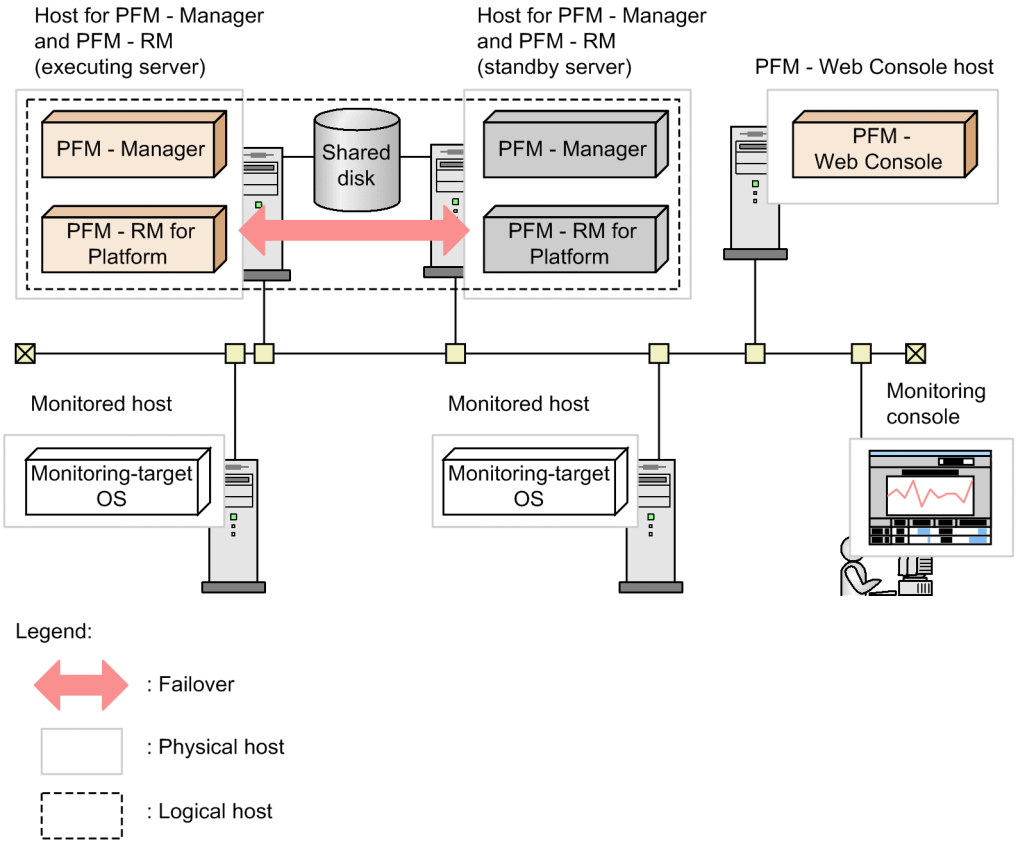
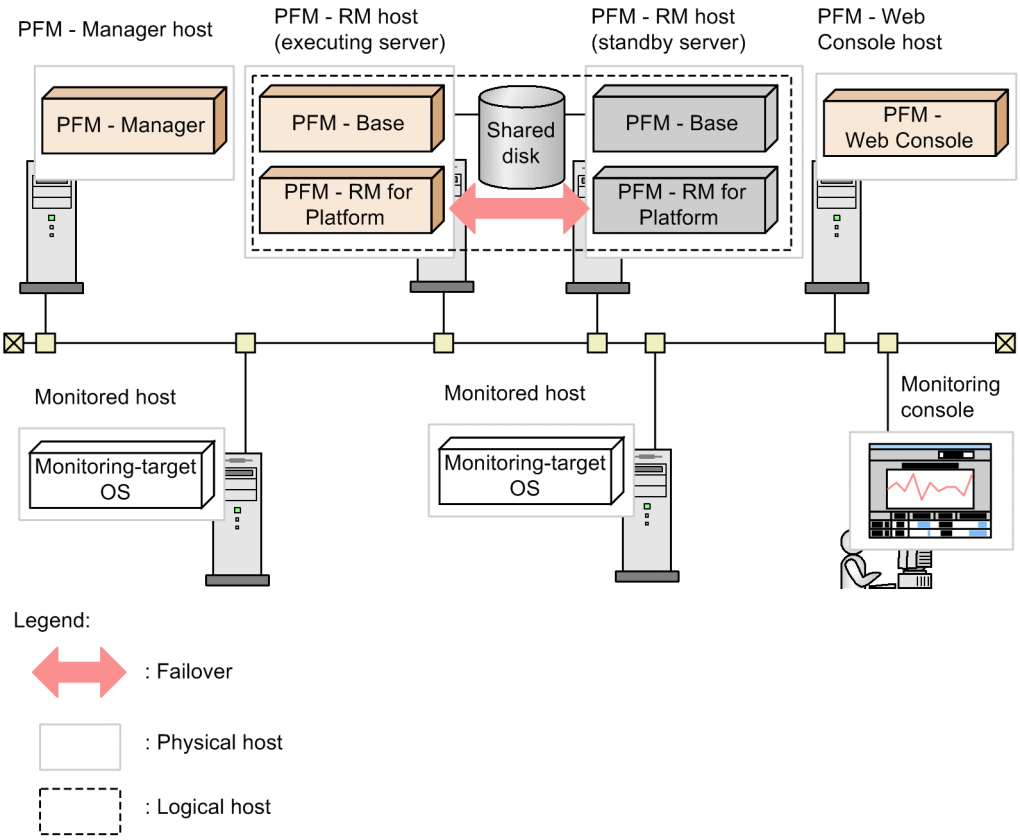


Figure 5–2: Example of the configuration of PFM - RM for Platform in a cluster system (when PFM - RM for Platform is installed on a different host from the PFM - Manager host)



PFM - RM for Platform in a cluster system runs in a logical host environment and monitors other hosts as monitoring targets. Therefore, you must configure the system in such a manner that the same host names can be used to connect to the monitored hosts from each host.

PFM - RM for Platform stores necessary information on the shared disk, such as definition and performance information, and inherits this information in the event of a failover. If a single logical host contains multiple Performance Management programs, all of them use the same shared directory.

You can run multiple PFM - RM for Platforms at the same node. If there are multiple cluster configurations (active-active configuration), run PFM - RM for Platform in each logical host environment. You can operate each PFM - RM for Platform independently and have them perform failover separately.

5.2 Processing when a failover occurs

If a failure occurs on the executing node, control shifts to the standby node.

This section describes the failover processing when a failure occurs in PFM - RM for Platform. It also describes the effects of a PFM - Manager failure on PFM - RM for Platform.

5.2.1 Failover when an error occurs at the PFM - RM host

The following figure shows the processing when failover occurs at the host PFM - RM host.

Figure 5–3: Processing when failover occurs at the PFM - RM host (when PFM - RM for Platform is installed on the PFM - Manager host)

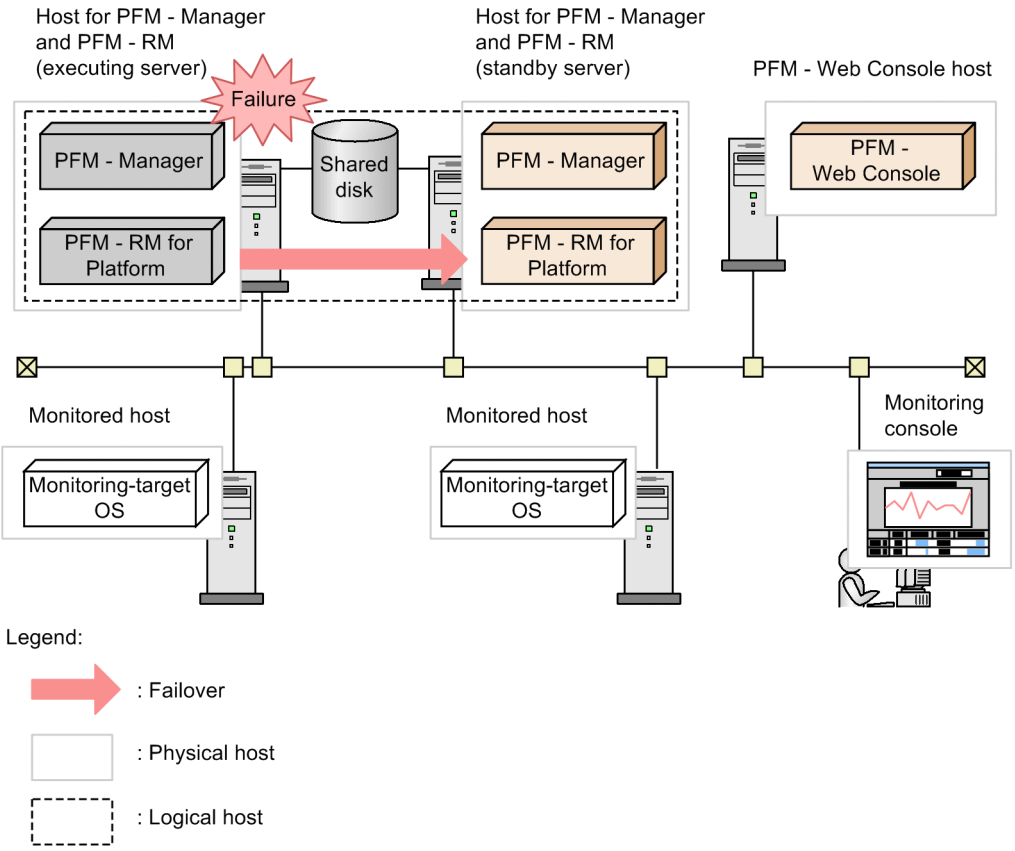
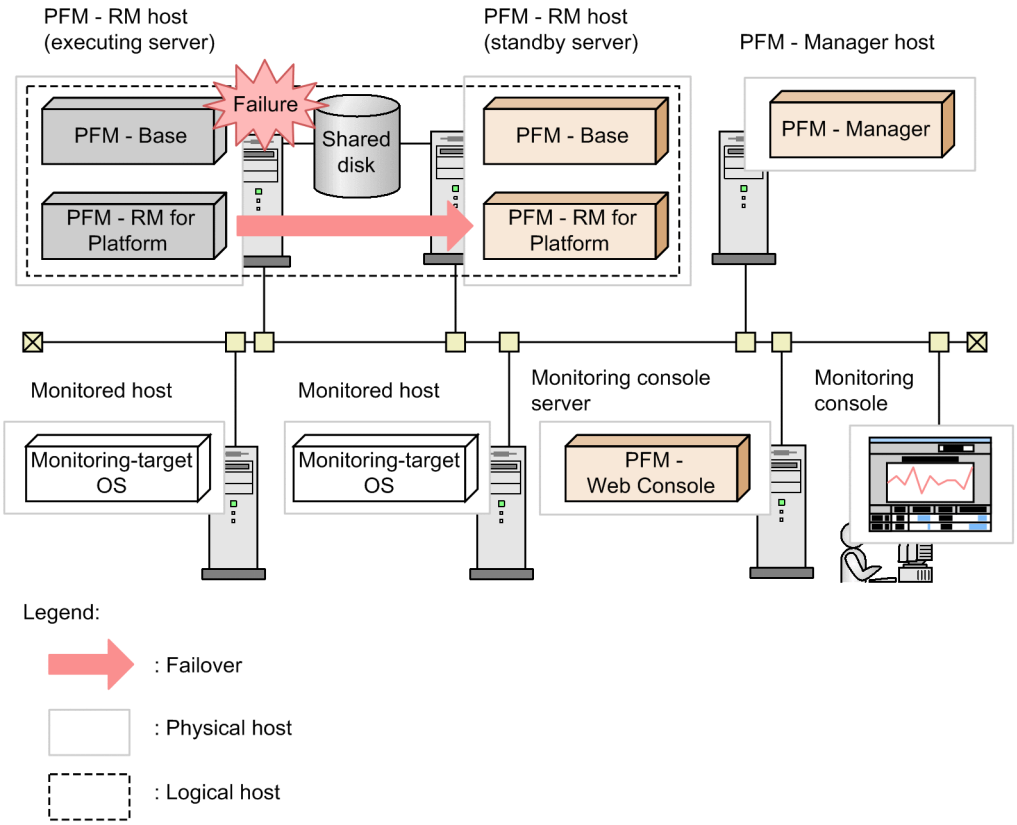


Figure 5–4: Processing when failover occurs at the PFM - RM host (when PFM - RM for Platform is installed on a different host from the PFM - Manager host)



If PFM - Web Console is used while PFM - RM for Platform is engaged in failover processing, the message `There was no answer(-6)` is displayed. If this message is displayed, wait until failover processing is completed.

Once failover is completed at PFM - RM for Platform, an attempt to use PFM - Web Console connects you to the PFM - RM for Platform that has started at the target node, so that you can perform operations.

5.2.2 Effects of PFM - Manager shutdown and the action to take

A shutdown of PFM - Manager has effects on the entire Performance Management system.

PFM - Manager provides centralized management of the agent information for PFM - RM for Platform that is running at each node. It also controls alarm event notifications when thresholds are exceeded during performance monitoring by PFM - RM for Platform as well as execution of actions based on alarm events.

The following describes the effects of a PFM - Manager shutdown on PFM - RM for Platform.

Effects

If PFM - Manager shuts down while PFM - RM for Platform is running, the effects described below result. Note that collection of performance data continues.

- Because alarm events cannot be reported to PFM - Manager, alarm events are retained for each alarm definition. PFM - RM for Platform retries notification until PFM - Manager starts. When the number of retained alarm events exceeds 3, the oldest alarm event is overwritten. If PFM - RM for Platform is shut down, the retained alarm events are deleted.

- Any notification of alarm status already sent to PFM - Manager is reset when PFM - Manager restarts. The alarm status is refreshed after PFM - Manager has checked the status of PFM - RM for Platform.
- Shutting down PFM - RM for Platform takes a while because no notification of this event can be sent to PFM - Manager.

Action

Start PFM - Manager. An active PFM - RM for Platform can continue its operation. However, alarms might not be notified as expected.

After PFM - Manager has been recovered, check the common message log for the `KAVE00024-I` message.

Evaluate the operation method, taking into account the effects of PFM - Manager shutdown. In addition to problems, events such as configuration change and maintenance might require shutdown of PFM - Manager. We recommend that you ensure that shutdowns for maintenance purposes be performed only when the shutdown will have the least adverse effects on operations.

5.3 Installation and setup in a cluster system (for Windows)

This section describes the procedures for installing and setting up PFM - RM for Platform in a cluster system.

For details about how to install and set up PFM - Manager, see the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

5.3.1 Items to be checked before installing in a cluster system (for Windows)

This subsection describes items to be checked before you start installation of PFM - RM for Platform.

(1) Prerequisites

Following are the prerequisites for using PFM - RM for Platform in a cluster system.

(a) Cluster system

Make sure that the following conditions are satisfied:

- The cluster system is controlled by cluster software.
- The cluster software is set up in such a manner that it controls startup and termination of the PFM - RM for Platform that is running on the logical host.

Iin addition, suppress error notification, as described in the following subsections.

Suppressing error notification using Dr. Watson in Windows Server 2003 (primary and secondary nodes)

Failover might fail if a message box for an application error is displayed in the Dr. Watson log. To protect against this possibility, error notification using this message box needs to be suppressed. Note that the suppression of error notification might adversely affect information acquisition in the event of application errors.

1. To enable the Dr. Watson setting, enter `drwtsn32 -i` at the command prompt.

   Dr. Watson is installed as the default application debugger.
2. From the **Start** menu, select **Run**.
3. Enter `drwtsn32` in the text box and click the **OK** button.
4. In the Dr. Watson dialog box, clear the **Visual Notification** check box.
5. Click the **OK** button.

Suppressing error notification to Microsoft (primary and secondary nodes)

In Windows, a dialog box reporting an error to Microsoft is displayed in the event of an application error. Because this dialog box might cause failover to fail, this error reporting needs to be suppressed.

In Windows Server 2003

1. In **Control Panel**, choose **System**.
2. In the System Properties dialog box, under the **Advanced** tab, click the **Error Reporting** button.
3. In the Error Reporting dialog box, select the **Disable error reporting** radio button, and then clear **But notify me when critical errors occur**.
4. Click the **OK** button.

In Windows Server 2008 or Windows Server 2012

1. Choose **Control Panel** > **System and Security** > **Action Center** > **Maintenance**.
2. In **Check for solutions to problem reports**, click **Settings**.
3. In the Choose when to check for solutions to problem reports dialog box, choose **Never check for solutions (not recommended).**
4. Click the **OK** button.

(b) Shared disk

Make sure that the following conditions are satisfied:

- A shared disk is available to each logical host and information can be inherited from the executing node to the standby node.
- The shared disk is connected to each node physically by Fibre Channel or SCSI.[#1]
- The shared disk can be placed offline forcibly by means such as the cluster software in order to implement failover even when there is still an active process that is using the shared disk.
- If multiple PFM products are running on the same logical host, the shared disk uses the same directory names.[#2]

#1

Performance Management does not support a configuration that uses a network drive or a disk replicated via the network as the shared disk.

#2

You can change the storage location of the Store database and store it in a different folder on the shared disk.

(c) Logical host names and logical IP addresses

Make sure that the following conditions are satisfied:

- Each logical host has a logical host name and a corresponding logical IP address, and that this information can be inherited from the executing node to the standby node.
- The logical host names and logical IP addresses are set in the `hosts` file and name server.
- If DNS operation is employed, the host name without the domain name is used as the logical host name, not the FQDN name.
- All physical and logical host names are unique within the system.

Important note

- Do not specify a physical host name (host name displayed by the `hostname` command) as a logical host name. If you do so, normal communication processing might not occur.
- A logical host name is expressed using from 1 to 32 bytes of alphanumeric characters. None of the following symbols nor the space character can be used:
  `/ \ : ; * ? ' " < > | & = , .`
- You cannot specify a logical host name that begins with the character string `localhost`, an IP address, or a hyphen (-).

(d) Settings for using IPv6

Performance Management supports both IPv4 and IPv6 network environments. Therefore, you can run Performance Management even in a network environment where IPv4 and IPv6 coexist.

PFM - RM for Platform can use IPv6 to communicate with PFM - Manager. However, this applies only when the OS of the hosts on which PFM - RM for Platform and PFM - Manager are installed are Windows Server 2008 R2, Windows Server 2012, or Linux. For details about the applicable scope of communication in the IPv4 and IPv6 environments, see *L. Communication in IPv4 and IPv6 Environments*.

To communicate in IPv6, you must enable the use of IPv6 on both the PFM - Manager host and the PFM - RM host. You specify this setting by executing the `jpcconf ipv6 enable` command. The following explains the conditions to use for determining whether you need to execute this command.

Cases in which you need to execute the `jpcconf ipv6 enable` command:

- When all hosts are being changed from an IPv4 environment to an IPv6 environment
- In an environment where IPv4 and IPv6 coexist and PFM - Manager is being changed from an IPv4 environment to an IPv6 environment

Cases in which you do not need to execute the `jpcconf ipv6 enable` command:

- When all hosts are already in an IPv6 environment
- In an environment where IPv4 and IPv6 coexist and PFM - Manager is already in an IPv6 environment

An example of executing the `jpcconf ipv6 enable` command follows:

```
jpcconf ipv6 enable
```

Execute the `jpcconf ipv6 enable` command separately on the executing node and on the standby node.

For details about the `jpcconf ipv6 enable` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*. For details about the conditions and timing for executing the `jpcconf ipv6 enable` command, see the chapter that describes an example of a network configuration that includes an IPv6 environment in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

When PFM - RM for Platform will use IPv6 to communicate with monitored hosts, specify a monitored host name that can be resolved.

PFM - RM for Platform uses a resolvable IP address to communicate with a monitoring target. When PFM - RM for Platform communicates with a monitoring target in an environment where IPv4 and IPv6 coexist, PFM - RM for Platform will not try to communicate using another IP address if communication using a resolvable IP address fails.

For example, if a connection attempt using IPv4 fails, PFM - RM for Platform will not retry using IPv6. Conversely, if a connection attempt using IPv6 fails, PFM - RM for Platform will not retry using IPv4. Therefore, make sure beforehand that connection can be established.

(e) WMI connection

Make sure that the following conditions are satisfied:

- The same user account that can connect to the monitored hosts by using WMI is available in the environments for both the executing node and the standby node.

For details about the WMI connection settings, see *3.1.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows)*.

(f) SSH connection

Make sure that the following conditions are satisfied:

- A private key using the same path is available in the environments for both the executing node and the standby node.
- That private key can be used to connect to the monitored hosts.
- PuTTY is installed on the same path in the environments for both the executing node and the standby node.
- ActivePerl is installed on the same path in the environments for both the executing node and the standby node.

Note:

Use one of the following methods to register the private and public keys:

- Copy the private key created on the executing server to the standby server, and then establish its correspondence with the public key that is distributed from the executing server to the monitored host.
- Create public keys on both the executing and standby servers, and then establish correspondence between them by registering both public keys on the monitored hosts.

For details about the SSH connection settings, see *3.1.6 SSH connection setting method for Windows (when the PFM - RM host is running Windows and the monitored host is running UNIX)*.

(2) Information needed for setting up PFM - RM for Platform for logical host operation

If you run PFM - RM for Platform on a logical host, you need the information listed in the table below in addition to the environment information that is needed for setting up a normal PFM - RM for Platform.

Table 5–1: Information needed for setting up PFM - RM for Platform for logical host operation

No.	Item	Example
1	Logical host name	`jp1-halrmp`
2	Logical IP address	`172.16.92.100`
3	Shared disk	`S:\jp1`

If multiple Performance Management programs are running on the same logical host, all of them must use folders on the same shared disk.

For details about the space requirements on the shared disk, see *A. Estimating System Requirements*.

(3) Notes about logical host failover

If you employ a system configuration in which PFM - RM for Platform runs on a logical host, evaluate whether the entire logical host should failover in the event of a PFM - RM for Platform failure.

If a PFM - RM for Platform failure is to result in failover of the entire logical host, any other job application that is running on the logical host will also result in failover, which might affect the job adversely.

Typically, we recommend that you use one of the following cluster software settings so that errors on PFM - RM for Platform do not affect the operation of other applications:

- Operation of PFM - RM for Platform is not monitored.
- Detection of PFM - RM for Platform errors does not result in failover.

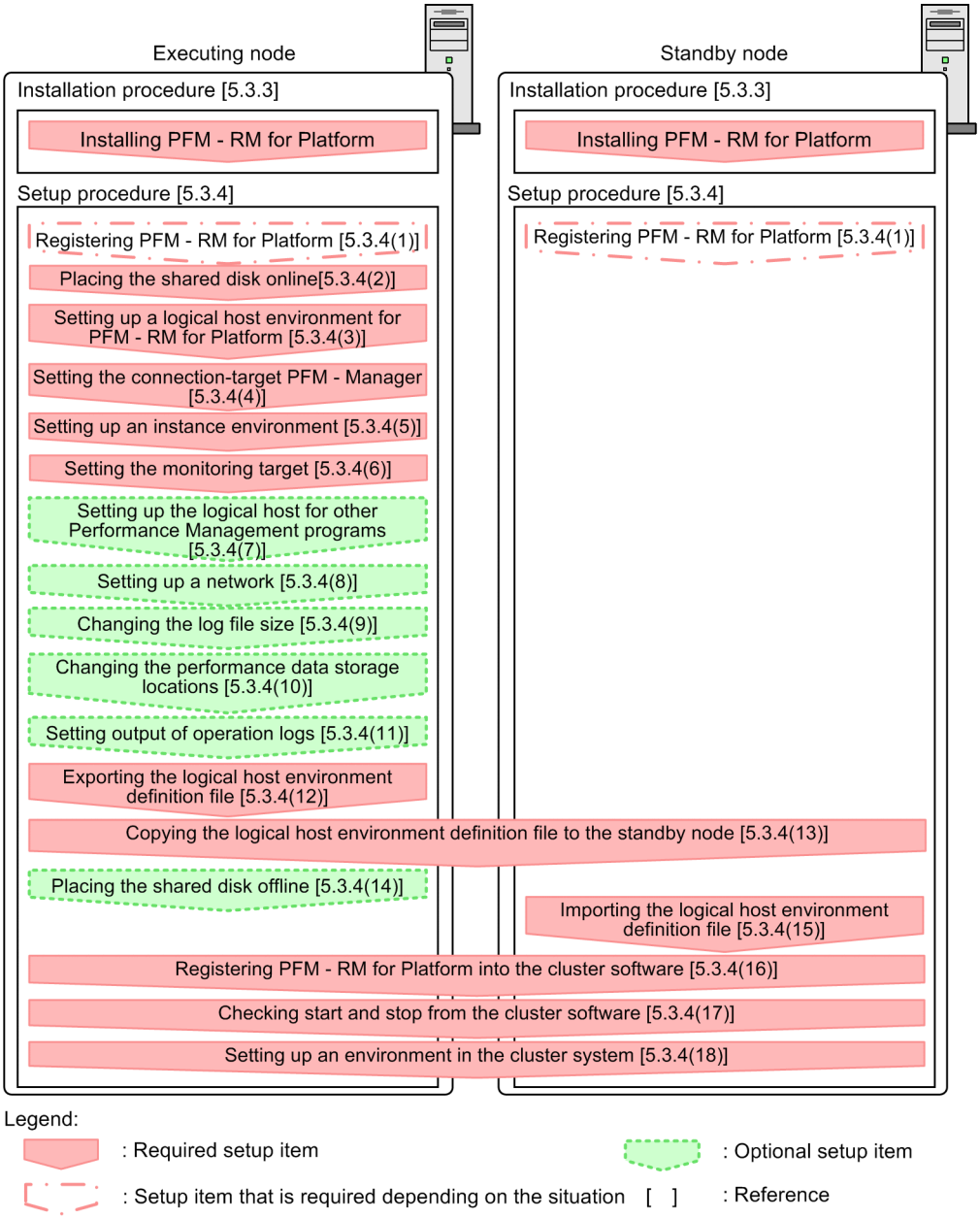
(4) Notes about upgrading when logical operation is used

To upgrade a PFM - RM for Platform that is running on a logical host, you must place the shared disk online at either the executing node or the standby node.

5.3.2 Flow of installation and setup in a cluster system (for Windows)

The following figure shows the procedures for installing and setting up PFM - RM for Platform in a cluster system.

Figure 5–5: Installation and setup procedures in a cluster system (for Windows)



Note:

Setting up PFM - RM for Platform in a logical host environment does not automatically inherit the existing PFM - RM Platform definition from the physical host environment. New environments are created when an instance environment is set up in the logical and physical host environments.

For setup commands that require a user input, you can select whether to execute the commands in the interactive or non-interactive mode.

When a command is executed in the interactive mode, the user must enter a value in response to the instruction from the command.

When a command is executed in the non-interactive mode, no user input is required because option specification or a definition file replaces the input step required during interactive command execution. Furthermore, batch processing or remote execution can automate the setup procedure, thereby reducing the workload on the administrator and the operating costs. Commands in the non-interactive mode are convenient in the following cases:

- You want to change the password used for connecting to monitoring targets on a regular basis.
- You want to improve the efficiency of the procedure for adding multiple monitoring targets.

For details about commands, see the manual *Job Management Partner 1/Performance Management Reference*.

5.3.3 Installation procedure in a cluster system (for Windows)

Install PFM - Base and PFM - RM for Platform on both the executing node and the standby node.

Important note

The installation target is the local disk. Do not install PFM - RM for Platform on a shared disk.

The installation procedure is the same as for non-cluster systems. For details about the installation procedure, see *3.1.3 Installation procedure for the Windows edition*.

5.3.4 Setup procedure in a cluster system (for Windows)

This subsection describes the setup needed for running Performance Management in a cluster system.

To run Performance Management in a cluster system, you must set up both the executing node and the standby node. Set up the executing node first, and then set up the standby node.

Executing system indicates an item that is to be executed at the executing node, and Standby system indicates an item that is to be executed at the standby node. Optional indicates the following setup items:

- Setup item that is required depending on the environment in use
- Setup item for changing the default settings

Important note

Do not set `JPC_HOSTNAME` as an environment variable because it is used by Performance Management. If it is set as an environment variable by mistake, Performance Management will not function correctly.

(1) Registering PFM - RM for Platform Executing system Standby system Optional

To achieve central management of PFM - RM for Platform in the Performance Management system, you must register PFM - RM for Platform into PFM - Manager and PFM - Web Console.

You must register PFM - RM for Platform at the following times:

- When you add a new PFM - RM for Platform in the Performance Management system.
- When you update the Data model version for the registered PFM - RM for Platform.

You use PFM - Manager and PFM - Web Console to register PFM - RM for Platform. The registration procedure is the same as when a cluster system is not used. For details about the procedure, see *3.1.4(1) Registering PFM - RM for Platform*.

(2) Placing the shared disk online Executing system

Make sure that the shared disk is online.

If the shared disk is not in online status, use a program such as the cluster software or a volume manager to place it online.

(3) Setting up a logical host environment for PFM - RM for Platform Executing system

Execute the `jpcconf ha setup` command to create a logical host environment.

This command creates a logical host environment by copying necessary data to the shared disk and setting definitions for a logical host.

Note

Before you execute the command, stop all Performance Management programs and services in the entire Performance Management system. For details about how to stop services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

To set up a logical host environment for PFM - RM for Platform:

1. Execute the `jpcconf ha setup` command to create a logical host environment for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf ha setup -key RMPlatform -lhost jp1-halrmp -d S:\jp1
   ```

   Use the `-lhost` option to specify the logical host name. This example specifies `jp1-halrmp` as the logical host name. If you employ DNS operations, specify the logical host name without the domain name.

   Specify in the `-d` option a folder name on the shared disk within the environment folder. For example, if `-d S:\jp1` is specified, `S:\jp1\jp1pc` is created, and then files for the logical host environment are created.

2. Execute the `jpcconf ha list` command to check the logical host settings.

Execute the following command:

```
jpcconf ha list -key all
```

Make sure that the created logical host environment is correct.

(4) Setting the connection-target PFM - Manager Executing system

Execute the `jpcconf mgrhost define` command to set the PFM - Manager that manages PFM - RM for Platform.

To set the connection-target PFM - Manager:

1. Execute the `jpcconf mgrhost define` command to set the connection-target PFM - Manager.
   Execute the following command:

   ```
   jpcconf mgrhost define -host jp1-hal -lhost jp1-halrmp
   ```

   Specify in the `-host` option the host name of the connection-target PFM - Manager. If the connection-target PFM - Manager is to run on a logical host, specify in the `-host` option the logical host name of the connection-target PFM - Manager. This example specifies `jp1-hal` as the PFM - Manager's logical host name.

   Use the `-lhost` option to specify the logical host name of PFM - RM for Platform. This example specifies `jp1-halrmp` as the logical host name of PFM - RM for Platform.

   The example above shows execution in the interactive mode, but you can also execute the `jpcconf mgrhost define` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(5) Setting up an instance environment Executing system

Execute the `jpcconf inst setup` command to set up an instance environment for PFM - RM for Platform.

The setup procedure is the same as when a cluster system is not employed. However, in the case of a cluster system, you must specify the logical host name in the `-lhost` option when you execute the `jpcconf inst setup` command.

The following shows how to specify the `jpcconf inst setup` command for a cluster system:

```
jpcconf inst setup -key RMPlatform -lhost logical-host-name -inst instance-
name
```

The example above shows execution in the interactive mode, but you can also execute the `jpcconf inst setup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

For details about the settings and procedure, see *3.1.4(2) Setting up an instance environment*.

(6) Setting the monitoring target Executing system

Execute the `jpcconf target setup` command to set information about the monitored host for PFM - RM for Platform.

The setting procedure is the same as when a cluster system is not employed.

However, in the case of a cluster system, you must specify the logical host name in the `-lhost` option when you execute the `jpcconf target setup` command.

The following shows how to specify the `jpcconf target setup` command for a cluster system:

```
jpcconf target setup -key RMPlatform -lhost logical-host-name -inst
instance-name -target monitoring-target-name
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf target setup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

For details about the settings and procedure, see *3.1.4(3) Setting the monitored host*.

(7) Setting up the logical host for other Performance Management programs Executing system Optional

If you have other PFM - Manager, PFM - Agent, or PFM - RM programs to be set up on the same logical host in addition to PFM - RM for Platform, set them up at this stage.

For details about the setup procedure, see the chapter that describes the configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

(8) Setting up a network Executing system Optional

You specify network settings if you need to change the network environment settings as appropriate to the network configuration where Performance Management is used.

The two network environment settings are described below. Change these settings if necessary.

- Setting IP addresses

  Set this information to use Performance Management in a network that is connected to multiple LANs. To specify an IP address to be used, directly edit the contents of the `jpchosts` file.

  Copy the edited `jpchosts` file from the executing node to the standby node under *physical-host-installation-folder* `\jp1pc\`.

  For details about how to set IP addresses, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Setting port numbers

  If you establish communication between Performance Management programs via a firewall, use the `jpcconf port define` command to set the port numbers.

  For details about how to set port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

(9) Changing the log file size Executing system Optional

The operation status of Performance Management is output to a log file unique to Performance Management. This log file is called the *common message log*. The common message log consists of two files with a default size of 2,048 kilobytes each. If necessary, use this setting to change this file size.

For details, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(10) Changing the performance data storage locations Executing system Optional

This setting is used to change the storage locations, backup folder, export folder, or import folder for the performance data that is managed by PFM - RM for Platform.

For details about the setting method, see *3.6.1 Changing performance data storage locations*.

(11) Action log output setting Executing system Optional

This setting is required in order to output action logs in the event of an alarm.

An action log consists of log information about exceeded threshold values caused by factors such as system loading; its output is linked with the alarm function. For details about the setting method, see *I. Outputting Action Log Data*.

(12) Exporting the logical host environment definition file Executing system

After you have created a logical host environment for PFM - RM for Platform, export the environment definition to a file.

This export process involves output of the definition information for the Performance Management program that has been set up on the logical host to a file in the batch mode. If you are setting up other Performance Management programs on the same logical host, export the environment definition after all the setup processes are completed.

To export the logical host environment definition:

1. Execute the `jpcconf ha export` command to export the logical host environment definition.

   Output the definition information for the logical host environment that has been created so far to an export file. You can assign any name to the export file.

   For example, to export the logical host environment definition to the `lhostexp.txt` file, execute the following command:

   ```
   jpcconf ha export -f lhostexp.txt
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf ha export` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(13) Copying the logical host environment definition file to the standby node Executing system Standby system

Copy from the executing node to the standby node the logical host environment definition file exported in *(12) Exporting the logical host environment definition file*.

(14) Placing the shared disk offline Executing system Optional

Use a program such as the cluster software or a volume manager to place the shared disk offline and finish the procedure.

If you will be using the shared disk after you complete this procedure, there is no need to place it offline.

(15) Importing the logical host environment definition file Standby system

Import to the standby node the export file that was copied from the executing node.

Use the `jpcconf ha import` command to specify settings for executing at the standby node the Performance Management program on the logical host that was created at the executing node. If multiple Performance Management programs have been set up on the same logical host, the settings for all the programs are imported in the batch mode.

When you execute this command, there is no need to keep the shared disk in online status.

To import the logical host environment definition file:

1. Execute the `jpcconf ha import` command to import the logical host environment definition.
   Execute the following command:

   ```
   jpcconf ha import -f lhostexp.txt
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf ha import` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

   This command changes settings in such a manner that the environment for the standby node becomes the same as for the export file. As a result, the setup for starting PFM - RM for Platform on the logical host is performed.

   If a fixed port number has been set by the `jpcconf port define` command during the setup, it is also set in the same manner.

2. Execute the `jpcconf ha list` command to check the logical host settings.
   Execute the following command:

   ```
   jpcconf ha list -key all
   ```

   Make sure that the displayed information is the same as when the `jpcconf ha list` command is executed at the executing node.

(16) Registering PFM - RM for Platform into the cluster software Executing system Standby system

To run a Performance Management program in a logical host environment, you must register the program into the cluster software and set up the environment in such a manner that the Performance Management program is started and terminated from the cluster software.

For details about how to register PFM - RM for Platform into the cluster software, see the cluster software documentation.

This subsection describes the settings for registering PFM - RM for Platform into the cluster software using an example of items that are registered into Windows MSCS.

For PFM - RM for Platform, register the services shown in the table below into the cluster software.

For dependency settings when PFM - RM for Platform coexists with PFM - Manager's logical host, see the chapter that describes planning and operation in the *Job Management Partner 1/Performance Management User's Guide*.

Table 5–2: PFM - RM for Platform services to be registered into the cluster software

No.	Name	Service name	Resource dependencies
1	`PFM - RM Store for Platform` *instance-name* [*LHOST*]	`JP1PCAGT_7S`_*instance-name* [*LHOST*]	• IP address resources • Physical disk resources
2	`PFM - RM for Platform` *instance-name* [*LHOST*]	`JP1PCAGT_7A`_*instance-name* [*LHOST*]	• Cluster resources in No. 1

No.	Name	Service name	Resource dependencies
3	PFM - Action Handler [*LHOST*]	JP1PCMGR_PH [*LHOST*]	• IP address resources • Physical disk resources

Replace [*LHOST*] with the logical host name. If the instance name is SDC1 and the logical host name is jp1-halrmp, then the name of the service is PFM - RM Store for Platform SDC1 [jp1-halrmp], and the service name is JP1PCAGT_7S_SDC1 [jp1-halrmp].

In the case of MSCS, register these services as MSCS resources. Set each resource as follows:

- In **Resource type**, register as **Generic Service**.
- Set **Name**, **Service name**, and **Resource Dependencies** as shown in Table *5-2 PFM - RM for Platform services to be registered into the cluster software*.
- Do not set **Start parameters** or **Registry Replication**.
- On the **Advanced** page in **Properties**, specify the settings according to whether you want a failover to occur in the event of a Performance Management program failure.

  For example, the following settings result in failover in the event of a PFM - RM for Platform failure:

  - **Restart**: Selected
  - **Apply to group**: Cleared
  - **Threshold** for the restart retry count: 3#

  #

  As a guideline, set 3 in **Threshold** for the restart retry count.

Note

A service registered in the cluster is started and stopped from the cluster. Therefore, set **Startup type** to **Manual** so that the service will not be started automatically during OS startup. Immediately after the setup is performed by the jpcconf ha setup command, the service is set to **Manual**.

Make sure that you do not use the following command to forcibly stop services:

```
jpcspm stop -key all -lhost logical-host-name -kill immediate
```

(17) Checking start and stop from the cluster software Executing system Standby system

Make sure that the Performance Management programs function normally by starting and terminating the programs from the cluster software at each node.

(18) Setting up an environment in the cluster system Executing system Standby system

After you have finished setting up the Performance Management programs, set up an environment for them so that PFM - Web Console can be used to display the monitoring target's operation status as a report according to the operating procedures and can send notifications to the user in the event of problems at the monitoring target.

For details about how to set up an environment for the Performance Management programs, see the chapter that describes the configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

5.3.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows) in a cluster system

For details about the WMI connection setting method, see *3.1.1(5) Environment settings required for collecting performance data (when both the PFM - RM host and the monitored hosts are running Windows)* and *3.1.5 WMI connection setting method (when both the PFM - RM host and the monitored host are running Windows)*.

5.3.6 SSH connection setting method in a cluster system (when the PFM - RM host is running Windows and the monitored host is running UNIX) (for Windows)

For details about the SSH connection setting method, see *3.1.1(6) Environment settings required for collecting performance data (when the PFM - RM host is running Windows and the monitored hosts are running UNIX)* and *3.1.6 SSH connection setting method for Windows (when the PFM - RM host is running Windows and the monitored host is running UNIX)*.

5.4 Installation and setup in a cluster system (for UNIX)

This section describes the procedures for installing and setting up PFM - RM for Platform in a cluster system.

For details about how to install and set up PFM - Manager, see the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

5.4.1 Items to be checked before installing in a cluster system (for UNIX)

This subsection describes items to be checked before you start installation of PFM - RM for Platform.

(1) Prerequisites

Following are the prerequisites for using PFM - RM for Platform in a cluster system.

(a) Cluster system

Make sure that the following conditions are satisfied:

- The cluster system is controlled by cluster software.
- The cluster software is set up in such a manner that it controls startup and termination of the PFM - RM for Platform that is running on the logical host.

(b) Shared disk

Make sure that the following conditions are satisfied:

- A shared disk is available to each logical host and information can be inherited from the executing node to the standby node.
- The shared disk is connected to each node physically by Fibre Channel or SCSI.[#1]
- The shared disk can be placed offline forcibly by means such as the cluster software in order to implement failover even when there is still an active process that is using the shared disk.
- If multiple PFM products are running on the same logical host, the shared disk uses the same directory names.[#2]

#1

Performance Management does not support a configuration that uses a network drive or a disk replicated via the network as the shared disk.

#2

You can change the storage location of the Store database and store it in a different directory on the shared disk.

(c) Logical host names and logical IP addresses

Make sure that the following conditions are satisfied:

- Each logical host has a logical host name and a corresponding logical IP address, and that this information can be inherited from the executing node to the standby node.
- The logical host names and logical IP addresses are set in the `hosts` file and name server.
- If DNS operation is employed, the host name without the domain name is used as the logical host name, not the FQDN name.

- All physical and logical host names are unique within the system.

Important note

- Do not specify a physical host name (host name displayed by the `uname -n` command) as a logical host name. If you do so, normal communication processing might not occur.
- A logical host name is expressed as 1 to 32 bytes of alphanumeric characters. None of the following symbols nor the space character can be used:
  `/ \ : ; * ? ' " < > | & = , .`
- A logical host name cannot begin with `localhost`, an IP address, or the hyphen (`-`).

(d) Settings for using IPv6

Performance Management supports both IPv4 and IPv6 network environments. Therefore, you can run Performance Management even in a network environment where IPv4 and IPv6 coexist.

PFM - RM for Platform can use IPv6 to communicate with PFM - Manager. However, this applies only when the OS of the hosts on which PFM - RM for Platform and PFM - Manager are installed are Windows Server 2008 R2, Windows Server 2012, or Linux. For details about the applicable scope of communication in the IPv4 and IPv6 environments, see *L. Communication in IPv4 and IPv6 Environments*.

To communicate in IPv6, you must enable the use of IPv6 on both the PFM - Manager host and the PFM - RM host. You specify this setting by executing the `jpcconf ipv6 enable` command. The following explains the conditions to use for determining whether you need to execute this command.

Cases in which you need to execute the `jpcconf ipv6 enable` command:

- When all hosts are being changed from an IPv4 environment to an IPv6 environment
- In an environment where IPv4 and IPv6 coexist and PFM - Manager is being changed from an IPv4 environment to an IPv6 environment

Cases in which you do not need to execute the `jpcconf ipv6 enable` command:

- When all hosts are already in an IPv6 environment
- In an environment where IPv4 and IPv6 coexist and PFM - Manager is already in an IPv6 environment

An example of executing the `jpcconf ipv6 enable` command follows:

```
jpcconf ipv6 enable
```

Execute the `jpcconf ipv6 enable` command separately on the executing node and the standby node.

For details about the `jpcconf ipv6 enable` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*. For details about the conditions and timing for executing the `jpcconf ipv6 enable` command, see the chapter that describes an example of a network configuration that includes an IPv6 environment in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

When PFM - RM for Platform will use IPv6 to communicate with monitored hosts, specify a monitored host name that can be resolved.

PFM - RM for Platform uses a resolvable IP address to communicate with a monitoring target. When PFM - RM for Platform communicates with a monitoring target in an environment where IPv4 and IPv6 coexist, PFM - RM for Platform will not try to communicate using another IP address if communication using a resolvable IP address fails.

For example, if a connection attempt using IPv4 fails, PFM - RM for Platform will not retry using IPv6. Conversely, if a connection attempt using IPv6 fails, PFM - RM for Platform will not retry using IPv4. Therefore, make sure beforehand that connection can be established.

(e) SSH connection

Make sure that the following conditions are satisfied:

- A private key on the same path is available in the environments for both the executing node and the standby node.
- That private key can be used to connect to the monitored hosts.

Note:

If you use the private key that is automatically generated when PFM - RM for Platform is installed, use one of the following methods to register the private and public keys:

- Copy the private key created at the executing server to the standby server, and then establish its correspondence with the public key that is distributed from the executing server to the monitored host.
- Create public keys at both executing and standby servers, and then establish correspondence between them by registering both public keys at the monitored hosts.

For details about the SSH connection settings, see *3.2.5 SSH (for UNIX) connection setting method*.

(2) Information needed for setting up PFM - RM for Platform for logical host operation

If you run PFM - RM for Platform on a logical host, you need the information listed in the table below in addition to the environment information that is needed for setting up a normal PFM - RM for Platform.

Table 5–3: Information needed for setting up PFM - RM for Platform for logical host operation

No.	Item	Example
1	Logical host name	`jp1-halrmp`
2	Logical IP address	`172.16.92.100`
3	Shared disk	`/jp1`

If multiple Performance Management programs are running on the same logical host, all of them must use directories on the same shared disk

For details about the space requirements on the shared disk, see *A. Estimating System Requirements*.

(3) Notes about logical host failover

If you employ a system configuration in which PFM - RM for Platform runs on a logical host, evaluate whether the entire logical host should failover in the event of a PFM - RM for Platform failure.

If a PFM - RM for Platform failure is to result in failover of the entire logical host, any other job application that is running on the logical host will also result in failover, which might affect the job adversely.

Typically, we recommend that you use one of the following cluster software settings so that errors on PFM - RM for Platform do not affect the operation of other applications:

- Operation of PFM - RM for Platform is not monitored.
- Detection of PFM - RM for Platform errors does not result in failover.

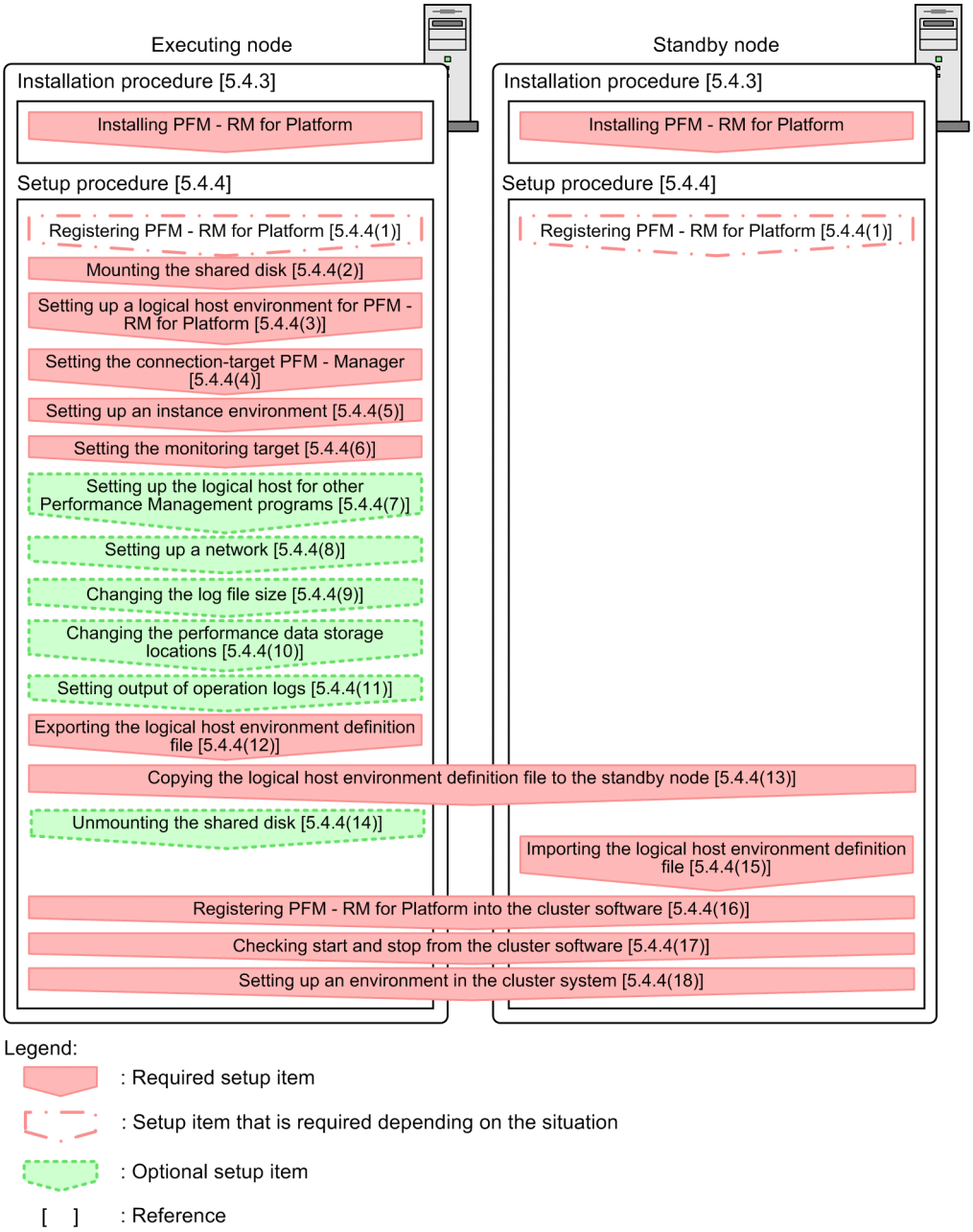
(4) Notes about upgrading when logical operation is used

To upgrade a PFM - RM for Platform that is running on a logical host, you must mount the shared disk at either the executing node or the standby node.

5.4.2 Flow of installation and setup in a cluster system (for UNIX)

The following figure shows the procedures for installing and setting up PFM - RM for Platform in a cluster system.

Figure 5–6: Installation and setup procedures in a cluster system (for UNIX)



Note:

Setting up a PFM - RM in a logical host environment does not inherit the existing PFM - RM definition in the physical host environment. A new environment is created when an instance environment is set up in the logical and physical host environments.

For setup commands that require a user input, you can select whether to execute the commands in the interactive or non-interactive mode.

When a command is executed in the interactive mode, the user must enter a value in response to the instruction from the command.

When a command is executed in the non-interactive mode, no user input is required because option specification or a definition file replaces the input step required during interactive command execution. Furthermore, batch processing or remote execution can automate the setup procedure, thereby reducing the workload on the administrator and the operating cost. Commands in the non-interactive mode are convenient in the following cases:

- You want to change the password used for connecting to monitoring targets on a regular basis.
- You want to improve the efficiency of the procedure for adding multiple monitoring targets.

For details about commands, see the manual *Job Management Partner 1/Performance Management Reference*.

5.4.3 Installation procedure in a cluster system (for UNIX)

Install PFM - Base and PFM - RM for Platform on both the executing node and the standby node.

The installation procedure is the same as for non-cluster systems. For details about the installation procedure, see *3.2.3 Installation procedure for the UNIX edition*.

5.4.4 Setup procedure in a cluster system (for UNIX)

This subsection describes the setup needed for running Performance Management in a cluster system.

To run Performance Management in a cluster system, you must set up both the executing node and the standby node. Set up the executing node first, and then set up the standby node.

Executing system indicates an item that is to be executed at the executing node, and Standby system indicates an item that is to be executed at the standby node. Optional indicates the following setup items:

- Setup item that is required depending on the environment in use
- Setup item for changing the default settings

> **Important note**
>
> Do not set `JPC_HOSTNAME` as an environment variable because it is used by Performance Management. If it is set as an environment variable by mistake, Performance Management will not function correctly.

(1) Registering PFM - RM for Platform Executing system Standby system Optional

To achieve central management of PFM - RM for Platform in the Performance Management system, you must register PFM - RM for Platform into PFM - Manager and PFM - Web Console.

You must register PFM - RM for Platform at the following times:

- When you add a new PFM - RM for Platform in the Performance Management system.
- When you update the Data model version for the registered PFM - RM for Platform.

You use PFM - Manager and PFM - Web Console to register PFM - RM for Platform. The registration procedure is the same as when a cluster system is not used. For details about the procedure, see *3.2.4(2) Registering PFM - RM for Platform*.

(2) Mounting the shared disk Executing system

Make sure that the shared disk is mounted.

If the shared disk is not mounted, use a program such as the cluster software or a volume manager to mount it.

(3) Setting up a logical host environment for PFM - RM for Platform Executing system

Execute the `jpcconf ha setup` command to create a logical host environment. This command creates a logical host environment by copying necessary data to the shared disk and setting definitions for a logical host.

Note

Before you execute the command, stop all Performance Management programs and services in the entire Performance Management system. For details about how to stop services, see the chapter that describes the startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

To set up a logical host environment for PFM - RM for Platform:

1. Execute the `jpcconf ha setup` command to create a logical host environment for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf ha setup -key RMPlatform -lhost jp1-halrmp -d /jp1
   ```

   Use the `-lhost` option to specify the logical host name. This example specifies `jp1-halrmp` as the logical host name. If you employ DNS operations, specify the logical host name without the domain name.

   Specify in the `-d` option a directory name on the shared disk within the environment directory. For example, if `-d /jp1` is specified, `/jp1/jp1pc` is created, and then files for the logical host environment are created.

2. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

   ```
   jpcconf ha list -key all
   ```

   Make sure that the created logical host environment is correct.

(4) Setting the connection-target PFM - Manager Executing system

Execute the `jpcconf mgrhost define` command to set the PFM - Manager that manages PFM - RM for Platform.

To set the connection-target PFM - Manager:

1. Execute the `jpcconf mgrhost define` command to set the connection-target PFM - Manager.

   Execute the following command:

   ```
   jpcconf mgrhost define -host jp1-hal -lhost jp1-halrmp
   ```

   Specify in the `-host` option the host name of the connection-target PFM - Manager. If the connection-target PFM - Manager is to run on a logical host, specify in the `-host` option the logical host name of the connection-target PFM - Manager. This example specifies `jp1-hal` as the PFM - Manager's logical host name.

   Use the `-lhost` option to specify the logical host name of PFM - RM for Platform. This example specifies `jp1-halrmp` as the logical host name of PFM - RM for Platform.

   The example above shows execution in the interactive mode, but you can also execute the `jpcconf mgrhost define` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(5) Setting up an instance environment Executing system

Execute the `jpcconf inst setup` command to set up an instance environment for PFM - RM for Platform.

The setup procedure is the same as when a cluster system is not employed. However, in the case of a cluster system, you must specify the logical host name in the `-lhost` option when you execute the `jpcconf inst setup` command.

The following shows how to specify the `jpcconf inst setup` command for a cluster system:

```
jpcconf inst setup -key RMPlatform -lhost logical-host-name -inst instance-
name
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf inst setup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

For details about the settings and procedure, see *3.2.4(3) Setting up an instance environment*.

(6) Setting the monitoring target Executing system

Execute the `jpcconf target setup` command to set information about the monitored host for PFM - RM for Platform.

The setting procedure is the same as when a cluster system is not employed.

However, in the case of a cluster system, you must specify the logical host name in the `-lhost` option when you execute the `jpcconf target setup` command.

The following shows how to specify the `jpcconf target setup` command for a cluster system:

```
jpcconf target setup -key RMPlatform -lhost logical-host-name -inst
instance-name -target monitoring-target-name
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf target setup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

For details about the settings and procedure, see *3.2.4(4) Setting the monitored host*.

(7) Setting up the logical host for other Performance Management programs Executing system Optional

If you have other PFM - Manager, PFM - Agent, or PFM - RM programs to be set up on the same logical host in addition to PFM - RM for Platform, set them up at this stage.

For details about the setup procedure, see the chapter that describes the configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

(8) Setting up a network Executing system Optional

You specify network settings if you need to change the network environment settings as appropriate to the network configuration where Performance Management is used.

The two network environment settings are described below. Change these settings if necessary.

- Setting IP addresses

  Set this information to use Performance Management in a network that is connected to multiple LANs. To specify an IP address to be used, directly edit the contents of the `jpchosts` file.

  Copy the edited `jpchosts` file from the executing node to the standby node under *physical-host-installation-directory*`/jp1pc/`.

  For details about how to set IP addresses, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Setting port numbers

  If you establish communication between Performance Management programs via a firewall, use the `jpcconf port define` command to set the port numbers.

  For details about how to set port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

(9) Changing the log file size Executing system Optional

The operation status of Performance Management is output to a log file unique to Performance Management. This log file is called the *common message log*. The common message log consists of two files with a default size of 2,048 kilobytes each. If necessary, use this setting to change this file size.

For details, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(10) Changing the performance data storage locations Executing system Optional

This setting is used to change the storage locations, backup directory, export directory, or import directory for the performance data that is managed by PFM - RM for Platform

For details about the setting method, see *3.6.1 Changing performance data storage locations*.

(11) Action log output setting Executing system Optional

This setting is required in order to output action logs in the event of an alarm.

An action log consists of log information about exceeded threshold values caused by factors such as system loading; its output is linked with the alarm function. For details about the setting method, see *I. Outputting Action Log Data*.

(12) Exporting the logical host environment definition file Executing system

After you have created a logical host environment for PFM - RM for Platform, export the environment definition to a file.

This export process involves output of the definition information for the Performance Management program that has been set up on the logical host to a file in the batch mode. If you are setting up other Performance Management programs on the same logical host, export the environment definition after all the setup processes are completed.

To export the logical host environment definition:

1. Execute the `jpcconf ha export` command to export the logical host environment definition.

Output the definition information for the logical host environment that has been created so far to an export file. You can assign any name to the export file.

For example, to export the logical host environment definition to the `lhostexp.txt` file, execute the following command:

```
jpcconf ha export -f lhostexp.txt
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf ha export` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(13) Copying the logical host environment definition file to the standby node Executing system Standby system

Copy from the executing node to the standby node the logical host environment definition file exported in *(12) Exporting the logical host environment definition file*.

(14) Unmounting the shared disk Executing system Optional

Unmount the file system and finish the procedure.

If you will be using the shared disk after you complete this procedure, there is no need to unmount the file system.

Note

If the shared disk is unmounted but the specified environment directory contains the `jp1pc` directory and that directory has files under it, the setup is performed without unmounting the shared disk.

In such a case, perform the following procedure:

1. Use the `tar` command to archive the `jp1pc` directory that is located in the specified environment directory 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 all files and directories under the `jp1pc` directory that is located in the specified environment directory on the local disk.

(15) Importing the logical host environment definition file Standby system

Import to the standby node the export file that was copied from the executing node.

Use the `jpcconf ha import` command to specify settings for executing at the standby node the Performance Management program on the logical host that was created at the executing node. If multiple Performance Management programs have been set up on the same logical host, the settings for all the programs are imported in the batch mode.

When you execute this command, there is no need to keep the shared disk mounted.

To import the logical host environment definition file:

1. Execute the `jpcconf ha import` command to import the logical host environment definition.

   Execute the following command:

```
jpcconf ha import -f lhostexp.txt
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf ha import` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

This command changes settings in such a manner that the environment for the standby node becomes the same as for the export file. As a result, the setup for starting PFM - RM for Platform on the logical host is performed.

If a fixed port number has been set by the `jpcconf port define` command during the setup, it is also set in the same manner.

2. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

```
jpcconf ha list -key all
```

   Make sure that the displayed information is the same as when the `jpcconf ha list` command is executed at the executing node

(16) Registering PFM - RM for Platform into the cluster software Executing system Standby system

To run a Performance Management program in a logical host environment, you must register the program into the cluster software and set up the environment in such a manner that the Performance Management program is started and terminated from the cluster software.

For details about how to register PFM - RM for Platform into the cluster software, see the cluster software documentation.

This subsection describes the settings for registering PFM - RM for Platform into the cluster software.

When applications are registered into the UNIX cluster software, the following four items are typically required: *Start*, *Stop*, *Operation monitoring*, and *Forced stop*.

The following table shows how to set these items in PFM - RM for Platform.

Table 5–4: How to control a PFM - RM for Platform that is registered into the cluster software

No.	Item	Description
1	Start	Execute the following commands in the order shown to start PFM - RM for Platform: 1. `jpcspm start -key AH -lhost` *logical-host-name* 2. `jpcspm start -key RMPlatform -lhost` *logical-host-name* `-inst` *instance-name* The time to do this is after the shared disk and logical IP address become available.
2	Stop	Execute the following commands in the order shown to terminate PFM - RM for Platform: 1. `jpcspm stop -key RMPlatform -lhost` *logical-host-name* `-inst` *instance-name* 2. `jpcspm stop -key AH -lhost` *logical-host-name* The time to do this is before the shared disk and logical IP address become unavailable. If the service has stopped for a reason such as a failure, the `jpcspm stop` command returns a value of `3`. In such a case, the processing is treated as a normal termination because the service has stopped. If the cluster software uses the return value to determine the execution result, take appropriate action, such as setting the return value to `0`.
3	Operation monitoring	Execute the `ps` command to check whether the indicated process is running: • `ps -ef | grep "`*process-name logical-host-name*`" | grep -v "grep` *monitoring-target-process*`"`

No.	Item	Description
3	Operation monitoring	The monitoring-target processes are as follows: • `jpcagt7`, `agt7/jpcsto`, `jpcah` For process names, see the chapter that describes planning and operation in a cluster system in the *Job Management Partner 1/Performance Management User's Guide*. Note that a process might have been stopped temporarily during Performance Management operation for a reason such as the need to perform system maintenance. To prepare for this, we recommend that you provide a method for suppressing operation monitoring (for example, monitoring is not to be performed when the system detects a file that indicates that system maintenance is underway).
4	Forced stop	If forced termination is necessary, execute the following command: • `jpcspm stop -key all -lhost` *logical-host-name* `-kill immediate` You can specify only `all` as the service key in the `-key` option. **Note** If you execute this command, all Performance Management processes in the specified logical host environment are terminated forcibly by `SIGKILL` transmission. In this case, the Performance Management processes are terminated forcibly in units of logical hosts, not services. Specify the settings so that forced termination is used only when processes cannot be terminated by normal termination.

Notes:

- The Performance Management programs registered in the cluster are started and terminated by the cluster. Therefore, do not set automatic startup at the time of OS startup.
- If you execute Performance Management programs in a Japanese language environment, use the script registered in the cluster software to set up the `LANG` environment variable before executing Performance Management commands.
- If the cluster software uses the return value of a command to determine the execution result, specify the settings so that the return value of the Performance Management commands is converted to a value that can be handled by the cluster software. For details about the return values of Performance Management commands, see each command reference.
- The length of the text that can be displayed by the `ps` command depends on the OS. Set the text so that the total length of the logical host name and the instance name does not exceed 47 characters. If you use the `ps` command to monitor operations, make sure in advance that all logical hosts can be displayed by the `ps` command. Specify the settings so that if the displayed text is not complete, monitoring will apply based on the displayed characters. When you use the `ps` command to identify a specific process name and a logical host name, the command might fail to acquire a process name or a logical host name. If this occurs, the text might be displayed inside square brackets (`[]`). Check the reference for the `ps` command for your OS, and then re-execute the command.
- Start the monitored host first, and then start PFM - RM for Platform. During termination, terminate PFM - RM for Platform first, and then terminate the monitored host.

(17) Checking start and stop from the cluster software Executing system Standby system

Make sure that the Performance Management programs function normally by starting and terminating the programs from the cluster software at each node.

(18) Setting up an environment in the cluster system Executing system Standby system

After you have finished setting up the Performance Management programs, set up an environment for them so that PFM - Web Console can be used to display the monitoring target's operation status as a report according to the operating procedures and can send notifications to the user in the event of problems at the monitoring target.

For details about how to set up an environment for the Performance Management programs, see the chapter that describes the configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

5.4.5 SSH connection setting method in a cluster system (for UNIX)

For details about how to set SSH connection, see *3.2.1(5) Environment settings required for collecting performance data (for UNIX)* and *3.2.5 SSH (for UNIX) connection setting method*.

5.5 Uninstallation and unsetup in a cluster system (for Windows)

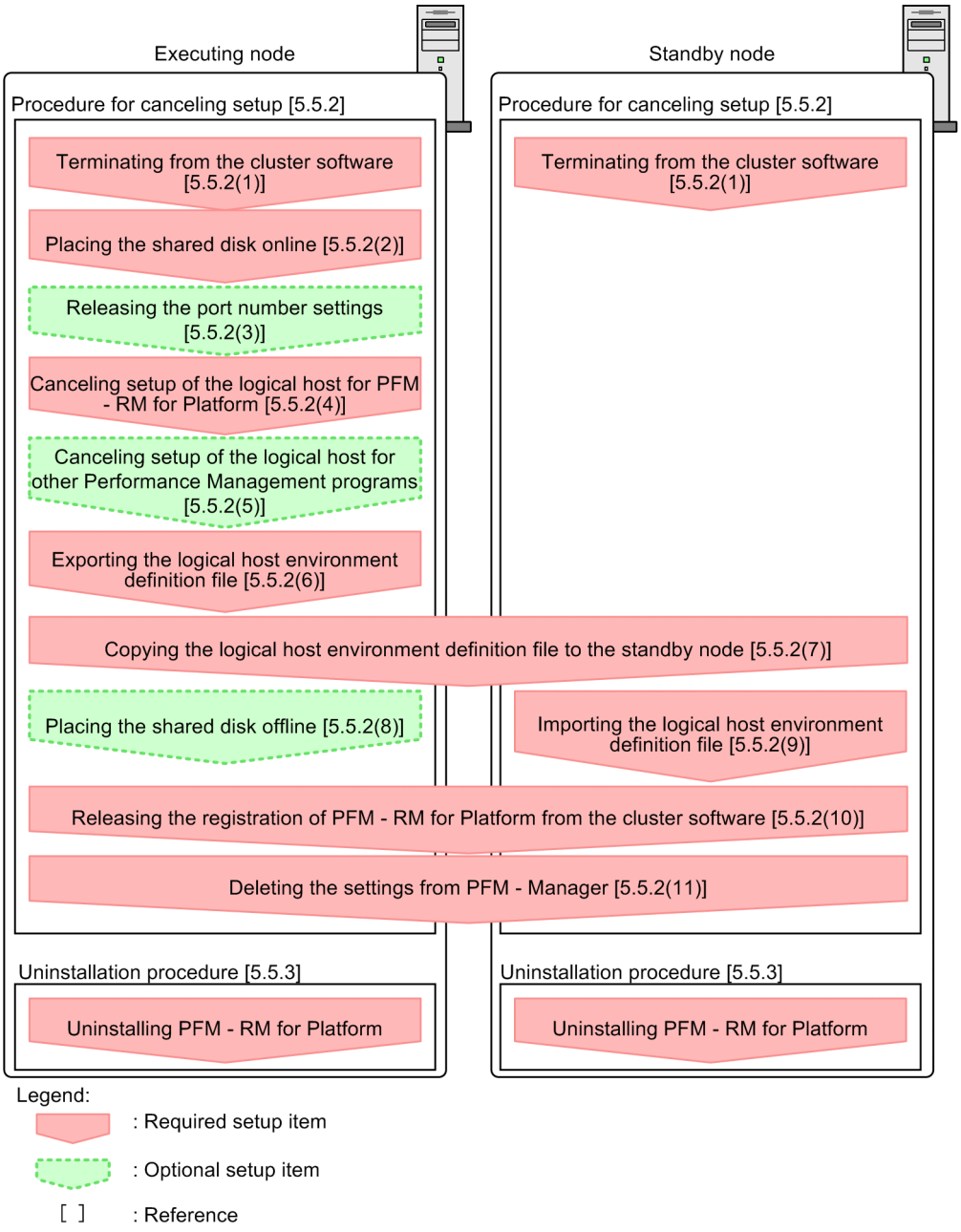
This section describes the procedures for uninstalling and canceling the setup of a PFM - RM for Platform that is running in a cluster system.

For details about uninstalling and canceling the setup of PFM - Manager, see the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

5.5.1 Flow of uninstallation and unsetup in a cluster system (for Windows)

The following figure shows the procedure for uninstalling and canceling the setup of a PFM - RM for Platform that is running in a cluster system.

Figure 5–7: Procedure for uninstalling and canceling the setup of a PFM - RM for Platform in a cluster system (for Windows)



5.5.2 Unsetup procedure in a cluster system (for Windows)

Cancel the setup of the logical host environment.

This procedure must be performed at both the executing node and the standby node. Cancel the setup at the executing node first, and then at the standby node.

Note that Executing system indicates the items to be executed at the executing node, Standby system indicates the items to be executed at the standby node, and Optional indicates the following setup items:

- Setup items that are required depending on the environment in use

- Setup items for changing the default settings

The following subsections describe how to cancel the setup of PFM - RM for Platform.

(1) Terminating from the cluster software Executing system Standby system

Use the cluster software to stop the Performance Management programs and services that are running at the executing and standby nodes.

For details about how to stop programs and services, see the cluster software documentation.

(2) Placing the shared disk online Executing system

Make sure that the shared disk is online.

If the shared disk is not in online status, use a program such as the cluster software or a volume manager to place it online.

(3) Releasing the port number settings Executing system Optional

This procedure is required only when the `jpcconf port define` command was used to set port numbers during setup in an environment that uses a firewall.

For details about how to release port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

(4) Canceling setup of the logical host for PFM - RM for Platform Executing system

This subsection describes how to cancel the setup of the logical host.

If a logical host environment is deleted while the shared disk is in offline status, the logical host settings are deleted from the physical host, but the folders and files are not deleted from the shared disk. In such a case, you must place the shared disk online and manually delete the `jp1pc` folder under the environment folder.

To cancel the setup of the logical host for PFM - RM for Platform:

1. Execute the `jpcconf ha list` command to check the logical host settings.
   Execute the following command:

   ```
   jpcconf ha list -key all-lhost logical-host-name
   ```

   You must check the current settings before you cancel the setup of the logical host environment. Check such information as the name of the logical host and the path to the shared disk.

2. Execute the `jpcconf target unsetup` command to delete information about the monitoring host for PFM - RM for Platform.
   Execute the following command:

   ```
   jpcconf target unsetup -key RMPlatform -lhost logical-host-name -inst
   instance-name -target monitoring-target-name
   ```

   The `jpcconf target unsetup` command excludes the specified monitored host on the logical host as a monitoring target.

3. Execute the `jpcconf inst unsetup` command to delete the instance environment for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf inst unsetup -key RMPlatform -lhost logical-host-name -inst
   instance-name
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf inst unsetup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

   The `jpcconf inst unsetup` command deletes the settings for starting the instance of the logical host. It also deletes files for the instance from the shared disk.

4. Execute the `jpcconf ha unsetup` command to delete the logical host environment for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf ha unsetup -key RMPlatform -lhost logical-host-name
   ```

   The `jpcconf ha unsetup` command deletes the settings for starting PFM - RM for Platform on the logical host. It also deletes files for the logical host from the shared disk.

5. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

   ```
   jpcconf ha list -key all
   ```

   Make sure that PFM - RM for Platform has been deleted from the logical host environment.

(5) Canceling setup of the logical host for other Performance Management programs Executing system Optional

If you are also canceling from the same logical host the setup of Performance Management programs other than PFM - RM for Platform, do so at this stage.

For details about the procedure for canceling the setup, see the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*. Also see the chapter that describes cluster system operation in each PFM - RM manual or PFM - Agent manual.

(6) Exporting the logical host environment definition file Executing system

After you have deleted the logical host environment for PFM - RM for Platform, export the environment definition to a file.

Performance Management achieves a matching environment in the executing and standby nodes by importing and exporting environment definitions. When the environment definition exported from the executing node (definition from which the Performance Management definition has been deleted) is imported to the standby node, the system compares it with the environment definition existing in the standby node (definition that still contains the Performance Management definition) to determine the differences (the portion deleted at the executing node), and then deletes the Performance Management environment definition.

To export the logical host environment definition file:

1. Execute the `jpcconf ha export` command to export the logical host environment definition.

Output the logical host environment definition information for Performance Management to an export file. You can assign any name to the export file. For example, to export the logical host environment definition to the `lhostexp.txt` file, execute the following command:

```
jpcconf ha export -f lhostexp.txt
```

This example shows execution in the interactive mode, but you can also execute the `jpcconf ha export` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(7) Copying the logical host environment definition file to the standby node Executing system Standby system

Copy from the executing node to the standby node the logical host environment definition file that was exported in *(6) Exporting the logical host environment definition file*.

(8) Placing the shared disk offline Executing system Optional

Use a program such as the cluster software or a volume manager to place the shared disk in offline status and finish the procedure.

If you will be using the shared disk after this procedure is completed, there is no need to place it in offline status.

(9) Importing the logical host environment definition file Standby system

Import to the standby node the export file that was copied from the executing node. At the standby node, there is no need to place the shared disk in offline status during the import processing.

To import the logical host environment definition file:

1. Execute the `jpcconf ha import` command to import the logical host environment definition.

   Execute the following command:

   ```
   jpcconf ha import -f lhostexp.txt
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf ha import` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

   This command changes settings in such a manner that the environment for the standby node becomes the same as for the export file. As a result, the settings for starting PFM - RM for Platform on the logical host are deleted. If you have canceled the setup of other Performance Management programs on the logical host, those settings are also deleted. If a fixed port number was set by the `jpcconf port define` command during the setup, it is also released.

2. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

   ```
   jpcconf ha list -key all
   ```

   Make sure that the displayed information is the same as when the `jpcconf ha list` command is executed at the executing node.

(10) Releasing the registration of PFM - RM for Platform from the cluster software Executing system Standby system

From the cluster software, delete the settings related to PFM - RM for Platform on the logical host.

For details about how to delete the settings, see the cluster software documentation.

(11) Deleting the settings from PFM - Manager Executing system Standby system

From PFM - Web Console, log in to PFM - Manager and delete the settings related to the PFM - RM for Platform that you want to unsetup.

To delete the settings from PFM - Manager:

1. From PFM - Web Console, delete the agent.
2. Delete the agent information from PFM - Manager.
   For example, if PFM - Manager is running on logical host `jp1-hal` and PFM - RM for Platform is running on logical host `jp1-halrmp`, execute the following command:
   ```
   jpcconf ha list -key all\tools\jpctool service delete -id service-ID -
   host jp1-halrmp -lhost jp1-hal
   ```
   In *service-ID*, specify the service ID of the agent that is to be deleted.
3. Restart the PFM - Manager service.
   For details about how to start services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.
4. Apply the service information of PFM - Manager host.
   To apply the deletion of the service information to the PFM - Web Console host, synchronize the agent information between the PFM - Manager host and the PFM - Web Console host. To synchronize the agent information, use the `jpctool service sync` command.

5.5.3 Uninstallation procedure in a cluster system (for Windows)

Uninstall PFM - RM for Platform from both the executing node and the standby node.

The uninstallation procedure is the same as when a cluster system is not employed. For details about the procedure, see *3.3.3 Procedure for uninstalling the Windows edition*.

Notes

- Before you uninstall PFM - RM for Platform, stop all Performance Management programs and services at the node where PFM - RM for Platform is to be uninstalled.
- If you uninstall PFM - RM for Platform without deleting the logical host environment, the environment folders might remain. In such a case, manually delete the environment folders.

5.6 Uninstallation and unsetup in a cluster system (for UNIX)

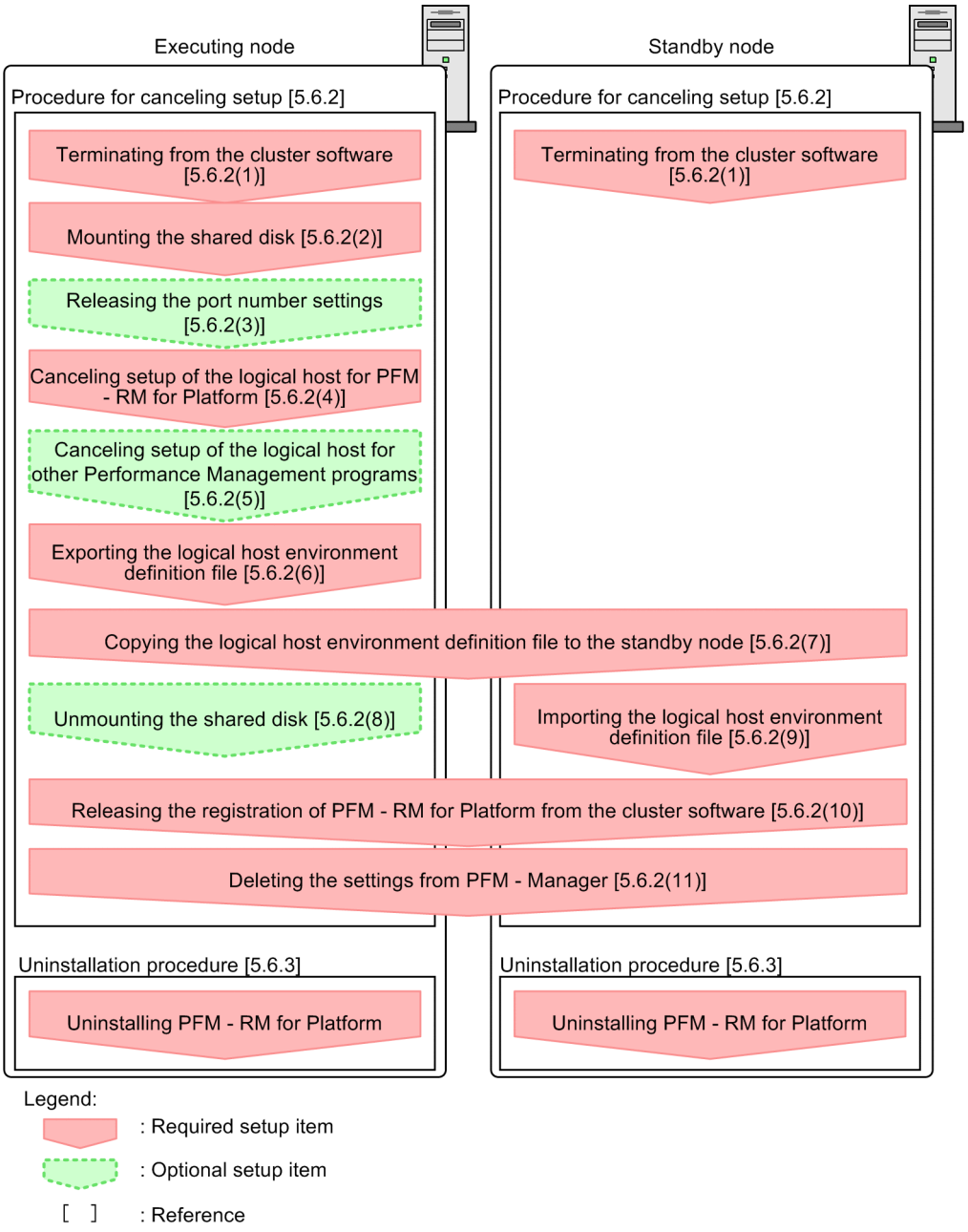
This section describes the procedures for uninstalling and canceling the setup of a PFM - RM for Platform that is running in a cluster system.

For details about uninstalling and canceling the setup of PFM - Manager, see the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

5.6.1 Flow of uninstallation and unsetup in a cluster system (for UNIX)

The following figure shows the procedure for uninstalling and canceling the setup of a PFM - RM for Platform that is running in a cluster system.

Figure 5–8: Procedure for uninstalling and canceling the setup of a PFM - RM for Platform in a cluster system (for UNIX)



5.6.2 Unsetup procedure in a cluster system (for UNIX)

Cancel the setup of the logical host environment.

This procedure must be performed at both the executing node and the standby node. Cancel the setup at the executing node first, and then at the standby node.

Note that Executing system indicates the items to be executed at the executing node, Standby system indicates the items to be executed at the standby node, and Optional indicates the following setup items:

- Setup items that are required depending on the environment in use

- Setup items for changing the default settings

The following subsections describe how to cancel the setup of PFM - RM for Platform.

(1) Terminating from the cluster software Executing system Standby system

Use the cluster software to stop the Performance Management programs and services that are running at the executing and standby nodes.

For details about how to stop programs and services, see the cluster software documentation.

(2) Mounting the shared disk Executing system

Make sure that the shared disk is mounted.

If the shared disk is not mounted, use a program such as the cluster software or a volume manager to mount it.

Note

If the shared disk is unmounted but the environment directory on the logical host whose setup is to be canceled contains the `jp1pc` directory and there are files under the `jp1pc` directory, the setup cancellation is performed without unmounting the shared disk. In this case, perform the following procedure:

1. Use the `tar` command to archive the `jp1pc` directory that is located in the environment directory on the logical host whose setup is to be canceled on the local disk.
2. Mount the shared disk.
3. If the environment directory on the logical host whose setup is to be canceled does not exist on the shared disk, create an environment directory.
4. Expand the `tar` file in the environment directory on the logical host whose setup is to be canceled on the shared disk.
5. Unmount the shared disk.
6. Delete all files and directories under the `jp1pc` directory that is located in the environment directory on the logical host whose setup is to be canceled on the local disk.

(3) Releasing the port number settings Executing system Optional

This procedure is required only if the `jpcconf port define` command was used to set port numbers during setup in an environment that uses a firewall.

For details about how to release port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*.

(4) Canceling setup of the logical host for PFM - RM for Platform Executing system

This subsection describes how to cancel the setup of the logical host.

If a logical host environment is deleted while the shared disk is in offline status, the logical host settings are deleted from the physical host, but the directories and files are not deleted from the shared disk. In such a case, you must place the shared disk online and manually delete the `jp1pc` directory under the environment directory.

To cancel the setup of the logical host for PFM - RM for Platform:

1. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

   ```
   jpcconf ha list -key all -lhost logical-host-name
   ```

   You must check the current settings before you cancel the setup of the logical host environment. Check such information as the name of the logical host and the path to the shared disk.

2. Execute the `jpcconf target unsetup` command to delete information about the monitoring host for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf target unsetup -key RMPlatform -lhost logical-host-name -inst
   instance-name -target monitoring-target-name
   ```

   The `jpcconf target unsetup` command excludes the specified monitored host on the logical host as a monitoring target.

3. Execute the `jpcconf inst unsetup` command to delete the instance environment for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf inst unsetup -key RMPlatform -lhost logical-host-name -inst
   instance-name
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf inst unsetup` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

   The `jpcconf inst unsetup` command deletes the settings for starting the instance of the logical host. It also deletes files for the instance from the shared disk.

4. Execute the `jpcconf ha unsetup` command to delete the logical host environment for PFM - RM for Platform.

   Execute the following command:

   ```
   jpcconf ha unsetup -key RMPlatform -lhost logical-host-name
   ```

   The `jpcconf ha unsetup` command deletes the settings for starting PFM - RM for Platform on the logical host. It also deletes files for the logical host from the shared disk.

5. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

   ```
   jpcconf ha list -key all
   ```

   Make sure that PFM - RM for Platform has been deleted from the logical host environment.

(5) Canceling setup of the logical host for other Performance Management programs Executing system Optional

If you are also canceling from the same logical host the setup of Performance Management programs other than PFM - RM for Platform, do so at this stage.

For details about the procedure for canceling the setup, see the chapter that describes configuration and operation of cluster systems in the *Job Management Partner 1/Performance Management User's Guide*. Also see the chapter that describes cluster system operation in each PFM - RM manual or PFM - Agent manual.

(6) Exporting the logical host environment definition file Executing system

After you have deleted the logical host environment for PFM - RM for Platform, export the environment definition to a file.

Performance Management achieves a matching environment in the executing and standby nodes by importing and exporting environment definitions. When the environment definition exported from the executing node (definition from which the Performance Management definition has been deleted) is imported to the standby node, the system compares it with the environment definition existing in the standby node (definition that still contains the Performance Management definition) to determine the differences (the portion deleted at the executing node), and then deletes the Performance Management environment definition.

To export the logical host environment definition file:

1. Execute the `jpcconf ha export` command to export the logical host environment definition.

   Output the logical host environment definition information for Performance Management to an export file. You can assign any name to the export file. For example, to export the logical host environment definition to the `lhostexp.txt` file, execute the following command:

   ```
   jpcconf ha export -f lhostexp.txt
   ```

   This example shows execution in the interactive mode, but you can also execute the `jpcconf ha export` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(7) Copying the logical host environment definition file to the standby node Executing system Standby system

Copy from the executing node to the standby node the logical host environment definition file that was exported in *(6) Exporting the logical host environment definition file*.

(8) Unmounting the shared disk Executing system Optional

Unmount the file system and finish the procedure.

If you will be using the shared disk after this procedure is completed, there is no need to unmount the file system.

(9) Importing the logical host environment definition file Standby system

Import to the standby node the export file that was copied from the executing node. At the standby node, there is no need to unmount the shared disk during the import processing.

To import the logical host environment definition file:

1. Execute the `jpcconf ha import` command to import the logical host environment definition.

   Execute the following command:

   ```
   jpcconf ha import -f lhostexp.txt
   ```

This example shows execution in the interactive mode, but you can also execute the `jpcconf ha import` command in the non-interactive mode. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

This command changes settings in such a manner that the environment for the standby node becomes the same as in the export file. As a result, the settings for starting PFM - RM for Platform on the logical host are deleted. If you have canceled the setup of other Performance Management programs on the logical host, those settings are also deleted. If a fixed port number was set by the `jpcconf port define` command during the setup, it is also released.

2. Execute the `jpcconf ha list` command to check the logical host settings.

   Execute the following command:

   ```
   jpcconf ha list -key all
   ```

   Make sure that the displayed information is the same as when the `jpcconf ha list` command is executed at the executing node.

(10) Releasing the registration of PFM - RM for Platform from the cluster software Executing system Standby system

From the cluster software, delete the settings related to PFM - RM for Platform on the logical host.

For details about how to delete the settings, see the cluster software documentation.

(11) Deleting the settings from PFM - Manager Executing system Standby system

From PFM - Web Console, log in to PFM - Manager and delete the settings related to the PFM - RM for Platform that you want to unsetup.

To delete the settings from PFM - Manager:

1. From PFM - Web Console, delete the agent.

2. Delete the agent information from PFM - Manager.

   For example, if PFM - Manager is running on logical host `jp1-hal` and PFM - RM for Platform is running on logical host `jp1-halrmp`, execute the following command:

   ```
   jpctool service delete -id service-ID -host jp1-halrmp -lhost jp1-hal
   ```

   In *service-ID*, specify the service ID of the agent that is to be deleted.

3. Restart the PFM - Manager service.

   For details about how to start services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

4. Apply the service information of PFM - Manager host.

   To apply the deletion of the service information to the PFM - Web Console host, synchronize the agent information between the PFM - Manager host and the PFM - Web Console host. To synchronize the agent information, use the `jpctool service sync` command.

5.6.3 Uninstallation procedure in a cluster system (for UNIX)

Uninstall PFM - RM for Platform from both the executing node and the standby node.

The uninstallation procedure is the same as when a cluster system is not employed. For details about the procedure, see *3.4.3 Procedure for uninstalling the UNIX edition*.

Notes

- Before you uninstall PFM - RM for Platform, stop all Performance Management programs and services at the node where PFM - RM for Platform is to be uninstalled.
- If you uninstall PFM - RM for Platform without deleting the logical host environment, the environment directories might remain. In such a case, manually delete the environment directories.

5.7 Changing the PFM - RM for Platform system configuration

When a change occurs, such as the monitoring target system's network configuration and host names, you must change the system configuration for PFM - RM for Platform.

When you change the system configuration for PFM - RM for Platform, you must also change the settings for PFM - Manager and PFM - Web Console. For details about how to change the system configuration for Performance Management, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. When you rename a logical host, some additions of PFM - Agent require additional tasks. PFM - RM for Platform requires no additional tasks.

5.8 Changing the PFM - RM for Platform operation method in a cluster system

This section describes how to change the PFM - RM for Platform operation method in a cluster system.

For details about how to change the operation method for the entire Performance Management system, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

5.8.1 Updating an instance environment in a cluster system

To update an instance environment in a cluster system, check the logical host name and instance name, and then update each setting for the instance environment. Perform the instance environment setup on the PFM - RM host at the executing node.

Check the information to be updated in advance by referencing *3.6.2 Updating an instance environment*.

Use the `jpcconf ha list` command to check the logical host name and instance name; use the `jpcconf inst setup` command to update the instance environment.

To update multiple instance environments, repeat the procedure described below.

To update an instance environment:

1. Check the logical host name and instance name.

   Execute the `jpcconf ha list` command specifying the service key that indicates the PFM - RM for Platform running in the instance environment that you want to update.

   For example, to check the logical host name and instance name of PFM - RM for Platform, execute the following command:

   `jpcconf ha list -key all`

   If the set logical host name is `jp1-halrmp` and the instance name is `SDC1`, the command displays as follows:

   Output example:

   ```
   Logical Host Name   Key          Environment Directory   [Instance Name]
   ------------------  ------------ ----------------------  ----------------
   jp1-halrmp          RMPlatform   path-of-logical-host    SDC1
   ```

2. If services of PFM - RM for Platform are running in the instance environment that is to be updated, stop them from the cluster software.

3. If the shared disk was placed offline (or unmounted) in step 2, use a program such as the cluster software or a volume manager to place it online (or mount it).

4. Execute the `jpcconf inst setup` command specifying the service key that indicates PFM - RM for Platform in the instance environment that you want to update.

   For example, to update the instance environment where the logical host name for PFM - RM for Platform is `jp1-halrmp` and the instance name is `SDC1`, execute the following command:

   `jpcconf inst setup -key RMPlatform -lhost jp1-halrmp -inst SDC1`

This example shows execution in the interactive mode, but you can also execute the `jpcconf inst setup` command in the non-interactive mode. For details about how to execute this command in the non-interactive mode, see *3.1.4(2) Setting up an instance environment*.

If you execute the `jpcconf inst setup` command in the non-interactive mode, skip step 5.

5. Update the instance environment for PFM - RM for Platform.

   Enter the instance environment settings for PFM - RM for Platform according to the command's instructions. For details about each instance environment setting for PFM - RM for Platform, see *3.6.2 Updating an instance environment*. The current settings are displayed (note that the value of `RMHost_Password` is not displayed). To not change a displayed value, simply press the return key. When all entries have been completed, the instance environment is updated.

6. Restart the services for the updated instance environment from the cluster software.

   For details about how to start and stop services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

Important note

To change the value of an item that cannot be updated, you must delete the instance environment, and then re-create it.

For details about the commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

5.8.2 Updating a monitoring target in a cluster system

To update a monitoring target in a cluster system, check the monitoring target name, and then update the monitoring target. Perform the monitoring target settings on the PFM - RM host at the executing node.

Check the information to be updated in advance by referencing *3.1.4(3) Setting the monitored host* for Windows and *3.2.4(4) Setting the monitored host* for UNIX.

Use the `jpcconf target list` command to check the monitoring target name; use the `jpcconf target display` command to check the settings for the monitoring target; use the `jpcconf target setup` command to update the monitoring target.

Reference note

When you update the monitoring target, there is no need to stop services of PFM - RM for Platform.

To update multiple monitoring targets, repeat the procedure described below.

To update the monitoring target:

1. Check the name of the monitoring target.

   Execute the `jpcconf target list` command specifying the service key that indicates the PFM - RM for Platform that is monitoring the target to be updated, the logical host name, and the instance name.

   For example, to check the name of the monitoring target for the PFM - RM for Platform whose logical host name is `jp1-halrmp` and instance name is `SDC1`, execute the following command:

`jpcconf target list -key RMPlatform -lhost jp1-halrmp -inst SDC1`

When this command is executed, the following information is displayed:

Output example:

```
Targets:
targethost1
targethost2
Groups:
All
```

2. Check the settings for the monitoring target.

   Execute the `jpcconf target display` command specifying the service key that indicates the PFM - RM for Platform that is monitoring the target to be updated, the logical host name, the instance name, and the monitoring target name.

   For example, to check the settings for the monitoring target whose name is `targethost1`, logical host name is `jp1-halrmp`, and instance name is `SDC1`, execute the following command:

   `jpcconf target display -key RMPlatform -lhost jp1-halrmp -inst SDC1 -target targethost1`

3. If the shared disk is in offline status (or is unmounted), use a program such as the cluster software or a volume manager to place it online (or mount it).

4. Execute the `jpcconf target setup` command specifying the service key that indicates the PFM - RM for Platform that is monitoring the target to be updated, the logical host name, the instance name, and the monitoring target name.

   For example, to update the monitoring target whose name is `targethost1`, logical host name is `jp1-halrmp`, and instance name is `SDC1`, execute the following command:

   `jpcconf target setup -key RMPlatform -lhost jp1-halrmp -inst SDC1 -target targethost1`

   This example shows execution in the interactive mode, but you can also execute the `jpcconf target setup` command in the non-interactive mode. For details about how to execute this command in the non-interactive mode, see *3.1.4(3) Setting the monitored host*.

   If you execute the `jpcconf target setup` command in the non-interactive mode, skip step 5.

5. Update the monitoring target of PFM - RM for Platform.

   Enter the monitoring target information for PFM - RM for Platform according to the command's instructions. For details about the monitoring target information for PFM - RM for Platform, see *3.6.3 Updating a monitoring target*. The current settings are displayed (note that the value of `Password` is not displayed). To not change a displayed value, simply press the return key. When all entries have been completed, the monitoring target is updated.

   Important note

   To change the value of an item that cannot be updated, you must delete the monitoring target information, and then re-create it.

5.8.3 Importing and exporting the logical host environment definition file in a cluster system

Import and export the logical host environment definition file only if you have performed the following operations:

- You changed the node configuration on the logical host when you set up the logical host, instance environment, and monitoring target.

  The following subsections show how to set up a logical host for PFM - RM for Platform:

  - For Windows: See *5.3.4(3) Setting up a logical host environment for PFM - RM for Platform*.
  - For UNIX: See *5.4.4(3) Setting up a logical host environment for PFM - RM for Platform*.

  The following subsections show how to set up an instance environment:

  - For Windows: See *5.3.4(5) Setting up an instance environment*.
  - For UNIX: See *5.4.4(5) Setting up an instance environment*.

  The following subsections show how to set up the monitoring target:

  - For Windows: See *5.3.4(6) Setting the monitoring target*.
  - For UNIX: See *5.4.4(6) Setting the monitoring target*.
- You executed an operation that requires export of the logical host environment definition file when you set up a logical host for other Performance Management programs.

  The following subsections show how to set up the logical host for other Performance Management programs:

  - For Windows: See *5.3.4(7) Setting up the logical host for other Performance Management programs*.
  - For UNIX: See *5.4.4(7) Setting up the logical host for other Performance Management programs*.
- You set port numbers during network setup.

  The following subsections show how to set up a network:

  - For Windows: See *5.3.4(8) Setting up a network*.
  - For UNIX: See *5.4.4(8) Setting up a network*.

The following subsections show how to export and import the logical host environment definition file:

- For Windows: See *5.3.4(12) Exporting the logical host environment definition file* through *5.3.4(15) Importing the logical host environment definition file*.
- For UNIX: See *5.4.4(12) Exporting the logical host environment definition file* through *5.4.4(15) Importing the logical host environment definition file*.

If you have only updated the instance environment and monitoring target, there is no need to import or export the logical host environment definition file.

For details about how to set up an instance environment, see *5.8.1 Updating an instance environment in a cluster system*. For details about how to update the monitoring target, see *5.8.2 Updating a monitoring target in a cluster system*.

6 Monitoring Template

This chapter describes the monitoring template for PFM - RM for Platform.

Overview of the monitoring template

A set of alarms and reports provided by PFM - RM for Platform is called a *monitoring template*. You can define alarms and reports by the following methods:

- Use the alarms and reports defined by PFM - RM for Platform
- Copy and customize the alarms and reports defined by PFM - RM for Platform
- Use a wizard to define new information

Because the necessary information for reports and alarms is predefined in the provided monitoring template, you can use the provided monitoring template as-is, or you can copy the provided template's reports and alarms and customize them as appropriate for your environment. Thus, it is not necessary to use the wizard to create new definitions, which simplifies the preparations for monitoring the operation status of a monitoring target.

This chapter describes the alarm and report settings in the monitoring template that have been defined by PFM - RM for Platform.

For details about how to use the monitoring template, see the chapter that describes report creation for operation analysis or operation monitoring by alarms in the *Job Management Partner 1/Performance Management User's Guide*.

Note:

The threshold value specified in the monitoring template is for reference only. To use the alarm from the monitoring template, you need to copy it and specify a threshold value that is appropriate to your environment and OS.

Format of alarm explanations

This section describes the format used to explain alarms. The alarms are presented in alphabetical order.

Alarm name

Indicates the alarm's name in the monitoring template.

Overview

Provides an overview of the target that can be monitored by the alarm.

Main settings

Explains in tabular format the main settings for this alarm.

This table lists the correspondence between settings on the Properties window of PFM - Web Console and the alarm settings defined in the monitoring template.

To display the Properties window in PFM - Web Console, click the alarm icon on the **Alarms** page, and then click the **Properties** method. For details about the settings for each alarm, check the Properties window.

If the abnormal condition is the same as the warning condition in a conditional expression, the system issues only the abnormal alarm event.

Alarm table

Indicates the alarm table that contains this alarm.

Related reports

Indicates the reports in the monitoring template that are associated with this alarm.

To display these reports in PFM - Web Console, on the **Agents** page, click the agent icon, and then click the icon displayed in the **Display Alarm Status** method.

Alarm table

A table containing one or more alarms is called an *alarm table*. The alarms defined in the monitoring template of PFM - RM for Platform are in alarm table format and are stored in the `RM Platform` folder that is displayed on the **Alarms** page of PFM - Web Console.

The alarm table name is as follows:

- PFM RM Platform Template Alarms 09.10
- PFM RM Platform Template Alarms [APP] 09.10
- PFM RM Platform Template Alarms [PS] 09.10
- PFM RM Platform Template Alarms [SVC] 09.10

Item in square brackets ([]) in an alarm name

Square brackets (`[]`) indicate the monitoring item to which the alarm table corresponds. An alarm table without square brackets (`[]`) is an alarm table that groups other basic alarms.

09.10 at the end of the alarm table name

The numerics (09.10) at the end of the alarm table name indicate the alarm table's version number.

When you use alarms defined in the monitoring template, check the version of the alarm table used in the Performance Management system for version compatibility. For details about the alarm table version and version compatibility, see *H. Version Compatibility*.

The following table lists (in alphabetical order) and describes the alarms defined in the monitoring template of PFM - RM for Platform.

Table 6–1: List of alarms

Alarm table name	Alarm name	Monitoring target	Purpose
PFM RM Platform Template Alarms 09.10	Available Memory	Size of the unused physical memory area (megabytes)	Monitoring operation status
	CPU Usage	Processor usage rate (%)	Monitoring performance data
	Disk Busy %	Percentage of time the disk was busy (%)	
	Disk Free Size	Size of the unused area on the logical disk (in megabytes)	Monitoring operation status
	Disk Service Time	Device usage (in busy status)	Monitoring performance data
	Disk Space	Ratio of the free area on the logical disk to the total available area (%)	Monitoring operation status
	I/O Wait Time	Percentage of the time all processors in the entire host were in I/O wait status (%)	Monitoring performance data
	Kernel CPU	Percentage of the time all processors in the entire host were running in the kernel mode (%)	
	Network Received	Rate of data received by the network interface (bytes/second)	
	Page Faults	Page fault count	
	Pagescans	Page scan rate	

Alarm table name	Alarm name	Monitoring target	Purpose
PFM RM Platform Template Alarms 09.10	Processor Queue	Number of requests in the processor queue that are ready for execution	Monitoring performance data
	Run Queue	Number of threads in the execution queue	
	Swap Outs	Number of pages that were swapped out	
	Target Host Status	Status of the connection to the monitored host	Monitoring operation status
	Used Swap Mbytes	Size of the memory used in the virtual memory area (in megabytes)	
	User CPU	Percentage of the time all processors in the entire host were running in the user mode (%)	Monitoring performance data
PFM RM Platform Template Alarms [PS] 09.10	Process Existence	Program name	Monitoring operation status
PFM RM Platform Template Alarms [SVC] 09.10	Service Stop	Service name used in the service control manager database and the service status at the time of data collection	
	Service Stop(dsp nm)	Name used by the user interface program to identify a service and the service status at the time of data collection	
PFM RM Platform Template Alarms [APP] 09.10	Application Status	Status of the application being monitored by the Application Summary (`PD_APP2`) record	

PFM - RM for Platform provides in the monitoring template various alarms for monitoring the operation status in order to determine whether the system is running normally, as well as alarms for monitoring performance data in order to determine whether the system is providing adequate services. You can set use of the alarms that are appropriate to your purposes.

Note

Some fields used in alarms might not be supported by the OS of the monitored host. Do not use alarm fields that are not supported.

The following table shows which alarm fields are supported by the monitored host OSs.

Table 6–2: Support status of alarm fields (monitoring template)

Alarm name	OS of the monitored host					When an unsupported alarm is used by the OS
	Windows	HP-UX	Solaris	AIX	Linux	
Available Memory	Y	Y	Y	Y	Y	--
CPU Usage	Y	Y	Y	Y	Y	--
Disk Busy %	Y	Y	Y	Y	Y	--
Disk Free Size	Y	Y	Y	Y	Y	--
Disk Service Time	Y	Y	Y	Y	Y	--
Disk Space	Y	Y	Y	Y	Y	--
I/O Wait Time	N	Y	Y	Y	Y	No alarm event is issued because the field does not match the conditional expression for alarm.
Kernel CPU	Y	Y	Y	Y	Y	--

Alarm name	OS of the monitored host					When an unsupported alarm is used by the OS
	Windows	HP-UX	Solaris	AIX	Linux	
Network Received	Y	N	N	N	N	No alarm event is issued because the field does not match the conditional expression for alarm.
Page Faults	Y	N	Y	Y	N	No alarm event is issued because the field does not match the conditional expression for alarm.
Pagescans	N	Y	N	Y	N	No alarm event is issued because the field does not match the conditional expression for alarm.
Processor Queue	Y	N	N	N	N	No alarm event is issued because the field does not match the conditional expression for alarm.
Run Queue	N	Y	Y	Y	Y	No alarm event is issued because the field does not match the conditional expression for alarm.
Swap Outs	N	Y	Y	N	Y	No alarm event is issued because the field does not match the conditional expression for alarm.
Target Host Status	Y	Y	Y	Y	Y	--
Used Swap Mbytes	Y	Y	Y	Y	Y	--
User CPU	Y	Y	Y	Y	Y	--
Process Existence	Y	Y	Y	Y	Y	--
Service Stop	Y	N	N	N	N	No alarm event is issued because the field does not match the conditional expression for an alarm.
Service Stop(dsp nm)	Y	N	N	N	N	No alarm event is issued because the field does not match the conditional expression for an alarm.
Application Status	Y	Y	Y	Y	Y	--

Legend:

Y: Field's use is supported for alarms.

N: Field's use is not supported for alarms.

--: Not applicable

Application Status

Overview

The Application Status alarm monitors the status of the application being monitored by the Application Summary (`PD_APP2`) record.

Main settings

Table 6–3: PFM - Web Console alarm property setting (Application Status)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Status of application(%CVS1) has changed`
	Enable alarm	Selected
	Evaluate all data	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Do not specify.
	interval(s)	`0`
	occurrence(s) during	`0`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`Application Summary (APP2)`
	Field	• `Application Name` • `Application Exist` • `Application Status`

	Abnormal condition	`Application Name = *`
		`AND Application Exist = ABNORMAL`
		`AND Application Status = ABNORMAL`

	Warning condition	`Application Name = *`
		`AND Application Exist = NORMAL`
		`AND Application Status = ABNORMAL`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms [APP] 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/Application Status`

Available Memory

Overview

The Available Memory alarm monitors the unused size of the physical memory area (in megabytes).

The monitored value is the total size of zero memory, available memory, and standby memory (already cached) that can be allocated to processes or that can be used immediately by the system during collection. This is the most recent monitored value, not an average value.

Main settings

Table 6–4: Alarm property settings in PFM - Web Console (Available Memory)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Available memory is below %CVS megabytes`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`Free Mem Mbytes`
	Abnormal condition	`Free Mem Mbytes < 3`
	Warning condition	`Free Mem Mbytes < 4`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/Memory Used Status`

CPU Usage

Overview

The CPU Usage alarm monitors the processor usage rate (%). The monitored value is the percentage of time the processor was executing non-idle threads.

The maximum value is 100% regardless of the multiprocessor environment.

Main settings

Table 6–5: Alarm property settings in PFM - Web Console (CPU Usage)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`CPU is at %CVS% utilization`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	Occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`CPU %`
	Abnormal condition	`CPU % >= 90`
	Warning condition	`CPU % >= 80`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Status Reporting/Real-Time/CPU Used Status`

Disk Busy %

Overview

The Disk Busy % alarm monitors the disk busy rate (%). The monitored value is the percentage of time the disk was busy during read and write request processing.

This value might exceed `100` if processing for the device is executed continuously.

Main settings

Table 6–6: Alarm property settings in PFM - Web Console (Disk Busy %)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Disk busy(%CVS1) is %CVS2%`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`5`
	occurrence(s) during	`4`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`Physical Disk Overview (PI_PDSK)`
	Field	• `ID` • `Busy %`
	Abnormal condition	`ID <> "_Total"` `AND (Busy % >= "90")`
	Warning condition	`ID <> "_Total"` `AND (Busy % >= "80")`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/Physical Disk Busy Status`

Note

To display a value in the message text, set a field in the alarm condition expression. For the Disk Busy % alarm, a condition value that always satisfies the ID field is specified.

Disk Free Size

Overview

The Disk Free Size alarm monitors the size of the unused area on the logical disk.

Main settings

Table 6–7: Alarm property settings in PFM - Web Console (Disk Free Size)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Disk free size(%CVS1) is %CVS2 megabytes`
	Enable alarm	Selected
	Evaluate all data	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	--
	interval(s)	--
	occurrence(s) during	--
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`Logical Disk Overview (PI_LDSK)`
	Field	• `ID` • `Free Mbytes`
	Abnormal condition	`ID <> "_Total"` `AND (Free Mbytes < "5120")`
	Warning condition	`ID <> "_Total"` `AND (Free Mbytes < "10240")`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Status Reporting/Real-Time/Free Megabytes - Logical Disk`

Note

To display a value in the message text, set a field in the alarm condition expression. For the Disk Free Size alarm, a condition value that always satisfies the ID field (drive name) is set.

Disk Service Time

Overview

The Disk Service Time alarm monitors the device usage (in busy status). The monitored value is the average time required for a request to be completed from the time it goes into the I/O queue.

Main settings

Table 6–8: Alarm property settings in PFM - Web Console (Disk Service Time)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Average disk time(%CVS1) is %CVS2 secs`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`Physical Disk Overview (PI_PDSK)`
	Field	• `ID` • `Avg Disk Time`
	Abnormal condition	`ID <> "_Total"` `AND Avg Disk Time > 0.1`
	Warning condition	`ID <> "_Total"` `AND Avg Disk Time > 0.06`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Status Reporting/Real-Time/Avg Disk Time Status`

Disk Space

Overview

The Disk Space alarm monitors the ratio of the free area on the logical disk to the total available area.

Main settings

Table 6–9: Alarm property settings in PFM - Web Console (Disk Space)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	Available disk space(%CVS1) is %CVS2%
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	3
	occurrence(s) during	2
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	Logical Disk Overview (PI_LDSK)
	Field	• ID • Free Mbytes % • Size
	Abnormal condition	ID <> "_Total" AND (Free Mbytes % < 5 AND Size > 0)
	Warning condition	ID <> "_Total" AND (Free Mbytes % < 15 AND Size > 0)

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

Reports/RM Platform/Status Reporting/Real-Time/Free Megabytes - Logical Disk

I/O Wait Time

Overview

The I/O Wait Time alarm monitors the percentage of time all processors on the entire host were in I/O wait status.

Main settings

Table 6–10: Alarm property settings in PFM - Web Console (I/O Wait Time)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	I/O wait time is %CVS%
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	3
	occurrence(s) during	2
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	System Summary (PI)
	Field	Wait %
	Abnormal condition	Wait % > 80
	Warning condition	Wait % > 60

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

Reports/RM Platform/Status Reporting/Real-Time/CPU Used Status

Note

Do not use this alarm when the OS of the monitored host is Windows.

Kernel CPU

Overview

The Kernel CPU alarm monitors the percentage of time all processors in the entire host were running in the kernel mode.

Main settings

Table 6–11: Alarm property settings in PFM - Web Console (Kernel CPU)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Kernel mode CPU usage is %CVS%`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`System %`
	Abnormal condition	`System % > 75`
	Warning condition	`System % > 50`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Status Reporting/Real-Time/CPU Used Status`

Network Received

Overview

The Network Received alarm monitors for reception of data that exceeds the bandwidth of the network interface card.

Main settings

Table 6–12: Alarm property settings in PFM - Web Console (Network Received)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Received is %CVS bytes/sec`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`5`
	occurrence(s) during	`3`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`Network Interface Overview (PI_NET)`
	Field	`Rcvd Bytes/sec`
	Abnormal condition	`Rcvd Bytes/sec >= 50000`#1
	Warning condition	`Rcvd Bytes/sec >= 50000`#2

Legend:

--: The setting is always ignored.

#1

A guideline for the value to be set is about 70% of the NIC bandwidth.

#2

A guideline for the value to be set is about 50% of the NIC bandwidth.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/Network Data`

Note

- Do not use this alarm when the OS of the monitored host is UNIX.
- `50000` is set as the value for this alarm for both abnormal and warning conditions. To use this alarm, change the values for abnormal and warning conditions as appropriate to the user's environment.

Page Faults

Overview

The Page Faults alarm monitors the memory load status.

Main settings

Table 6–13: Alarm property settings in PFM - Web Console (Page Faults)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Page fault is %CVS/sec`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`Page Fault Counts/sec`
	Abnormal condition	`Page Fault Counts/sec >= 5`
	Warning condition	`Page Fault Counts/sec >= 4`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/System Overview`

Note

Do not use this alarm when the OS of the monitored host is HP-UX or Linux.

Pagescans

Overview

The Pagescans alarm monitors the virtual memory available to the system. The monitored value is the number of page scans per second.

Main settings

Table 6–14: Alarm property settings in PFM - Web Console (Pagescans)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Pagescan rate is %CVS/sec`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`Page Scan Counts/sec`
	Abnormal condition	`Page Scan Counts/sec > 150`
	Warning condition	`Page Scan Counts/sec > 100`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/System Overview`

Note

Do not use this alarm when the OS of the monitored host is Windows, Linux, or Solaris.

Process Existence

Overview

The Process Existence alarm monitors the existence of processes. If the existence of a process cannot be confirmed, it means that the process has stopped.

Main settings

Table 6–15: PFM - Web Console alarm property setting (Process Existence)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	Process status has changed
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Do not specify.
	interval(s)	0
	occurrence(s) during	0
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Normal**
Alarm Conditions	**Record**	Application Process Overview (PD_APS)
	Field	Program Name
	Abnormal condition	Program Name = jpcsto.exe#
	Warning condition	Program Name = jpcsto.exe#

Legend:

--: The setting is always ignored.

#

Specify the name of the program to be monitored. Make sure that the character string you enter matches what is entered in the Program Name field of the PD_APS record.

Any character in the information to be acquired that is not in the ASCII character set range of 0x20 to 0x7E will be converted to a hash mark (#: 0x23) before it is stored in the Program Name field of the PD_APS record. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter Ａ is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

Alarm table

PFM RM Platform Template Alarms [PS] 09.10

Related reports

None.

Processor Queue

Overview

The Processor Queue alarm monitors processor congestion.

Main settings

Table 6–16: Alarm property settings in PFM - Web Console (Processor Queue)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	Queue Length is %CVS
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	3
	occurrence(s) during	2
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	System Summary (PI)
	Field	Processor Queue Length
	Abnormal condition	Processor Queue Length >= 10
	Warning condition	Processor Queue Length >= 2

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

Reports/RM Platform/Status Reporting/Real-Time/CPU Used Status

Note

Do not use this alarm when the OS of the monitored host is UNIX.

Run Queue

Overview

The Run Queue alarm monitors the number of threads in the execution queue.

Main settings

Table 6–17: Alarm property settings in PFM - Web Console (Run Queue)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Run queue avg five minute is %CVS`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	--
	interval(s)	--
	occurrence(s) during	--
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`Run Queue Avg 5 min`
	Abnormal condition	`Run Queue Avg 5 min > 8`
	Warning condition	`Run Queue Avg 5 min > 4`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Status Reporting/Real-Time/CPU Used Status`

Note

Do not use this alarm when the OS of the monitored host is Windows.

Service Stop

Overview

The Service Stop alarm monitors the service name used in the service control manager database and the service status at the time of data collection. If the application service (process) is not active (running), it means that the service has stopped.

Main settings

Table 6–18: PFM - Web Console alarm property setting (Service Stop)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	State of service(%CVS1) has changed
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Do not specify.
	interval(s)	0
	occurrence(s) during	0
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	Application Service Overview (PD_ASVC)
	Field	• Service Name • State
	Abnormal condition	Service Name = JP1PCAGT_7S_RM# AND State <> Running
	Warning condition	Service Name = JP1PCAGT_7S_RM# AND State <> Running

Legend:

--: The setting is always ignored.

#

Specify the name of the service to be monitored. The settings in the table gives an example that sets the service name for a Remote Monitor Store service whose instance name is RM. Make sure that the character string you enter matches what is entered in the Service Name field of the PD_ASVC record.

Any character in the information to be acquired that is not in the ASCII character set range of 0x20 to 0x7E will be converted to a hash mark (#: 0x23) before it is stored in the Service Name field of the PD_ASVC record. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter Ａ is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

Alarm table

PFM RM Platform Template Alarms [SVC] 09.10

Related reports

None.

Note

Do not use this alarm if the OS of the monitored host is UNIX.

Service Stop(dsp nm)

Overview

The Service Stop(`dsp nm`) alarm monitors the name (display name) used by the user interface program to identify a service and the service status at the time of data collection. If the application service (process) is not active (running), it means that the service has stopped.

Main settings

Table 6–19: PFM - Web Console alarm property setting (Service Stop(dsp nm))

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`State of service(%CVS1) has changed`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Do not specify.
	interval(s)	`0`
	occurrence(s) during	`0`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`Application Service Overview (PD_ASVC)`
	Field	• `Display Name` • `State`
	Abnormal condition	`Display Name = PFM - RM Store for Platform RM`# `AND State <> Running`
	Warning condition	`Display Name = PFM - RM Store for Platform RM`# `AND State <> Running`

Legend:

--: The setting is always ignored.

#

Specify the display name of the service to be monitored. The settings in the table give an example that sets the display name for a Remote Monitor Store service whose instance name is `RM`. Make sure that the character string you enter here matches what is entered in the `Display Name` field of the `PD_ASVC` record.

Any character in the information to be acquired that is not in the ASCII character set range of `0x20` to `0x7E` will be converted to a hash mark (`#`: `0x23`) before it is stored in the Display Name field of the `PD_ASVC` record. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter Ａ is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

Alarm table

PFM RM Platform Template Alarms [SVC] 09.10

Related reports

None.

Note

Do not use this alarm if the OS of the monitored host is UNIX.

Swap Outs

Overview

The Swap Outs alarm monitors the swap area.

Main settings

Table 6–20: Alarm property settings in PFM - Web Console (Swap Outs)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Swapout rate is %CVS/sec`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	--
	interval(s)	--
	occurrence(s) during	--
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`Swap-Out Pages/sec`
	Abnormal condition	`Swap-Out Pages/sec > 200`
	Warning condition	`Swap-Out Pages/sec > 100`

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/System Overview`

Note

Do not use this alarm when the OS of the monitored host is Windows or AIX.

Target Host Status

Overview

The Target Host Status alarm monitors the status of the connection to the monitored host.

Main settings

Table 6–21: Alarm property settings in PFM - Web Console (Target Host Status)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	Target Host status has changed
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	3
	occurrence(s) during	2
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	System Status (PD)
	Field	Status
	Abnormal condition	Status <> SUCCESS
	Warning condition	Status <> SUCCESS

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

Reports/RM Platform/Troubleshooting/Recent Past/Target Host Status

Used Swap Mbytes

Overview

The Used Swap Mbytes alarm monitors the memory usage status.

Main settings

Table 6–22: Alarm property settings in PFM - Web Console (Used Swap Mbytes)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	`RM Platform`
	Alarm message	`Used swap is %CVS megabytes`
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	`3`
	occurrence(s) during	`2`
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	`System Summary (PI)`
	Field	`Used Swap Mbytes`
	Abnormal condition	`Used Swap Mbytes >= 1024`#1
	Warning condition	`Used Swap Mbytes >= 1024`#2

Legend:

--: The setting is always ignored.

#1

A guideline for the value to be set is about 90% of the value set for Total Swap Mbytes.

#2

Set the same value as for Total Mem Mbytes.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

`Reports/RM Platform/Troubleshooting/Real-Time/Pool Nonpaged Status`

Note

`1024` is set as the value for this alarm for both abnormal and warning conditions. To use this alarm, change the values for abnormal and warning conditions as appropriate to the user's environment.

User CPU

Overview

The User CPU alarm monitors the percentage of the time all processors in the entire host were running in the user mode.

Main settings

Table 6–23: Alarm property settings in PFM - Web Console (User CPU)

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	**Product**	RM Platform
	Alarm message	User mode CPU usage is %CVS%
	Enable alarm	Selected
	Monitoring time range	**Always monitor**
	Report alarm when the following damping condition is reached	Selected
	interval(s)	3
	occurrence(s) during	2
Action	**Email**	--
	Command	--
	SNMP	**Abnormal**, **Warning**, **Normal**
Alarm Conditions	**Record**	System Summary (PI)
	Field	User %
	Abnormal condition	User % > 85
	Warning condition	User % > 65

Legend:

--: The setting is always ignored.

Alarm table

PFM RM Platform Template Alarms 09.10

Related reports

Reports/RM Platform/Status Reporting/Real-Time/CPU Used Status

Format of report explanations

This section describes the format used to explain reports. The reports are presented in alphabetical order.

Report name

Indicates the report's name in the monitoring template.

A report whose name includes `(Multi-Agent)` displays information about multiple instances.

A report whose name does not include `(Multi-Agent)` displays information about a single instance.

Overview

Provides an overview of the information that can be displayed in the report.

Storage location

Indicates the storage location of the report.

Record

Indicates the record that contains the performance data used in the report. To display a historical report, you must specify information in advance in order to collect the indicated record. Before displaying a historical report, check the Agents window in PFM - Web Console to see if **Log** is set to **Yes**. This setting is not needed to display a real-time report.

Fields

Provides a table that describes the fields used in the report.

Drilldown reports (report level)

Provides a table that lists other reports in the monitoring template that are related to this report. To display these drilldown reports, in the PFM - Web Console Report window, select the name of the desired drilldown report from the drilldown report drop-down list, and then click **Display Reports**. Note that some reports do not have any drilldown reports.

Drilldown reports (field level)

Provides a table that describes reports in the monitoring template that are associated with fields used in this report. To display these drilldown reports, in the PFM - Web Console Report window, choose **Graph**, **List**, or **Table**. In the case of a historical report, you can display the drilldown report in smaller intervals by displaying it from the time item. Note that some reports do not have any drilldown reports.

For details about the drilldown reports, see the chapter that describes report creation for operation analysis in the *Job Management Partner 1/Performance Management User's Guide*.

Organization of report directories

The following shows the organization of the report directories for PFM - RM for Platform. Angle brackets enclose directory names.

```
+-- <RM Platform>
    +-- <Monthly Trend>
    |   +-- CPU Used Status
    |   +-- CPU Used Status (Multi-Agent)
    |   +-- Memory Used Status (Multi-Agent)
    +-- <Status Reporting>
    |   +-- <Daily Trend>
    |   |   +-- CPU Used Status (Multi-Agent)
    |   |   +-- Memory Paging Status
    |   |   +-- Memory Used Status
    |   |   +-- Memory Used Status (Multi-Agent)
    |   +-- <Real-Time>
    |   |   +-- Avg Disk Time Status
    |   |   +-- CPU Used Status
    |   |   +-- Free Megabytes - Logical Disk
    +-- <Troubleshooting>
        +-- <Real-Time>
        |   +-- CPU Per Processor Status
        |   +-- Memory Paging Status
        |   +-- Memory Used Status
        |   +-- Network Data
        |   +-- Physical Disk Busy Status
        |   +-- Pool Nonpaged Status
        |   +-- System Overview
        |   +-- Application Status
        |   +-- <Drillidown Only>
        |       +-- Application Process Status
        +-- <Recent Past>
            +-- Avg Disk Time Status
            +-- CPU Used Status
            +-- Free Megabytes - Logical Disk
            +-- Memory Paging Status
            +-- Memory Used Status
            +-- Network Data
            +-- Physical Disk Busy Status
            +-- Pool Nonpaged Status
            +-- System Overview
            +-- Target Host Status
            +-- <Drillidown Only>
                +-- Application Process Count
```

The following describes each directory.

`Monthly Trend` directory

This directory contains reports that display daily information for the past month. Use the reports in this directory to check monthly trends in the system.

`Status Reporting` directory

This directory contains reports that display daily information. Use the reports in this directory to check the overall status of the system. You can display real-time reports as well as historical reports.

`Daily Trend` directory

This directory contains reports for displaying hourly information for the past 24 hours. Use the reports in this directory to check the daily status of the system.

`Real-Time` directory

This directory contains real-time reports for checking the system status.

`Troubleshooting` directory

This directory contains reports for displaying information that is useful for resolving problems. In the event of a system problem, use the reports in this directory to check the cause of the problem.

`Real-Time` directory

This directory contains real-time reports for checking the current system status.

`Recent Past` directory

This directory contains historical reports for displaying minute-by-minute information for the past hour.

These directories also contain the following directory:

`Drilldown Only` directory

This directory contains a report that is displayed as a drilldown (field level) report. It is used to display the detailed information related to the fields of the main report.

List of reports

The following table lists and describes the reports defined in the monitoring template for PFM - RM for Platform.

Table 6–24: List of reports

Category	Report name	Displayed information
System	`System Overview` (real-time report indicating the system operation status)	Displays the current operation status of the system.
	`System Overview` (historical report indicating the system operation status)	Displays the minute-by-minute system operation status over the past hour.
	`Target Host Status` (historical report indicating the status of the connection to the monitored host and information about the OS of the monitored host)	Displays the minute-by-minute status of the connection to the monitored host and information about the OS of the monitored host over the past hour.
Disk	`Avg Disk Time Status` (real-time report indicating the average I/O time for the physical disk)	Displays the current average I/O operation time for the physical disk.
	`Avg Disk Time Status` (historical report indicating the average I/O time for the physical disk)	Displays minute-by-minute the average I/O operation time for the physical disk over the past hour.
	`Free Megabytes - Logical Disk` (real-time report indicating the available area on the logical disk)	Displays information about the area that is currently available on the logical disk.
	`Free Megabytes - Logical Disk` (historical report indicating the available area on the logical disk)	Displays minute-by-minute information about the area that is available on the logical disk over the past hour.
	`Physical Disk Busy Status` (real-time report indicating the length of time the disk was busy)	Displays the percentage of time the current disk was busy.
	`Physical Disk Busy Status` (historical report indicating the length of time the disk was busy)	Displays minute-by-minute information about the percentage of time the disk was busy over the past hour.
Network	`Network Data` (real-time report indicating the status of communication between networks)	Displays the current status of communication between networks.
	`Network Data` (historical report indicating the status of communication between networks)	Displays the minute-by-minute status of communication between networks over the past hour.
Processor	`CPU Per Processor Status` (real-time report indicating the processor usage rate for each processor)	Displays the current processor usage rate for each processor.
	`CPU Used Status` (real-time report indicating the CPU usage status)	Displays the current CPU usage status in the system.
	`CPU Used Status` (historical report indicating the CPU usage status (1 month))	Displays the daily CPU usage status over the past month.
	`CPU Used Status` (historical report indicating the CPU usage status (1 hour))	Displays the minute-by-minute CPU usage status in the system over the past hour.
	`CPU Used Status (Multi-Agent)` (historical report indicating the CPU usage status in multiple systems (1 month))	Displays the daily CPU usage status in multiple systems over the past month.
	`CPU Used Status (Multi-Agent)` (historical report indicating the CPU usage status in multiple systems (1 day))	Displays the hourly CPU usage status in multiple systems over the past day (24 hours).
Memory	`Memory Paging Status` (real-time report indicating information about memory and paging)	Displays current information about memory and paging.

Category	Report name	Displayed information
Memory	`Memory Paging Status` (historical report indicating information about memory and paging (1 day))	Displays hourly information about memory and paging over the past day (24 hours).
	`Memory Paging Status` (historical report indicating information about memory and paging (1 hour))	Displays minute-by-minute information about memory and paging over the past hour.
	`Memory Used Status` (real-time report indicating the physical memory usage status in the system)	Displays the current physical memory usage status in the system.
	`Memory Used Status` (historical report indicating the physical memory usage status in the system (1 day))	Displays the hourly physical memory usage status in the system over the past day (24 hours).
	`Memory Used Status` (historical report indicating the physical memory usage status in the system (1 hour))	Displays the minute-by-minute physical memory usage status in the system over the past hour.
	`Memory Used Status (Multi-Agent)` (historical report indicating the physical memory usage status in multiple systems (1 month))	Displays the daily physical memory usage status in multiple systems over the past month.
	`Memory Used Status (Multi-Agent)` (historical report indicating the physical memory usage status in multiple systems (1 day))	Displays the hourly physical memory usage status in multiple systems over the past day (24 hours).
	`Pool Nonpaged Status` (real-time report indicating the size of the physical memory in the system that cannot be paged out)	Displays the current size of the physical memory in the system that cannot be paged out.
	`Pool Nonpaged Status` (historical report indicating the size of the physical memory in the system that cannot be paged out)	Displays the minute-by-minute size of the physical memory in the system that cannot be paged out over the past hour.
Process	`Application Status` (real-time report indicating the operation status of an application)	Displays the current operation status of an application.
	`Application Process Status` (real-time report indicating the operation status of each process and service of an application)	Displays the current operation status of each process and service of an application.
	`Application Process Count` (historical report indicating the operation status of each process and service of an application)	Displays a summary of the minute-by-minute operation status of each process and service of an application collected over the past hour.

Application Process Count (historical report indicating the operation status of each process and service of an application)

Overview

The `Application Process Count` report displays a summary of the minute-by-minute operation status of each process and service of an application collected over the past hour. The display format is a line graph. This report is a drilldown report.

Storage location

`/RM Platform/Troubleshooting/Recent Past/Drilldown Only`

Record

`PD_APPC`

Fields

Table 6–25: Description of fields (Application Process Count (historical report indicating the operation status of each process and service of an application))

Field name	Description
Application Name	Application definition name specified during process monitoring setup
Monitoring Count	Number of running processes and services that match the monitoring condition
Monitoring Label	Name for identifying a specific monitoring condition
Monitoring Max	Maximum monitoring count
Monitoring Min	Minimum monitoring count
Monitoring Number	Monitoring condition number
Monitoring Status	Conditional result of the monitoring count `NORMAL`: No problem `ABNORMAL`: Abnormal
Polling Time	Time when the performance information was collected on the PFM - RM host
Target Host Time	Time when the performance information was collected on the monitored host

Application Process Status (real-time report indicating the operation status of each process and service of an application)

Overview

The `Application Process Status` report displays the current operation status of each process and service of an application. This is a drilldown report.

Storage location

`/RM Platform/Troubleshooting/Real-Time/Drilldown Only`

Record

`PD_APPD`

Fields

Table 6–26: Description of fields (Application Process Status (real-time report indicating the operation status of each process and service of an application))

Field name	Description
Application Name	Application definition name specified during process monitoring setup
Monitoring Condition	Conditional expression for identifying specific processes and services to be monitored
Monitoring Count	Number of running processes and services that match the monitoring condition
Monitoring Field	Field to be monitored
Monitoring Label	Name for identifying a specific monitoring condition
Monitoring Max	Maximum monitoring count
Monitoring Min	Minimum monitoring count
Monitoring Number	Monitoring condition number
Monitoring Status	Conditional result of the monitoring count `NORMAL`: No problem `ABNORMAL`: Abnormal
Polling Time	Time when the performance information was collected on the PFM - RM host
Target Host Time	Time when the performance information was collected on the monitored host

Drilldown report (field level)

Table 6–27: Description of drilldown report (field level) (Application Process Status (real-time report indicating the operation status of each process and service of an application))

Report name	Description
`Application Process Count`	Displays a summary of the minute-by-minute operation status of each process and service of an application collected over the past hour. To display this report, click the **Monitoring Count** field.

Application Status (real-time report indicating the operation status of an application)

Overview

The `Application Status` report displays the current operation status of an application. The display format is a table.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PD_APP2`

Fields

Table 6–28: Description of fields (Application Status (real-time report indicating the operation status of an application))

Field name	Description
Application Exist	Application status specified during process monitoring setup. An application status is a result obtained based on the statuses of the processes and services specified as monitoring targets. To check the statuses of the processes and services specified as monitoring targets, see `Monitoring Status` displayed in the Application Process Count (`PD_APPC`) record and Application Process Detail (`PD_APPD`) record. `NORMAL`: The status of at least one of the monitoring targets is normal. `ABNORMAL`: The statuses of all monitoring targets are abnormal.
Application Name	Application definition name specified during process monitoring setup
Application Status	Application status specified during process monitoring setup. An application status is a result obtained based on the statuses of the processes and services specified as monitoring targets. To check the statuses of the processes and services specified as monitoring targets, see `Monitoring Status` displayed in the Application Process Count (`PD_APPC`) record and Application Process Detail (`PD_APPD`) record. `NORMAL`: The statuses of all monitoring targets are normal. `ABNORMAL`: The status of at least one of the monitoring targets is abnormal.
Polling Time	Time when the performance information was collected on the PFM - RM host
Target Host Time	Time when the performance information was collected on the monitored host

Drilldown report (field level)

Table 6–29: Description of drilldown report (field level) (Application Status (real-time report indicating the operation status of an application))

Report name	Description
`Application Process Status`	Displays the current operation status of each process and service of an application. To display this report, click the **Application Name** field.

Avg Disk Time Status (real-time report indicating the average I/O time for the physical disk)

Overview

The `Avg Disk Time Status` report displays the current average I/O operation time for the physical disk. The display format is a bar graph.

Storage location

`/RM Platform/Status Reporting/Real-Time`

Record

`PI_PDSK`

Fields

Table 6–30: Description of fields (Avg Disk Time Status (Real-time report indicating the average I/O time for the physical disk))

Field name	Description
Avg Disk Time	Average disk I/O operation time (seconds)
ID	**In Windows:** Physical disk number **In UNIX:** Device name
Polling Time	Time the performance data was collected on the PFM - RM host
Read Counts/sec	Disk read processing speed (times/second)
Read MBytes/sec	Speed of data transfer to the disk during read processing (megabytes/second)
Target Host Time	Time the performance data was collected on the monitored host
Total Counts/sec	Disk read and write processing speed (times/second)
Total MBytes/sec	Speed of data transfer between disks during read and write processing (megabytes/second)
Write Counts/sec	Disk write processing speed (times/second)
Write MBytes/sec	Speed of data transfer to the disk during write processing (megabytes/second)

Avg Disk Time Status (historical report indicating the average I/O time for the physical disk)

Overview

The `Avg Disk Time Status` report displays minute-by-minute the average I/O operation time for the physical disk over the past hour. The display format is a bar graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI_PDSK`

Fields

Table 6–31: Description of fields (Avg Disk Time Status (historical report indicating the average I/O time for the physical disk))

Field name	Description
Avg Disk Time	Average disk I/O operation time (seconds)
ID	**In Windows:** Physical disk number **In UNIX:** Device name
Polling Time	Time the performance data was collected on the PFM - RM host
Read Counts/sec	Disk read processing speed (times/second)
Read MBytes/sec	Speed of data transfer to the disk during read processing (megabytes/second)
Target Host Time	Time the performance data was collected on the monitored host
Total Counts/sec	Disk read and write processing speed (times/second)
Total MBytes/sec	Speed of data transfer between disks during read and write processing (megabytes/second)
Write Counts/sec	Disk write processing speed (times/second)
Write MBytes/sec	Speed of data transfer to the disk during write processing (megabytes/second)

CPU Per Processor Status (real-time report indicating the processor usage rate for each processor)

Overview

The `CPU Per Processor Status` report displays the current processor usage rate for each processor. The display format is a stacked bar graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI_CPU`

Fields

Table 6–32: Description of fields (CPU Per Processor Status (real-time report indicating the processor usage rate for each processor))

Field name	Description
CPU %	Processor's CPU usage rate (%)
ID	Processor ID
Idle %	Percentage of the time the processor was in idle status (%)
Interrupt Counts/sec	**In Windows:** Frequency of hardware interrupt reception processing performed by the processor (times/second); *hardware* refers to devices that generate interrupts, such as the system clock, mouse, disk driver, data communication line, NIC, and other peripheral devices. This value does not include DPC (delayed procedure call) interrupts. Normally, if the value of this field increases greatly while there is no system activity, a hardware problem is suspected (such as a slow device). **In UNIX:** Frequency of interrupts (times/second)
Polling Time	Time the performance data was collected on the PFM - RM host
System %	Usage rate for a processor that was executed in the kernel mode (%)
Target Host Time	Time the performance data was collected on the monitored host
User %	Usage rate for a processor that was executed in the user mode (%)
Wait %	Percentage of the time the processor was in I/O wait status (%)

CPU Used Status (real-time report indicating the CPU usage status)

Overview

The `CPU Used Status` report displays the current CPU usage status in the system. The display format is a line graph.

Storage location

`/RM Platform/Status Reporting/Real-Time`

Record

`PI`

Fields

Table 6–33: Description of fields (CPU Used Status (real-time report indicating the CPU usage status))

Field name	Description
Active CPUs	Number of processors
CPU %	Processor usage rate (%). This is also the average value for all processors.
Idle %	Percentage of the time the processor was in idle status (%). This is also the average value for all processors.
Interrupt Counts/sec	**In Windows:** Frequency of hardware interrupt reception processing performed by the processor (times/second); *hardware* refers to devices that generate interrupts, such as system clock, mouse, disk driver, data communication line, NIC, and other peripheral devices. This value does not include DPC (delayed procedure call) interrupts. Normally, if the value of this field increases greatly while there is no system activity, a hardware problem is suspected (such as a slow device). **In UNIX:** Frequency of interrupts (times/second)
Polling Time	Time the performance data was collected on the PFM - RM host
Processor Queue Length	Number of requests ready for execution that are waiting in the processor queue for processor time. Normally, if the queue length exceeds 2 continuously, the processor is busy.
Run Queue Avg 5 min	Average number of threads waiting in the execution queue for the past 5 minutes. In the case of UNIX (HP-UX, Solaris, and AIX), this value does not include the number of threads waiting for I/O. In Linux, this value does contain the number of threads waiting for I/O.
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
Target Host Time	Time the performance data was collected on the monitored host
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.
Wait %	Percentage of the time the processor was in I/O wait status (%). This is also the average value for all processors.

Drilldown report (report level)

Table 6–34: Description of drilldown report (report level) (CPU Used Status (real-time report indicating the CPU usage status))

Report name	Description
`CPU Per Processor Status`	Displays the current processor usage rate for each processor.

CPU Used Status (historical report indicating the CPU usage status (1 month))

Overview

The `CPU Used Status` report displays the daily CPU usage status over the past month. The display format is a line graph.

Storage location

`/RM Platform/Monthly Trend`

Record

`PI`

Fields

Table 6–35: Description of fields (CPU Used Status (historical report indicating the CPU usage status (1 month)))

Field name	Description
Active CPUs	Number of processors
CPU %	Processor usage rate (%). This is also the average value for all processors.
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.

CPU Used Status (historical report indicating the CPU usage status (1 hour))

Overview

The `CPU Used Status` report displays the minute-by-minute CPU usage status over the past hour. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI`

Fields

Table 6–36: Description of fields (CPU Used Status (historical report indicating the CPU usage status (1 hour)))

Field name	Description
Active CPUs	Number of processors
CPU %	Processor usage rate (%). This is also the average value for all processors.
Idle %	Percentage of the time the processor was in idle status (%). This is also the average value for all processors.
Interrupt Counts/sec	**In Windows:** Frequency of hardware interrupt reception processing performed by the processor (times/second); *hardware* refers to devices that generate interrupts, such as system clock, mouse, disk driver, data communication line, NIC, and other peripheral devices. This value does not include DPC (delayed procedure call) interrupts. Normally, if the value of this field increases greatly while there is no system activity, a hardware problem is suspected (such as a slow device). **In UNIX:** Frequency of interrupts (times/second)
Polling Time	Time the performance data was collected on the PFM - RM host
Processor Queue Length	Number of requests ready for execution that are waiting in the processor queue for processor time. Normally, if the queue length exceeds 2 continuously, the processor is busy.
Run Queue Avg 5 min	Average number of threads waiting in the execution queue for the past 5 minutes. In the case of UNIX (HP-UX, Solaris, and AIX), this value does not include the number of threads waiting for I/O. In Linux, this value does contain the number of threads waiting for I/O.
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
Target Host Time	Time the performance data was collected on the monitored host
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.
Wait %	Percentage of the time the processor was in I/O wait status (%). This is also the average value for all processors.

CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 month))

Overview

The `CPU Used Status (Multi-Agent)` report displays the daily CPU usage status in multiple systems over the past month. The display format is a line graph.

Storage location

`/RM Platform/Monthly Trend`

Record

`PI`

Fields

Table 6–37: Description of fields (CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 month)))

Field name	Description
Active CPUs	Number of processors
Agent Host	Identifier including the name of the host where PFM - RM for Platform is running
CPU %	Processor usage rate (%). This is also the average value for all processors.
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.

Drilldown report (report level)

Table 6–38: Description of drilldown report (report level) (CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 month)))

Report name	Description
`CPU Used Status`	Displays the minute-by-minute CPU usage status in the system over the past hour.

CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 day))

Overview

The `CPU Used Status (Multi-Agent)` report displays the hourly CPU usage status in multiple systems over the past day (24 hours). The display format is a line graph.

Storage location

`/RM Platform/Status Reporting/Daily Trend`

Record

`PI`

Fields

Table 6–39: Description of fields (CPU Used Status (Multi-Agent) (historical report indicating the CPU usage status in multiple systems (1 day)))

Field name	Description
Active CPUs	Number of processors
Agent Host	Identifier including the name of the host where PFM - RM for Platform is running
CPU %	Processor usage rate (%). This is also the average value for all processors.
Idle %	Percentage of the time the processor was in idle status (%). This is also the average value for all processors.
Interrupt Counts/sec	**In Windows:** Frequency of hardware interrupt reception processing performed by the processor (times/second); *hardware* refers to devices that generate interrupts, such as system clock, mouse, disk driver, data communication line, NIC, and other peripheral devices. This value does not include DPC (delayed procedure call) interrupts. Normally, if the value of this field increases greatly while there is no system activity, a hardware problem is suspected (such as a slow device). **In UNIX:** Frequency of interrupts (times/second)
Processor Queue Length	Number of requests ready for execution that are waiting in the processor queue for processor time. Normally, if the queue length exceeds 2 continuously, the processor is busy.
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.
Wait %	Percentage of the time the processor was in I/O wait status (%). This is also the average value for all processors.

Free Megabytes - Logical Disk (real-time report indicating the available area on the logical disk)

Overview

The `Free Megabytes - Logical Disk` report displays information about the area that is currently available on the logical disk. The display format is a bar graph.

Storage location

`/RM Platform/Status Reporting/Real-Time`

Record

`PI_LDSK`

Fields

Table 6–40: Description of fields (Free Megabytes - Logical Disk (real-time report indicating the available area on the logical disk))

Field name	Description
Device Name	Device name
Free Mbytes	Size of the unused area (megabytes)
Free Mbytes %	Percentage of unused area (%)
ID	**In Windows:** Logical disk volume name **In UNIX:** Mount point of the file system
Polling Time	Time the performance data was collected on the PFM - RM host
Size	Disk size (megabytes)
Target Host Time	Time the performance data was collected on the monitored host

Free Megabytes - Logical Disk (historical report indicating the available area on the logical disk)

Overview

The `Free Megabytes - Logical Disk` report displays minute-by-minute information about the area that is available on the logical disk over the past hour. The display format is a bar graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI_LDSK`

Fields

Table 6–41: Description of fields (Free Megabytes - Logical Disk (historical report indicating the available area on the logical disk))

Field name	Description
Device Name	Device name
Free Mbytes	Size of unused area (megabytes)
Free Mbytes %	Percentage of unused area (%)
ID	**In Windows:** Logical disk volume name **In UNIX:** Mount point of the file system
Polling Time	Time the performance data was collected on the PFM - RM host
Size	Disk size (megabytes)
Target Host Time	Time the performance data was collected on the monitored host

Memory Paging Status (real-time report indicating information about memory and paging)

Overview

The `Memory Paging Status` report displays current information about memory and paging. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI`

Fields

Table 6–42: Description of fields (Memory Paging Status (real-time report indicating information about memory and paging))

Field name	Description
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Target Host Time	Time the performance data was collected on the monitored host
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)

Field name	Description
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

Memory Paging Status (historical report indicating information about memory and paging (1 day))

Overview

The `Memory Paging Status` report displays hourly information about memory and paging over the past day (24 hours). The display format is a line graph.

Storage location

`/RM Platform/Status Reporting/Daily Trend`

Record

`PI`

Fields

Table 6–43: Description of fields (Memory Paging Status (historical report indicating information about memory and paging (1 day)))

Field name	Description
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes)

Field name	Description
Used Swap Mbytes	**In UNIX:** Size of the swap area used (megabytes)

Memory Paging Status (historical report indicating information about memory and paging (1 hour))

Overview

The `Memory Paging Status` report displays minute-by-minute information about memory and paging over the past hour. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI`

Fields

Table 6–44: Description of fields (Memory Paging Status (historical report indicating information about memory and paging (1 hour)))

Field name	Description
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Target Host Time	Time the performance data was collected on the monitored host
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)

Field name	Description
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

Memory Used Status (real-time report indicating the physical memory usage status in the system)

Overview

The `Memory Used Status` report displays the current physical memory usage status in the system. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI`

Fields

Table 6–45: Description of fields (Memory Used Status (real-time report indicating the physical memory usage status in the system))

Field name	Description
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Target Host Time	Time the performance data was collected on the monitored host
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)

Field name	Description
Used Mem Mbytes	Size of the physical memory area used (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

Memory Used Status (historical report indicating the physical memory usage status in the system (1 day))

Overview

The `Memory Used Status` report displays the hourly physical memory usage status in the system over the past day (24 hours). The display format is a line graph.

Storage location

`/RM Platform/Status Reporting/Daily Trend`

Record

`PI`

Fields

Table 6–46: Description of fields (Memory Used Status (historical report indicating the physical memory usage status in the system (1 day)))

Field name	Description
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)
Used Mem Mbytes	Size of the physical memory area used (megabytes)

Field name	Description
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

Memory Used Status (historical report indicating the physical memory usage status in the system (1 hour))

Overview

The `Memory Used Status` report displays the minute-by-minute physical memory usage status in the system over the past hour. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI`

Fields

Table 6–47: Description of fields (Memory Used Status (historical report indicating the physical memory usage status in the system (1 hour)))

Field name	Description
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Target Host Time	Time the performance data was collected on the monitored host
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)

Field name	Description
Used Mem Mbytes	Size of the physical memory area used (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

Memory Used Status (Multi-Agent) (historical report indicating the physical memory usage status in multiple systems (1 month))

Overview

The `Memory Used Status (Multi-Agent)` report displays the daily physical memory usage status in multiple systems over the past month. The display format is a stacked bar graph.

Storage location

`/RM Platform/Monthly Trend`

Record

`PI`

Fields

Table 6–48: Description of fields (Memory Used Status (Multi-Agent) (historical report indicating the physical memory usage status in multiple systems (1 month)))

Field name	Description
Agent Host	Identifier including the name of the host where PFM - RM for Platform is running
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Total Mem Mbytes	Size of the physical memory (megabytes)
Used Mem %	Physical memory usage rate (%)
Used Mem Mbytes	Size of the physical memory area used (megabytes)

Memory Used Status (Multi-Agent) (historical report indicating the physical memory usage status in multiple systems (1 day))

Overview

The `Memory Used Status (Multi-Agent)` report displays the hourly physical memory usage status in multiple systems over the past day (24 hours). The display format is a stacked bar graph.

Storage location

`/RM Platform/Status Reporting/Daily Trend`

Record

`PI`

Fields

Table 6–49: Description of fields (Memory Used Status (Multi-Agent) (historical report indicating the physical memory usage status in multiple systems (1 day)))

Field name	Description
Agent Host	Identifier including the name of the host where PFM - RM for Platform is running
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page-In Pages/sec	Rate at which pages were paged in (pages/second)
Page-Out Pages/sec	Rate at which pages were paged out (pages/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Used Mem %	Physical memory usage rate (%)
Used Mem Mbytes	Size of the physical memory area used (megabytes)

Network Data (real-time report indicating the status of communication between networks)

Overview

The `Network Data` report displays the current status of communication between networks. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI_NET`

Fields

Table 6–50: Description of fields (Network Data (real-time report indicating the status of communication between networks))

Field name	Description
ID	Instance name of the network
Max Transmission Unit	Maximum packet size (bytes)
Polling Time	Time the performance data was collected on the PFM - RM host
Rcvd Bytes/sec	Rate of data received by the network interface (bytes/second)
Rcvd Packets/sec	Rate of packets received by the network interface (packets/second)
Sent Bytes/sec	Rate of data sent by the network interface (bytes/second)
Sent Packets/sec	Rate of packets sent by the network interface (packets/second)
Target Host Time	Time the performance data was collected on the monitored host
Total Bytes/sec	Rate of data sent and received by the network interface (bytes/second)
Total Packets/sec	Rate of packets sent and received by the network interface (packets/second)

Network Data (historical report indicating the status of communication between networks)

Overview

The `Network Data` report displays the minute-by-minute status of communication between networks over the past hour. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI_NET`

Fields

Table 6–51: Description of fields (Network Data (historical report indicating the status of communication between networks))

Field name	Description
ID	Instance name of the network
Max Transmission Unit	Maximum packet size (bytes)
Polling Time	Time the performance data was collected on the PFM - RM host
Rcvd Bytes/sec	Rate of data received by the network interface (bytes/second)
Rcvd Packets/sec	Rate of packets received by the network interface (packets/second)
Sent Bytes/sec	Rate of data sent by the network interface (bytes/second)
Sent Packets/sec	Rate of packets sent by the network interface (packets/second)
Target Host Time	Time the performance data was collected on the monitored host
Total Bytes/sec	Rate of data sent and received by the network interface (bytes/second)
Total Packets/sec	Rate of packets sent and received by the network interface (packets/second)

Physical Disk Busy Status (real-time report indicating the length of time the disk was busy)

Overview

The `Physical Disk Busy Status` report displays the percentage of time the current disk was busy. The display format is a bar graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI_PDSK`

Fields

Table 6–52: Description of fields (Physical Disk Busy Status (real-time report indicating the length of time the disk was busy))

Field name	Description
Busy %	Percentage of the time the disk was busy during read and write request processing. In UNIX, this value might exceed 100 when device processing is executed continuously.
ID	**In Windows:** Physical disk number **In UNIX:** Device name
Polling Time	Time the performance data was collected on the PFM - RM host
Queue Length	**In Windows:** Average number of read and write requests placed in the disk queue **In UNIX:** Length of the device queue. A one-second volume of I/O processing is indicated as 1.
Read Counts/sec	Disk read processing speed (times/second)
Read MBytes/sec	Speed of data transfer to the disk during read processing (megabytes/second)
Target Host Time	Time the performance data was collected on the monitored host
Total Counts/sec	Disk read and write processing speed (times/second)
Total MBytes/sec	Speed of data transfer between disks during read and write processing (megabytes/second)
Write Counts/sec	Disk write processing speed (times/second)
Write MBytes/sec	Speed of data transfer to the disk during write processing (megabytes/second)

Physical Disk Busy Status (historical report indicating the length of time the disk was busy)

Overview

The `Physical Disk Busy Status` report displays minute-by-minute information about the percentage of time the disk was busy over the past hour. The display format is a bar graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI_PDSK`

Fields

Table 6–53: Description of fields (Physical Disk Busy Status (historical report indicating the length of time the disk was busy))

Field name	Description
Busy %	Percentage of time the disk was busy during read and write request processing. In UNIX, this value might exceed 100 when device processing is executed continuously.
ID	**In Windows:** Physical disk number **In UNIX:** Device name
Polling Time	Time the performance data was collected on the PFM - RM host
Queue Length	**In Windows:** Average number of read and write requests placed in the disk queue **In UNIX:** Length of the device queue. A one-second volume of I/O processing is indicated as 1.
Read Counts/sec	Disk read processing speed (times/second)
Read MBytes/sec	Speed of data transfer to the disk during read processing (megabytes/second)
Target Host Time	Time the performance data was collected on the monitored host
Total Counts/sec	Disk read and write processing speed (times/second)
Total MBytes/sec	Speed of data transfer between disks during read and write processing (megabytes/second)
Write Counts/sec	Disk write processing speed (times/second)
Write MBytes/sec	Speed of data transfer to the disk during write processing (megabytes/second)

Pool Nonpaged Status (real-time report indicating the size of physical memory in the system that cannot be paged out)

Overview

The `Pool Nonpaged Status` report displays the current size of the physical memory in the system that cannot be paged out. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI`

Fields

Table 6–54: Description of fields (Pool Nonpaged Status (real-time report indicating the size of physical memory in the system that cannot be paged out))

Field name	Description
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Pool Nonpaged KBytes	Size of the physical memory that cannot be paged out and that was used to allocate area when system components executed tasks (kilobytes). Normally, if server activity has not increased but the value of this field keeps increasing, a process that causes a memory leak might be executing.
Target Host Time	Time the performance data was collected on the monitored host
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)

Field name	Description
Used Mem Mbytes	Size of the physical memory area used (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

Pool Nonpaged Status (historical report indicating the size of physical memory in the system that cannot be paged out)

Overview

The `Pool Nonpaged Status` report displays the minute-by-minute size of the physical memory in the system that cannot be paged out over the past hour. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI`

Fields

Table 6–55: Description of fields (Pool Nonpaged Status (historical report indicating the size of physical memory in the system that cannot be paged out))

Field name	Description
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Page Fault Counts/sec	Frequency of page faults (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Pool Nonpaged KBytes	Size of the physical memory that cannot be paged out and that was used to allocate area when system components executed tasks (kilobytes). Normally, if server activity has not increased but the value of this field keeps increasing, a process that causes a memory leak might be executing.
Target Host Time	Time the performance data was collected on the monitored host
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)

Field name	Description
Used Mem Mbytes	Size of the physical memory area used (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)

System Overview (real-time report indicating the system operation status)

Overview

The `System Overview` report displays the current operation status of the system. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Real-Time`

Record

`PI`

Fields

Table 6–56: Description of fields (System Overview (real-time report indicating the system operation status))

Field name	Description
Active CPUs	Number of processors
CPU %	Processor usage rate (%). This is also the average value for all processors.
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Idle %	Percentage of the time the processor was in idle status (%). This is also the average value for all processors.
Page Fault Counts/sec	Frequency of page faults (times/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Pool Nonpaged KBytes	Size of the physical memory that cannot be paged out and that was used to allocate area when system components executed tasks (kilobytes). Normally, if server activity has not increased but the value of this field keeps increasing, a process that causes a memory leak might be executing.
Run Queue Avg 5 min	Average number of threads waiting in the execution queue for the past 5 minutes. In the case of UNIX (HP-UX, Solaris, and AIX), this value does not include the number of threads waiting for I/O. In Linux, this value does contain the number of threads waiting for I/O.
Swap-In Pages/sec	Frequency of page loading by swap-in processing (pages/second). In AIX, this is the frequency of page loading by swap-in processing only in the paging area (pages/second).

Field name	Description
Swap-Out Pages/sec	Frequency of page removal by swap-out processing (pages/second). In AIX, this is the frequency of page removal by swap-out processing only in the paging area (pages/second).
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
Target Host Time	Time the performance data was collected on the monitored host
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)
Used Mem Mbytes	Size of the physical memory area used (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.
Wait %	Percentage of the time the processor was in I/O wait status (%). This is also the average value for all processors.

System Overview (historical report indicating the system operation status)

Overview

The `System Overview` report displays the minute-by-minute system operation status over the past hour. The display format is a line graph.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PI`

Fields

Table 6–57: Description of fields (System Overview (historical report indicating the system operation status))

Field name	Description
Active CPUs	Number of processors
CPU %	Processor usage rate (%). This is also the average value for all processors.
Free Mem %	Percentage of the physical memory size actually available to applications (%)
Free Mem Mbytes	Size of the physical memory actually available to applications (megabytes)
Free Swap %	**In Windows:** Percentage of unused space in the virtual memory area (%) **In UNIX:** Percentage of unused space in the swap area (%)
Free Swap Mbytes	**In Windows:** Size of the unused space in the virtual memory area (megabytes) **In UNIX:** Size of the unused space in the swap area (megabytes)
Idle %	Percentage of the time the processor was in idle status (%). This is also the average value for all processors.
Page Fault Counts/sec	Frequency of page faults (times/second)
Page Scan Counts/sec	Frequency of page scans (times/second)
Paging Pages/sec	Rate at which pages were being paged in and out when a page fault occurred (pages/second). This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value exceeds 5 continuously, the memory might be the bottleneck in the system.
Polling Time	Time the performance data was collected on the PFM - RM host
Pool Nonpaged KBytes	Size of the physical memory that cannot be paged out and that was used to allocate area when system components executed tasks (kilobytes). Normally, if server activity has not increased but the value of this field keeps increasing, a process that causes a memory leak might be executing.
Run Queue Avg 5 min	Average number of threads waiting in the execution queue for the past 5 minutes. In the case of UNIX (HP-UX, Solaris, and AIX), this value does not include the number of threads waiting for I/O. In Linux, this value does contain the number of threads waiting for I/O.

Field name	Description
Swap-In Pages/sec	Frequency of page loading by swap-in processing (pages/second). In AIX, this is the frequency of page loading by swap-in processing only in the paging area (pages/second).
Swap-Out Pages/sec	Frequency of page removal by swap-out processing (pages/second). In AIX, this is the frequency of page removal by swap-out processing only in the paging area (pages/second).
System %	Usage rate for a processor that was executed in the kernel mode (%). This is also the average value for all processors.
Target Host Time	Time the performance data was collected on the monitored host
Total Mem Mbytes	Size of the physical memory (megabytes)
Total Swap Mbytes	**In Windows:** Size of the virtual memory area (megabytes) **In UNIX:** Size of the swap area (megabytes)
Used Mem %	Physical memory usage rate (%)
Used Mem Mbytes	Size of the physical memory area used (megabytes)
Used Swap %	**In Windows:** Virtual memory usage rate (%) **In UNIX:** Swap area usage rate (%)
Used Swap Mbytes	**In Windows:** Size of the virtual memory area used (committed) (megabytes) **In UNIX:** Size of the swap area used (megabytes)
User %	Usage rate for a processor that was executed in the user mode (%). This is also the average value for all processors.
Wait %	Percentage of the time the processor was in I/O wait status (%). This is also the average value for all processors.

Drilldown report (field level)

Table 6–58: Description of drilldown report (field level) (System Overview (historical report indicating the system operation status))

Report name	Description
`CPU Used Status`	Displays the minute-by-minute CPU usage status in the system over the past hour. To display this report, click the CPU % field.

Target Host Status (historical report indicating the status of the connection to the monitored host and information about the OS of the monitored host)

Overview

The `Target Host Status` report displays the minute-by-minute status of the connection to the monitored host and information about the OS of the monitored host over the past hour.

Storage location

`/RM Platform/Troubleshooting/Recent Past`

Record

`PD`

Fields

Table 6–59: Description of fields (Target Host Status (historical report indicating the status of the connection to the monitored host and information about the OS of the monitored host))

Field name	Description
Detail	Detailed information about the monitored host
OS Type	Name of the OS of the monitored host
Polling Time	Time the performance data was collected on the PFM - RM host
Processor Type	Processor type of the monitored host
Reason	Cause of `ERROR` in the Status field. If the value of Status field is `SUCCESS`, this field contains a null character string. When `Connection failed` is displayed: Connection failed. When `Authorization failed` is displayed: Authentication failed. When `Response invalid` is displayed: An unexpected response was received from the server. When `Collection error` is displayed**:** A collection error occurred. When `Collection timeout` is displayed: A collection timeout occurred. When `Invalid environment(SSH_Client)` is displayed: The file specified in `SSH_Client` when the instance environment was set up does not exist (when the PFM - RM host is running Windows and the monitored host is running UNIX). When `Invalid environment(Perl_Module)` is displayed: The file specified in `Perl_Module` when the instance environment was set up does not exist (when the PFM - RM host is running Windows and the monitored host is running UNIX). When `Invalid environment(Private_Key_File)` is displayed: The file specified in `Private_Key_File` when the monitored host was set up does not exist (when the PFM - RM host is running Windows and the monitored host is running UNIX).
Status	Connection status.

Field name	Description
Status	When `SUCCESS` is displayed: Execution is underway. When `ERROR` is displayed: Connection failed.
Target Host Time	Time the performance data was collected on the monitored host
Version	OS version of the monitored host

7 Records

This chapter describes the records for PFM - RM for Platform. For details about how to collect performance data for each record, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide* or the chapter that describes the management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

Data model

The records and fields of PFM - RM for Platform are referred to collectively as a *data model*. A specific version number is assigned to the data model for PFM - RM for Platform.

For details about the relationship between the PFM - RM for Platform version and the data model version, see *H. Version Compatibility*.

To check the data model version of your PFM - RM for Platform, use the Properties window of PFM - Web Console. To open the Properties window, on the **Agents** page of PFM - Web Console, click the agent icon, and then click the **Properties** method.

For details about the data model, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Format of record explanations

The records for PFM - RM for Platform are described in this chapter in alphabetical order.

Each record explanation contains the following subsections:

Function

Provides an overview of the performance data that is stored in the record and includes important information that should be noted.

Default and changeable values

Consists of a table of the default values for the performance data collection conditions that are defined for the record, and indicates whether each value can be changed by the user.

The table below lists and describes the items that are presented in *Default and changeable values*. For details about each item described in this table, see the chapter that describes the management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

Table 7–1: Default and changeable values (record)

Item	Description	Changeable
`Collection Interval`	Performance data collection interval (in seconds)	`Y`: Changeable `N`: Not changeable
`Collection Offset`#1	Delay (offset value) for starting performance data collection (in seconds). For details about the offset value, see the chapter that describes the management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*. For details about the performance data collection start time, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.	
`Log`	Whether collected performance data is stored in the Store database: `Yes`: Stored. However, if `Collection Interval=0` is set, no collected performance data is stored. `No`: Not stored.	
`LOGIF`	Conditions for storing collected performance data in the Store database	
`Sync Collection With`#2	Whether performance data is to be collected along with the record displayed in the `Description` record property. For details, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.	
`Over 10 Sec Collection Time`#3	Whether record collection takes 10 seconds or longer `Yes`: Record collection sometimes takes 10 seconds or longer. `No`: Record collection takes less than 10 seconds.	

#1

The value must be in the range from 0 to 32,767 seconds (but within the collection interval specified in `Collection Interval`). This value is used to distribute the workload of collection processing so as to avoid concentration of the workload when multiple data items are

collected. Note that the recording time for data collection is the same as for `Collection Interval` regardless of the `Collection Offset` value.

To change the `Collection Offset` value, specify an appropriate value taking into account the workload of collection processing.

#2

When `Sync Collection With` is displayed, `Collection Interval` and `Collection Offset` are not displayed.

#3

This item is displayed when historical data collection takes priority over real-time report display processing. For details, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

ODBC key field

Indicates the ODBC key field that is required in order that the record data stored in the Store database can be used by SQL statements with PFM - Manager. Some ODBC key fields are common to all records, and some are specific to individual records. This section presents the ODBC key field that is specific to each record. Note that only multi-instance records have a specific ODBC key field.

For details about the ODBC key fields common to all records, see *List of ODBC key fields*. For details about how to use the ODBC key fields, see the chapter that describes linkage to an ODBC-compatible application program in the *Job Management Partner 1/Performance Management User's Guide*.

Lifetime

Indicates the period during which consistency is guaranteed for the performance data that is collected in the record.

For details about the lifetime, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Record size

Indicates the amount of performance data that can be collected and stored in the record during a single collection operation.

Fields

Provides a table that describes the record's fields. The table contains the following columns:

PFM - View name (PFM - Manager name)

PFM - View name

Indicates the field name (PFM - View name) that is displayed with PFM - Web Console.

PFM - Manager name

Indicates the field name (PFM - Manager name) to be specified in SQL statements when statements are used from PFM - Manager to access the field data stored in the Store database.

Specify the record ID at the beginning of an SQL statement. For example, to specify the Polling Time (`POLLING_TIME`) field of the System Status (`PD`) record, specify `PD_POLLING_TIME`.

Description

Describes the performance data that is stored in each field.

The performance data in each field can be obtained in the following ways:

- Obtaining an average or a rate from the current data and the data collected during the previous interval
- Obtaining by using only the current data that has been collected

- Obtaining from the data in other fields

The value obtained at the set data collection interval is used, unless indicated otherwise.

When records of the PI record type are summarized for a historical report with a value other than *minute* specified as the reporting interval, the following types of values can be displayed:

- Average value over the summarized intervals
- Last value collected
- Total value
- Minimum value
- Maximum value

A displayed field value is the average value over the summarized intervals, unless indicated otherwise.

Summary rule

Indicates the summarization method used by Remote Monitor Store to summarize the data. This summarization method is referred to as the *summary rules*. For summarization rules, see *Summarization rules*.

Grouping rule

Indicates the method for consolidating performance information for remote agents that belong to the same instance. This summarization method is referred to as the *grouping rules*. For grouping rules, see *Grouping rules*.

Format

Indicates the data type of the field's value. For data types, see *List of data types*.

Delta

Indicates whether the value is a delta value. In contrast to data collected as a cumulative value, data expressed by the amount the value has changed is called a *delta*. For details about deltas, see *Field values*.

Unsupported

Indicates the OSs of the monitored host that do not support use of the field.

List of ODBC key fields

Some ODBC key fields are common to all records, and some are specific to individual records. This section presents the ODBC key fields common to all records. With PFM - Manager, ODBC key fields are required in order for you to use SQL statements to access record data stored in the Storage database.

The table below lists the ODBC key fields that are common to all records. For details about the ODBC key fields specific to individual records, see the details for each record.

Table 7–2: List of ODBC key fields common to all records

ODBC key field	ODBC format	Data	Description
*record-ID*_DATE	SQL_INTEGER	Internal	Key in the record that indicates the record creation date
*record-ID*_DATETIME	SQL_INTEGER	Internal	Combination of the *record-ID*_DATE and *record-ID*_TIME fields
*record-ID*_DEVICEID	SQL_VARCHAR	Internal	Indicates one of the following: • *instance-name*[*monitored-host -name*@*PFM-RM-host-name*] • *instance-name*[all@*PFM-RM-host-name*]
*record-ID*_DRAWER_TYPE	SQL_VARCHAR	Internal	Type. Valid values are as follows: • m: Minute • H: Hour • D: Day • W: Week • M: Month • Y: Year
*record-ID*_PROD_INST	SQL_VARCHAR	Internal	Instance name of PFM - RM for Platform
*record-ID*_PRODID	SQL_VARCHAR	Internal	Product ID of PFM - RM for Platform
*record-ID*_RECORD_TYPE	SQL_VARCHAR	Internal	Identifier indicating the record type (4 bytes)
*record-ID*_TIME	SQL_INTEGER	Internal	Record creation time (Greenwich mean time)

Summarization rules

For records of the PI record type, the data that is collected is stored in the Store database. This includes data collected at the interval set in `Collection Interval`, as well as data that is collected on a specific interval basis derived from defined rules (such as minute, hour, day, week, month, or year). The type of summarization is defined for each field; this definition is referred to as the *summary rules*.

Some summary rules require intermediate data to be retained during the summarization period. In such a case, a field for retaining the intermediate data is added to the record in the Store database; this is called an *added field*. Some added fields are displayed as record fields in PFM - Web Console. These added fields that are displayed in PFM - Web Console can be used as fields for display in historical reports.

As distinguished from the *added fields* that are created by summarization, the fields described in each record explanation are called *fixed fields*.

The name of an added field is as follows:

- Name of an added field that is stored in the Store database
  PFM - Manager name of the fixed field with a suffix
- Name of an added field that is displayed in PFM - Web Console
  PFM - View name of the fixed field with a suffix

The following table lists the suffixes for the PFM - Manager name, the suffixes for the corresponding PFM - View name, and the data that is stored in each field.

Table 7–3: List of suffixes for added fields

Suffix for PFM - Manager name	Suffix for PFM - View name	Stored data
`_TOTAL`	`(Total)`	Sum of the field's value in the records over the summary period
`_COUNT`	--	Number of records collected during the summary period
`_HI`	`(Max)`	Maximum field value in the records over the summary period
`_LO`	`(Min)`	Minimum field value in the records over the summary period

Legend:
--: There is no added field.

The following table lists and describes the summary rules.

Table 7–4: List of summary rules

Summary rule name	Description of summary rule
`COPY`	Stores the field value in the most recent record in the summary period.
`AVG`	Stores the average field value in the summary period. The formula is as follows: (*Sum-of-field-values*)/(*number-of-collected-records*) Added fields (Store database): • `_TOTAL` • `_COUNT` Added field (PFM - Web Console): • `(Total)`

Summary rule name	Description of summary rule
HILO	Stores the maximum, minimum, and average field values in the summary period. In the fixed field, the average value is stored. The formula is as follows: (*Sum-of-field-values*)/(*number-of-collected-records*) Added fields (Store database): • _HI • _LO • _TOTAL • _COUNT Added fields (PFM - Web Console): • (Max) • (Min) • (Total)
--	Indicates that data is not summarized.

Grouping rules

Performance data for the monitored hosts in the same instance environment is summarized as the data for the group agent based on predefined rules. This definition is referred to as the *grouping rules*.

The following table lists the grouping rules.

Table 7–5: List of grouping rules

Grouping rule name	Description of grouping rule
`ADD`	Stores the sum of all the performance data for the monitored hosts in the same instance environment.
`AVG`	Stores the average value of the performance data for the monitored hosts in the same instance environment.
`COPY`	Stores the value of specific performance data in all the performance data for the monitored hosts in the same instance environment.
`FIXED`	Stores a specific value regardless of the performance data.

List of data types

The table below lists the data types of the field values, together with their corresponding C and C++ data types. The values shown in the *Field* column under *Data type* are those shown in the *Format* column of the record field tables.

Table 7–6: List of data types

Data type		Size (bytes)	Description
Field	C and C++		
`char(n)`	`char()`	1	Character data (from 0x20 to 0x7e)
`double`	`double`	8	Numeric value (1.7E ± 308 (15 digits))
`long`	`long`	4	Numeric value (from -2,147,483,648 to 2,147,483,647)
`short`	`short`	2	Numeric value (from -32,768 to 32,767)
`string(n)`	`char[]`	Value in parentheses	Character string with a length of *n* bytes. The last character is the null.
`time_t`	`unsigned long`	4	Numeric value (from 0 to 4,294,967,295)
`timeval`	`struct`	8	Numeric value (the first 4 bytes are the seconds, the next 4 bytes are the microseconds)
`ulong`	`unsigned long`	4	Numeric value (from 0 to 4,294,967,295)
`ushort`	`unsigned short`	2	Numeric value (from 0 to 65,535)
`utime`	`struct`	8	Numeric value (the first 4 bytes are the seconds, the next 4 bytes are the microseconds)
`word`	`unsigned short`	2	Numeric value (from 0 to 65,535)
(Not applicable)	`unsigned char`	1	Numeric value (from 0 to 255)

Field values

This section describes the values stored in the fields.

For details about the source of data to be stored in the individual fields and the computation method (data sources), see *J. Data Sources of Records*.

Delta

In contrast to data collected as a cumulative value, a so-called *delta* value is data that indicates the amount by which the collection value has changed. For example, if the performance data value obtained during the first collection was `3` and the performance data value obtained during the second collection is `4`, then the cumulative value is `7` but the change in the collected value is `1`. In the tables, the *Delta* column indicates whether each field's value is a delta value. The performance data collected by PFM - RM for Platform varies as shown in the table below.

Note that the delta value can be a negative because it is a value relative to the previous data.

Table 7–7: Performance data collected by PFM - RM for Platform

Record type	Delta	Performance data referencing method	Indicate delta value#	Performance data value
PI record type	Yes	• Real-time report	Selected	The displayed value is the change amount.
			Not selected	The displayed value is the change amount.
		• Historical report • Alarm evaluation	--	The displayed value is the change amount.
	No	• Real-time report	Selected	The displayed value is the actual value at the time of data collection.
			Not selected	The displayed value is the actual value at the time of data collection.
		• Historical report • Alarm evaluation	--	The displayed value is the actual value at the time of data collection.
PD record type	Yes	• Real-time report	Selected	The displayed value is the change amount.
			Not selected	The displayed value is the cumulative value.
		• Historical report • Alarm evaluation	--	The displayed value is the cumulative value.
	No	• Real-time report	Selected	The displayed value is the actual value at the time of data collection.
			Not selected	The displayed value is the actual value at the time of data collection.
		• Historical report • Alarm evaluation	--	The displayed value is the actual value at the time of data collection.

Legend:

--: Not applicable because the item is not displayed.

#

Indicates whether one of the following items is selected in the check boxes for real-time report settings in PFM - Web Console:

- **Indicate delta value** in the report wizard's Edit > Indication Settings(Realtime) window
- **Indicate delta value** in **Indication Settings(Realtime)** on the **Properties** page in the Report window.

Notes about performance data collection

The following notes apply to collection of performance data:

- For a record of the PI record type to be stored, performance data must be collected at least twice.

  For the records of the PI record type, performance data is collected at the interval set by PFM - Web Console. However, no collected performance data is stored in the Store database at the time the performance data collection setting is executed in PFM - Web Console.

  Because historical data for records of the PI record type contains data (delta value) that requires a difference from the previously collected data, data obtained by two collections is required. Therefore, a maximum of twice the set time is required before historical data can be stored in the Store database.

  For example, if 300 seconds (5 minutes) is set as the performance data collection interval at 18:32 in PFM - Web Console, the first data collection will begin at 18:35. The next data collection will begin at 18:40. Historical data will be created from the data collected at 18:35 and 18:40; this historical data will be stored in the Store database at 18:40 (8 minutes after 18:32 when the settings were specified).
- In real-time reports, values are displayed from the first time data is collected. If a report requires initial data, 0 will be displayed as the initial value. For the second and subsequent data collections, the operation depends on the report.
- In the following cases, the value of the collected data is displayed after the second data collection:
  - **Indicate delta value** is not selected in the real-time report settings for records of the PI record type.
  - **Indicate delta value** is selected in the real-time report settings for records of the PD record type.
- In the following case, the difference between the first and second data is displayed at the time of the second data collection, and the value of the collected data is displayed at the time of the third and subsequent collections:
  - **Indicate delta value** is selected in the real-time report settings for records of the PI record type.
- If the monitoring target's channel is restarted when PFM - RM for Platform starts, the value of collected data might become negative. For the second and subsequent data that is collected, a positive value will be displayed as the difference between the data.

Fields that are added only when a record is recorded in the Store database

The following table lists the fields that are added only when data is recorded in the Store database.

Table 7–8: Fields that are added only when a record is recorded in the Store database

PFM - View name (PFM - Manager name)	Description	Format	Delta	Supported version
Agent Host (DEVICEID)	Identifier including the name of the host where PFM - RM for Platform is running	string (256)	No	All
Agent Instance (PROD_INST)	Instance name of PFM - RM for Platform	string (256)	No	All
Agent Type (PRODID)	Product ID of PFM - RM for Platform, expressed as a 1-byte identifier	char	No	All
Date (DATE)	Record creation date, in GMT (Greenwich Mean Time)[#1, #2]	char (3)	No	All
Date and Time (DATETIME)	Combination of the Date (DATE) and Time (TIME) fields[#2]	char (6)	No	All
Drawer Type (DRAWER_TYPE)	For a record of the PI record type, the data summarization type. The type displayed in PFM - Web Console reports differs from the type displayed using the ODBC driver.[#3]	char	No	All
GMT Offset (GMT_ADJUST)	Difference (in seconds) between Greenwich Mean Time and local time	long	No	All
Time (TIME)	Record creation time in GMT (Greenwich Mean Time)[#1, #2]	char (3)	No	All

#1

A relative time during summarization is set because data is summarized for records of the PI record type. The following table shows the setting for each record type:

Table 7–9: Setting for each record type

Type	Setting for each record type
Minute	At the 0 second of the time when the record was created.
Hour	At the 0 minute and 0 second of the time when the record was created.
Day	At 00:00:00 of the day when the record was created.
Week	At 00:00:00 on Monday of the week when the record was created.
Month	At 00:00:00 on the first of the month when the record was created.
Year	At 00:00:00 on January 1st of the year when the record was created.

#2

When data is displayed in reports and by the ODBC driver, the Date field is displayed in the format *YYYYMMDD*, the Date and Time field is displayed in the format *YYYYMMDD hh*:*mm*:*ss*, and the Time field is displayed in the format *hh*:*mm*:*ss*.

#3

The following table shows the summary type displayed in PFM - Web Console reports and the type displayed when the ODBC driver is used.

Table 7–10: Differences in summary type depending on the display method

Type	PFM - Web Console	ODBC driver
Minute	Minute	m
Hour	Hour	H
Day	Day	D
Week	Week	W
Month	Month	M
Year	Year	Y

Notes on records

This section provides notes about record collection.

Notes about preparing for collection of performance data

The following point should be noted before you collect performance data:

Changing registry

This note is applicable to Windows.

PFM - RM for Platform supports operation in an environment that is set up by the OS-provided standard method.

If you use special OS settings, such as by using a registry editor to directly edit registry information, performance data might not be collected correctly even if such customization is disclosed in the Microsoft technical support information.

Collecting historical data

For each record, PFM - RM for Platform stores historical data for all monitoring targets in an instance, or historical data summarized for each group agent, in the same data file. The maximum size limit for each data file is 2 gigabytes. Therefore, if an instance contains many monitoring targets or if a record contains many instances, it might not be possible to store all of the historical data in the Store database.

Of all the data collected, the historical data summarized for each group agent might cause a data file space shortage. Therefore, when using a group agent for monitoring, we recommend that you use real-time monitoring rather than monitoring based on historical data.

If you monitor based on history, you need to reduce the number of monitoring targets in the instance to prevent the data file size from exceeding 2 gigabytes, or use the `LOGIF` property to reduce the amount of data that is to be stored in the Store database.

For details about how to estimate the disk space that the Store database will occupy, see *A. Estimating System Requirements*.

Notes about identifying record instances

The following note is about identifying record instances.

When instances are not identified uniquely

This note applies only when the monitored host is running Windows.

PFM - RM for Platform collects performance data by referencing the most recent information at specific intervals. If PFM - RM for Platform cannot identify the record instance uniquely from the information acquired from the OS, it adds a number in the format #*n* (*n*: `1`, `2`, `3`, ...) at the end of the following field:

Record name	Field name
Network Interface Overview (`PI_NET`)	Interface (`INTERFACE`)

Notes about changing the system resources for the monitored host

The following note concerns changing the system resources for the monitored host.

Performance data before and after system resources are changed

When you change system resources for the monitored host, continuity between the performance data collected before and after the change is lost. Therefore, the performance data before and after the change must be handled as different sets of performance data.

Notes about records

Data values in a record whose instance name is `_Total`

The total and average values of all instances are collected as data values in the record whose instance name is indicated as `_Total` among all multi-instance records. If the instance environment is changed during the collection interval, values might not match.

Value exceeding the data type defined in the data model

PFM - RM for Platform does not support a value that is outside the permissible range for the data type defined in the data model. If a value exceeding the data type defined in the data model is collected, the values that are displayed might not be accurate.

When records are not created

If PFM - RM for Platform cannot collect the performance data for the field that is defined as the ODBC key field, no record is created.

Fields for which performance data is not collected during the first collection

Non-PD records contain fields for which performance data is not collected during the first collection. For these fields, performance data is collected during the second and subsequent collections.

When accurate performance data cannot be collected because of an action specific to the virtualization facility

You might not be able to collect accurate performance data due to an action specific to the virtualization facility, such as a time jump.

When accurate performance data cannot be collected from an AIX monitored host

If the instance settings of PFM - RM for Platform satisfy all of the following conditions, you might not be able to collect accurate performance information:

- An AIX host is set for the monitored host.
- The `iostat` kernel parameter of the monitored host is set to `false`.
- The `sar` command was executed on the monitored host.
- The `Std_Category` or `Disk_Category` property of the instance is set to `Y`.

When PFM - Agent for Platform is running on the monitored host, you might not be able to collect accurate performance information if the instance settings satisfy all of the following conditions:

- An AIX host is set for the monitored host.
- The `iostat` kernel parameter of the monitored host is set to `false`.
- The `Agent Configuration - sar Command Monitoring` property of PFM - Agent for Platform running on the monitored host is set to `Y`.
- The `Std_Category` or `Disk_Category` property of the instance is set to `Y`.

If the `Std_Category` property is set to `Y`, you might not be able to collect CPU-related performance information. If the `Disk_Category` property is set to `Y`, you might not be able to collect disk-related performance information.

When accurate performance data cannot be collected because of a change in the disk device

If the disk device indicated by the disk device name is changed by a change to the system, for example, continuity is lost in the performance information captured after the change to the system, even if the disk device name remains the same.

When accurate performance data cannot be collected because of the state of the mounted remote file system

Only operate PFM - RM for Platform when the information in the mounted remote file system can be referenced (the state in which the `df` command can be executed normally). If the `Disk_Category` property of the instance is set to `Y` while the mounted remote file system is not responding, the Remote Agent service cannot collect correct

performance data. For details about how to recover from this state, see *9.2.5(3) PFM - RM for Platform was started, but no performance data is being collected*.

List of records

The following table lists and describes the records that can be collected by PFM - RM for Platform and the information that is stored in each record.

Table 7–11: List of records

Category	Record name	Record ID	Information stored in record
Process	Application Process Count	PD_APPC	Performance data that summarizes, at a given point in time, the records stored in the Application Process Overview (PD_APS) and Application Service Overview (PD_ASVC) records for each of the processes and services being monitored on a per-application basis
	Application Process Detail	PD_APPD	Performance data that summarizes, at a given point in time, the records stored in the Application Process Overview (PD_APS) and Application Service Overview (PD_ASVC) records for each of the processes and services being monitored on a per-application basis. Provides more detailed performance data than the Application Process Count (PD_APPC) record.
	Application Process Overview	PD_APS	Performance data indicating the status of a process of the monitored host at a given point in time
	Application Service Overview	PD_ASVC	Performance data indicating the status, at a given point in time, of an application service such as the Win32 process registered in the service control manager (SCM) of the monitored host
	Application Summary	PD_APP2	Performance data that summarizes, at a given point in time, the records stored in the Application Process Overview (PD_APS) and Application Service Overview (PD_ASVC) records on a per-application basis
Disk	Logical Disk Overview	PI_LDSK	Performance data, taken at a specific interval, about the capacity of a logical disk at the monitored host
	Physical Disk Overview	PI_PDSK	Performance data, taken at a specific interval, about physical disks on the monitored host
Network	Network Interface Overview	PI_NET	Performance data, taken at a specific interval, about the network interface for the monitored host
Processor	Processor Overview	PI_CPU	Performance data, taken at a specific interval, about the processors on the monitored host
System	System Status	PD	Status of the connection to the monitored host and information about the OS of the monitored host at a specific time
	System Summary	PI	Performance data, taken at a specific interval, about the processors and memory in the entire system of the monitored host

Application Process Count (PD_APPC)

Function

The Application Process Count (PD_APPC) record stores performance data that summarizes, at a given point in time, the records stored in the Application Process Overview (PD_APS) and Application Service Overview (PD_ASVC) records for each of the processes and services being monitored on a per-application basis. This record is a multi-instance record.

Notes

- Information cannot be collected if connection to the monitored host fails.
- To change the application definition, you must change the setting from PFM - Web Console.

Default and changeable values

Item	Default value	Changeable
Sync Collection With	Detail Records ,APP2	N
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PD_APPC_APPLICATION_NAME

PD_APPC_MONITORING_NUMBER

Lifetime

From the time a condition is added in PFM - Web Console until the time the condition is deleted

Record size

- Fixed part: 1,034 bytes
- Variable part: 135 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	Record name. Always APPC	--	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created	--	COPY	time_t	No	--
Interval (INTERVAL)	Always 0	--	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host	--	COPY	string (256)	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Target Host (TARGET_HOST)	Monitored host name	--	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time the performance information was collected on the PFM - RM host	--	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time the performance information was collected on the monitored host	--	FIXED	string (32)	No	--
Application Name (APPLICATION_NAME)	Application definition name specified during process monitoring setup	--	COPY	string (64)	No	--
Monitoring Number (MONITORING_NUMBER)	Monitoring condition number	--	COPY	word	No	--
Monitoring Label (MONITORING_LABEL)	Name for identifying a specific monitoring condition	--	FIXED	string (32)	No	--
Monitoring Min (MONITORING_MIN)	Minimum monitoring count	--	ADD	ulong	No	--
Monitoring Max (MONITORING_MAX)	Maximum monitoring count	--	ADD	ulong	No	--
Monitoring Count (MONITORING_COUNT)	Number of running processes and services that match the monitoring condition	--	ADD	ulong	No	--
Monitoring Status (MONITORING_STATUS)	Conditional result of the monitoring count NORMAL: No problem ABNORMAL: Abnormal	--	FIXED	string (9)	No	--
Ext1 (EXT1)#	Extension field 1	--	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	--	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts (or there is no applicable summary rule).

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Application Process Detail (PD_APPD)

Function

The Application Process Detail (PD_APPD) record stores performance data that summarizes, at a given point in time, the records stored in the Application Process Overview (PD_APS) and Application Service Overview (PD_ASVC) records for each of the processes and services being monitored on a per-application basis. Provides more detailed performance data than the Application Process Count (PD_APPC) record. This record is a multi-instance record.

Notes

- Information cannot be collected if connection to the monitored host fails.
- To change the application definition, you must change the setting from PFM - Web Console.
- This record can be used in real-time reports only. If you try to display this record in a historical report, the error KAVJS5001-I occurs.

Default and changeable values

Item	Default value	Changeable
Sync Collection With	Detail Records , APP2	N
Log	No	N
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PD_APPD_APPLICATION_NAME

PD_APPD_MONITORING_NUMBER

Lifetime

From the time a condition is added in PFM - Web Console until the time the condition is deleted

Record size

- Fixed part: 1,034 bytes
- Variable part: 279 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	Record name. Always APPD	--	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created	--	COPY	time_t	No	--
Interval (INTERVAL)	Always 0	--	FIXED	ulong	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
VA DeviceID (VADEVICEID)	Device ID of the monitored host	--	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Monitored host name	--	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time the performance information was collected on the PFM - RM host	--	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time the performance information was collected on the monitored host	--	FIXED	string (32)	No	--
Application Name (APPLICATION_NAME)	Application definition name specified during process monitoring setup	--	COPY	string (64)	No	--
Monitoring Number (MONITORING_NUMBER)	Monitoring condition number	--	COPY	word	No	--
Monitoring Label (MONITORING_LABEL)	Name for identifying a specific monitoring condition	--	FIXED	string (32)	No	--
Monitoring Condition (MONITORING_CONDITION)	Conditional expression for identifying a specific process or service to be monitored	--	FIXED	string (128)	No	--
Monitoring Field (MONITORING_FIELD)	Field to be monitored	--	FIXED	string (16)	No	--
Monitoring Min (MONITORING_MIN)	Minimum monitoring count	--	ADD	ulong	No	--
Monitoring Max (MONITORING_MAX)	Maximum monitoring count	--	ADD	ulong	No	--
Monitoring Count (MONITORING_COUNT)	Number of running processes and services that match the monitoring condition	--	ADD	ulong	No	--
Monitoring Status (MONITORING_STATUS)	Conditional result of the monitoring count NORMAL: No problem ABNORMAL: Abnormal	--	FIXED	string (9)	No	--
Ext1 (EXT1)#	Extension field 1	--	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	--	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts (or there is no applicable summary rule).

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Application Process Overview (PD_APS)

Function

The Application Process Overview (PD_APS) record stores performance data indicating the status of a process of the monitored host at a given point in time. This record is a multi-instance record.

Notes

- Information cannot be collected if connection to the monitored host fails.
- Each process indicates a program being executed during collection.
- This record can be used in real-time reports only. If you try to display this record in a historical report, the error KAVJS5001-I occurs.
- Any character in the information to be acquired that is not in the ASCII character set range of 0x20 to 0x7E will be converted to a hash mark (#: 0x23) before it is stored in the Program Name (PROGRAM_NAME), Command Line (COMMAND_LINE), and Virtual Env ID (VIRTUAL_ENV_ID) fields. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter A is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

- The value in the Command Line (COMMAND_LINE) field might end in a space. Therefore, when defining a conditional expression for alarms or specifying the collection of process operation status information, note whether the value ends in a space.
- When the OS of the monitored host is Windows, the value in the Program Name (PROGRAM_NAME) field corresponds to the value displayed in the **Image Name** column when the **Processes** tab of Windows Task Manager is clicked.
- When the OS of the monitored host is Windows, the entire value in the Command Line (COMMAND_LINE) field might be enclosed in double quotation marks ("). When using the value in the Command Line (COMMAND_LINE) field to define a conditional expression for alarm, you must replace the double quotation marks (") with single-byte asterisks (*). For details about how to define a conditional expression for alarms, see the chapter that describes operation monitoring using an alarm in the *Job Management Partner 1/Performance Management User's Guide*.
- When the OS of the monitored host is a UNIX environment, the values in the Program Name (PROGRAM_NAME) and Command Line (COMMAND_LINE) fields correspond to the values displayed in the COMMAND column when the following ps command is executed with C specified in the LANG environment variable:
  - In AIX: ps -A -X -o comm,args
  - In HP-UX: UNIX95=1 ps -A -o comm,args
  - In Linux: ps -e -o comm,args
  - In Solaris: ps -e -o fname,args

  The first COMMAND column is stored in the Program Name (PROGRAM_NAME) field and the second COMMAND column is stored in the Command Line (COMMAND_LINE) field. Note that the value displayed in COMMAND column differs depending on the OS.

- When the OS of the monitored host is a UNIX environment, the value in the Terminal (TERMINAL) field corresponds to the value displayed in the TTY (TT) column when the ps command is executed. The displayed value differs depending on the OS.
- When the OS of the monitored host is a UNIX environment, the Virtual Env ID (VIRTUAL_ENV_ID) field displays a value only if the OS of the monitored host is AIX6.1 or later or Solaris10 or later. Nothing is displayed for other OSs.
- When the OS of the monitored host is a UNIX environment, n/a is displayed in the Terminal (TERMINAL) field for zombie processes.
- When the OS of the monitored host is the Workload Partition (WPAR) environment of AIX V6.1 or later, the Virtual Env ID (VIRTUAL_ENV_ID) field displays Global or global.

Default and changeable values

Item	Default value	Changeable
Sync Collection With	Detail Records,APP2	N
Log	No	N
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PD_APS_PID

PD_APS_PROGRAM_NAME

Lifetime

From process execution to termination

Record size

- Fixed part: 1,034 bytes
- Variable part: 4,500 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	Record name. Always APS	--	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created	--	COPY	time_t	No	--
Interval (INTERVAL)	Always 0	--	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host	--	COPY	string (256)	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Target Host (TARGET_HOST)	Monitored host name	--	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time the performance information was collected on the PFM - RM host	--	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time the performance information was collected on the monitored host	--	FIXED	string (32)	No	--
PID (PID)	Process ID	--	COPY	ulong	No	--
Program Name (PROGRAM_NAME)	Program name	--	COPY	string (257)	No	--
Parent PID (PARENT_PID)	Process ID of a parent process	--	FIXED	ulong	No	--
Command Line (COMMAND_LINE)	Command line	--	FIXED	string (4097)	No	--
Terminal (TERMINAL)	Name of the terminal on which the process was executed	--	FIXED	string (40)	No	Windows
Elapsed Time (ELAPSED_TIME)	Time elapsed since the process started	--	FIXED	utime	No	--
State (STATE)	Program status. One of the following values is set: In AIX: IDLE, ZOMBIE, STOP, RUN, SWAP, or NONE In HP-UX: IDLE, OTHER, RUN, SLEEP, STOP, ZOMBIE, or NONE In Solaris: ONCPU, RUN, SLEEP, STOP, ZOMBIE, or NONE In Linux: RUN, SLEEP, SWAP, STOP, ZOMBIE, or NONE	--	FIXED	string (10)	No	Windows
Virtual Env ID (VIRTUAL_ENV_ID)	Identifier of the virtualization environment created by the OS's virtualization system	--	FIXED	string (64)	No	Windows, HP-UX, Linux
Ext1 (EXT1)#	Extension field 1	--	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	--	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts (or there is no applicable summary rule).

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Application Service Overview (PD_ASVC)

Function

The Application Service Overview (PD_ASVC) record stores performance data indicating the status, at a given point in time, of an application service such as the Win32 process registered in the service control manager (SCM) of the monitored host. This record is a multi-instance record.

Notes

- Information cannot be collected if connection to the monitored host fails.
- This record is not created when the OS of the monitored host is UNIX.
- This record can be used in real-time reports only. If you try to display this record in a historical report, the error KAVJS5001-I occurs.
- Any character in the information to be acquired that is not in the ASCII character set range of 0x20 to 0x7E will be converted to a hash mark (#: 0x23) before it is stored in the Service Name (SERVICE_NAME) and Display Name (DISPLAY_NAME) fields. Note that multi-byte characters are processed in single-byte units during conversion. For example, the multi-byte (full-width) letter Ａ is converted as follows:

Information to be acquired		Information after conversion	
Character encoding	Binary	Binary	Character string
Shift-JIS	8260	2360	#`
EUC	A3C1	2323	##
UTF-8	EFBCA1	232323	###

- The value in the Service Name (SERVICE_NAME) field corresponds to the value displayed in **Service Name** when a service property is opened in the service control manager (SCM).
- The value in the Display Name (DISPLAY_NAME) field corresponds to the value displayed in **Displayed Service Name** when a service property is opened in the service control manager (SCM).

Default and changeable values

Item	Default value	Changeable
Sync Collection With	Detail Records,APP2	N
Log	No	N
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PD_ASVC_SERVICE_NAME

Lifetime

From service installation to uninstallation

Record size

- Fixed part: 1,034 bytes
- Variable part: 570 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	Record name. Always ASVC	--	COPY	char (8)	No	UNIX
Record Time (RECORD_TIME)	Time when the record was created	--	COPY	time_t	No	UNIX
Interval (INTERVAL)	Always 0	--	FIXED	ulong	No	UNIX
VA DeviceID (VADEVICEID)	Device ID of the monitored host	--	COPY	string (256)	No	UNIX
Target Host (TARGET_HOST)	Monitored host name	--	FIXED	string (33)	No	UNIX
Polling Time (POLLING_TIME)	Time the performance information was collected on the PFM - RM host	--	FIXED	string (32)	No	UNIX
Target Host Time (TARGET_HOST_TIME)	Time the performance information was collected on the monitored host	--	FIXED	string (32)	No	UNIX
Service Name (SERVICE_NAME)	Service name used in the service control manager database	--	COPY	string (257)	No	UNIX
Service Exit Code (SERVICE_EXIT_CODE)	Error code specific to each service. A value is set only when the value in the Win32 Exit Code field is 1066 (ERROR_SERVICE_SPECIFIC_ERROR).	--	FIXED	long	No	UNIX
Win32 Exit Code (WIN32_EXIT_CODE)	Service-related Windows error code	--	FIXED	long	No	UNIX
Display Name (DISPLAY_NAME)	Name used by the user interface program to identify a specific service	--	FIXED	string (257)	No	UNIX
State (STATE)	Service status at the time of data collection. One of the following values is set in this field: Continue Pending: Stop processing is in progress after the Restart button is pressed following a pause. Pause Pending: Pausing process is in progress. Paused: Paused state Running: Running state Start Pending: Start processing is in progress. Stop Pending: Stop processing is in progress.	--	FIXED	string (32)	No	UNIX

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
State (STATE)	Stopped: Stopped state Unknown: Unknown state	--	FIXED	string (32)	No	UNIX
Ext1 (EXT1)#	Extension field 1	--	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	--	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts (or there is no applicable summary rule).

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Application Summary (PD_APP2)

Function

Application Summary (PD_APP2) record stores performance data that summarizes, at a given point in time, the information stored in the Application Process Overview (PD_APS) and Application Service Overview (PD_ASVC) records on a per-application basis. This record is a multi-instance record.

Notes

- Information cannot be collected if connection to the monitored host fails.
- To change the application definition, you must change the setting from PFM - Web Console.

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PD_APP2_APPLICATION_NAME

Lifetime

From the time a condition is added in PFM - Web Console until the time the condition is deleted

Record size

- Fixed part: 1,034 bytes
- Variable part: 168 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	Record name. Always APP2	--	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created	--	COPY	time_t	No	--
Interval (INTERVAL)	Always 0	--	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host	--	COPY	string (256)	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Target Host (TARGET_HOST)	Monitored host name	--	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time the performance information was collected on the PFM - RM host	--	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time the performance information was collected on the monitored host	--	FIXED	string (32)	No	--
Application Name (APPLICATION_NAME)	Application definition name specified during process monitoring setup	--	COPY	string (64)	No	--
Application Status (APPLICATION_STATUS)	Status of the application specified during process monitoring setup. The application status is the result obtained based on the statuses of the processes and services specified as monitoring targets. To check the statuses of the processes and services specified as monitoring targets, see the Monitoring Status displayed in the Application Process Count (PD_APPC) and Application Process Detail (PD_APPD) records. NORMAL: All monitoring targets are normal. ABNORMAL: One or more of the monitoring targets is abnormal. UNKNOWN: Collection of information from the OS failed.	--	FIXED	string (10)	No	--
Application Exist (APPLICATION_EXIST)	Status of the application specified during process monitoring setup. The application status is the result obtained based on the statuses of the processes and services specified as monitoring targets. To check the statuses of the processes and services specified as monitoring targets, see the Monitoring Status displayed in the Application Process Count (PD_APPC) and Application Process Detail (PD_APPD) records. NORMAL: One or more of the monitoring targets is normal. ABNORMAL: All monitoring targets are abnormal. UNKNOWN: Collection of information from the OS failed.	--	FIXED	string (10)	No	--
Virtual Env ID (VIRTUAL_ENV_ID)	Identifier of the virtualization environment created by the virtualization system provided by the OS	--	FIXED	string (64)	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Case Sensitive (CASE_SENSITIVE)	Case-sensitive or not Yes: Case-sensitive No: Not case-sensitive	--	FIXED	string (4)	No	--
Ext1 (EXT1)#	Extension field 1	--	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	--	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts (or there is no applicable summary rule).

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Logical Disk Overview (PI_LDSK)

Function

The Logical Disk Overview (PI_LDSK) record stores performance data, taken at a specific interval, about the capacity of a logical disk at the monitored host. This is a multi-instance record.

Notes

- If the connection to the monitored host fails, the information cannot be collected.
- If you collect this record in a Windows environment, note the following:
  - This record collects performance information for hard disk drives and fixed disk drives. Performance information for other devices (such as network disks) cannot be monitored.
  - If a disk volume corresponding to the ID (ID) field is not accessible due to the security settings, no record for that disk volume is created. To create a record for such a disk volume, change the security settings so that the user account specified for User in the monitoring target settings can be used to access the disk volume.
  - If no drive letter or drive path is assigned to the disk volume, 0 is set in the Size (SIZE) field.
  - If multiple drive letters or drive paths are assigned to the same disk volume, 0 might be set in the Size (SIZE) field.
  - If you change the drive letter or drive path of a disk volume, restart the WMI service of the monitoring target you changed. If you try to collect records without restarting it, you might not be able to collect the records from that disk volume. Even if the record is collected, the Size (SIZE) field might contain a value of 0 and the ID (ID) field might contain the logical disk volume name before the change was made.
- If the OS of the monitored host is UNIX, and if Filesystem or Mounted on includes a space when you execute the df command on the monitored host, the Logical Disk Overview (PI_LDSK) record will not be correctly displayed.
- If the monitored host uses an optical drive, the Free Mbytes % field for the applicable instance is sometimes set to 0% when media is inserted into the drive. To remove the Free Mbytes % field from the alarm settings, specify ID <> *applicable-disk* in the alarm condition expression.

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PI_LDSK_ID

Lifetime

None

Record size

- Fixed part: 1,034 bytes
- Variable part: 1,216 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	The record name. This is always LDSK.	COPY	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created.	COPY	COPY	time_t	No	--
Interval (INTERVAL)	Interval during which the information is collected. [Units: seconds] If the data is summarized in historical reports, the last value stored is displayed.	COPY	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host.	COPY	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Name of the monitored host.	COPY	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time when performance data was collected on the PFM - RM host.	COPY	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time when performance data was collected on the monitored host.	COPY	FIXED	string (32)	No	--
ID (ID)	Windows: Logical disk volume name. UNIX: File system mount point.	COPY	COPY	string (1024)	No	--
Device Name (DEVICE_NAME)	Device name.	COPY	FIXED	string (40)	No	Windows
Free Mbytes (FREE_MBYTES)	Size of unused area. [Units: MB]	HILO	ADD	double	No	--
Free Mbytes % (FREE_MBYTES_PERCENT)	Percentage of area unused. [Units: %]	HILO	AVG	double	No	--
Size (SIZE)	Disk size. [Units: MB]	COPY	ADD	double	No	--
Ext1 (EXT1)#	Extension field 1	HILO	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	HILO	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts.

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule
Not sprtd on: Not supported on

#

This field is not used for operations.

Network Interface Overview (PI_NET)

Function

The Network Interface Overview (PI_NET) record stores performance data, taken at a specific interval, about the network interface for the monitored host. This is a multi-instance record.

Notes

- If the connection to the monitored host fails, the information cannot be collected.
- If the OS of the monitored host is Windows, Solaris, AIX, or Linux, and if this record is collected in an environment where IPv4 and IPv6 coexist, summarized information for both IPv4 and IPv6 is collected.
- If the OS of the monitored host is HP-UX, and if this record is collected in an environment where IPv4 and IPv6 coexist, information is collected separately for IPv4 and IPv6. In an IPv4 environment, IPv4: is attached to the beginning of the ID, while in an IPv6 environment, IPv6: is attached to the beginning of the ID.

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PI_NET_ID

Lifetime

None

Record size

- Fixed part: 1,034 bytes
- Variable part: 548 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	The record name. This is always NET.	COPY	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created.	COPY	COPY	time_t	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Interval (INTERVAL)	Interval during which the information is collected. [Units: seconds] If the data is summarized in historical reports, the last value stored is displayed.	COPY	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host.	COPY	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Name of the monitored host.	COPY	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time when performance data was collected on the PFM - RM host.	COPY	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time when performance data was collected on the monitored host.	COPY	FIXED	string (32)	No	--
ID (ID)	Instance name of network.	COPY	COPY	string (256)	No	--
Max Transmission Unit (MAX_TRANSMISSION_UNIT)	Maximum packet size. [Units: bytes]	COPY	FIXED	ulong	No	Windows
Rcvd Packets/sec (RCVD_PACKETS_PER_SEC)	Rate of receiving network interface packets. [Units: packets/second]	HILO	AVG	double	No	--
Sent Packets/sec (SENT_PACKETS_PER_SEC)	Rate of transmitting network interface packets. [Units: packets/second]	HILO	AVG	double	No	--
Total Packets/sec (TOTAL_PACKETS_PER_SEC)	Total rate of receiving and transmitting network interface packets. [Units: packets/second]	HILO	AVG	double	No	--
Rcvd Bytes/sec (RCVD_BYTES_PER_SEC)	Rate of receiving network interface data. [Units: bytes/second]	HILO	AVG	double	No	UNIX
Sent Bytes/sec (SENT_BYTES_PER_SEC)	Rate of transmitting network interface data. [Units: bytes/second]	HILO	AVG	double	No	UNIX
Total Bytes/sec (TOTAL_BYTES_PER_SEC)	Total rate of receiving transmitting network interface data. [Units: bytes/second]	HILO	AVG	double	No	UNIX
Ext1 (EXT1)#	Extension field 1	HILO	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	HILO	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts.

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Physical Disk Overview (PI_PDSK)

Function

The Physical Disk Overview (PI_PDSK) record stores performance data, taken at a specific interval, about physical disks on the monitored host. This is a multi-instance record.

Notes

- If the connection to the monitored host fails, the information cannot be collected.
- Note the following points when collecting this record in a Windows environment:
  - If a security setting prevents access to the disk volume that corresponds to the ID (ID) field, no record is created for this disk volume. To create a record of the disk volume, set the security setting in the monitoring target setup to allow the user account specified in User to access the disk volume.
  - If you change the drive letter or drive path of a disk volume, restart the WMI service of the monitoring target you changed. If you try to collect records without restarting it, you might not be able to collect the records from that disk volume. Even if a record is collected, the ID (ID) field might display the disk volume name before the change was made.
- If the OS of the monitored host is AIX, only the following users can collect this record information:
  - root user
  - User who belongs to both adm and system groups
- If the OS of the monitored host is AIX, and if you change the device name by using a command such as endev, performance data is collected for a different instance than the one that was present before the change.
- If the OS of the monitored host is the Workload Partition (WPAR) environment of AIX V6.1 or later, the information for this record cannot be collected.

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PI_PDSK_ID

Lifetime

None

Record size

- Fixed part: 1,034 bytes
- Variable part: 652 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	The record name. This is always PDSK.	COPY	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created.	COPY	COPY	time_t	No	--
Interval (INTERVAL)	Interval during which the information is collected. [Units: seconds] If the data is summarized in historical reports, the last value stored is displayed.	COPY	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host.	COPY	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Name of the monitored host.	COPY	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time when performance data was collected on the PFM - RM host.	COPY	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time when performance data was collected on the monitored host.	COPY	FIXED	string (32)	No	--
ID (ID)	Windows: Physical disk number. Unix: Device name.	COPY	COPY	string (256)	No	--
Avg Disk Time (AVG_DISK_TIME)	Average operation time for disk I/O. [Units: seconds]	HILO	AVG	double	No	--
Busy % (BUSY_PERCENT)	Percentage of time the disk was busy with read and write requests. [Units: %] In Unix, if a device continuously performs processing, 100 might be exceeded.	HILO	AVG	double	No	--
Read MBytes/sec (READ_MBYTES_PER_SEC)	Speed at which data is transmitted to disk during read processing. [Units: MB/second]	HILO	AVG	double	No	AIX, HP-UX
Write MBytes/sec (WRITE_MBYTES_PER_SEC)	Speed at which data is transmitted to disk during write processing. [Units: MB/second]	HILO	AVG	double	No	AIX, HP-UX
Total MBytes/sec (TOTAL_MBYTES_PER_SEC)	Speed at which data is transmitted between disks during read and write processing. [Units: MB/second]	HILO	AVG	double	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Read Counts/sec (READ_COUNTS_PER_SEC)	Speed of disk reads. [Units: reads/second]	HILO	AVG	double	No	AIX, HP-UX
Write Counts/sec (WRITE_COUNTS_PER_SEC)	Speed of disk writes. [Units: writes/second]	HILO	AVG	double	No	AIX, HP-UX
Total Counts/sec (TOTAL_COUNTS_PER_SEC)	Speed of disk reads and writes. [Units: reads and writes/second]	HILO	AVG	double	No	--
Queue Length (QUEUE_LENGTH)	Windows: Average number of read and write requests in the disk queue. Unix: Device queue length. One item of I/O processing per second is assumed.	HILO	AVG	double	No	--
Ext1 (EXT1)#	Extension field 1	HILO	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	HILO	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts.

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

Processor Overview (PI_CPU)

Function

The Processor Overview (PI_CPU) record stores performance data, taken at a specific interval, about the processors on the monitored host. This is a multi-instance record.

Notes

- If the connection to the monitored host fails, the information cannot be collected.
- If this record is collected in a Windows environment, 100 is set as the maximum value of the following fields whose ID (ID) field is _Total:
  - CPU % (CPU_PERCENT)
  - System % (SYSTEM_PERCENT)
  - User % (USER_PERCENT)
- If the OS of both the PFM - RM host and the monitored host is 64-bit Windows, you can collect a maximum of 32 pieces of CPU information.
- If the OS of the monitored host is AIX and a user other than the root user is collecting information, 0 is displayed in the following fields if that user does not belong to either the adm group or system group:
  - CPU % (CPU_PERCENT)
  - Idle % (IDLE_PERCENT)
  - System % (SYSTEM_PERCENT)
  - User % (USER_PERCENT)
  - Wait % (WAIT_PERCENT)
  - Ext1 (EXT1)
  - Ext2 (EXT2)
- If the OS of the monitored host is the Workload Partition (WPAR) environment of AIX V6.1 or later, 0 is displayed in the following fields:
  - CPU % (CPU_PERCENT)
  - Idle % (IDLE_PERCENT)
  - System % (SYSTEM_PERCENT)
  - User % (USER_PERCENT)
  - Wait % (WAIT_PERCENT)
  - Ext1 (EXT1)
  - Ext2 (EXT2)

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	No	Y

Item	Default value	Changeable
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

PI_CPU_ID

Lifetime

None

Record size

- Fixed part: 1,034 bytes
- Variable part: 544 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	The record name. This is always CPU.	COPY	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created.	COPY	COPY	time_t	No	--
Interval (INTERVAL)	Interval during which the information is collected. [Units: seconds] If the data is summarized in historical reports, the last value stored is displayed.	COPY	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host.	COPY	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Name of the monitored host.	COPY	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time when performance data was collected on the PFM - RM host.	COPY	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time when performance data was collected on the monitored host.	COPY	FIXED	string (32)	No	--
ID (ID)	Processor ID.	COPY	COPY	string (256)	No	--
CPU % (CPU_PERCENT)	Processor CPU usage. [Units: %]	HILO	AVG	double	No	--
Idle % (IDLE_PERCENT)	Percentage of time the processor was idle. [Units: %]	HILO	AVG	double	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	Windows: Rate at which the processor processed interrupt requests generated by hardware devices (for example, the system clock, mouse, disk drivers, data communication line, and NIC). DPC (delay procedure call) interrupts are not included. If this field increases greatly when there is no system activity, a hardware problem (e.g., a low-speed device) probably exists. [Units: times/second] Unix: Rate at which interrupts are generated. [Units: times/second]	HILO	AVG	double	No	HP-UX
System % (SYSTEM_PERCENT)	Percentage of processor usage in kernel mode. [Units: %]	HILO	AVG	double	No	--
User % (USER_PERCENT)	Percentage of processor usage in user mode. [Units: %]	HILO	AVG	double	No	--
Wait % (WAIT_PERCENT)	Percentage of time waiting for I/O. [Units: %]	HILO	AVG	double	No	Windows
Ext1 (EXT1)#	Extension field 1	HILO	AVG	double	No	Windows, HP-UX, Solaris
Ext2 (EXT2)#	Extension field 2	HILO	AVG	double	No	Windows, HP-UX, Solaris

Legend:

--: Supported on all OSs of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

System Status (PD)

Function

The System Status (PD) record stores the status of the connection to the monitored host and information about the OS of the monitored host at a specific time.

Notes

If the connection to the monitored host fails, information is collected only in the following fields:

- Record Type (INPUT_RECORD_TYPE)
- Record Time (RECORD_TIME)
- Interval (INTERVAL)
- VA DeviceID (VADEVICEID)
- Target Host (TARGET_HOST)
- Polling Time (POLLING_TIME)
- Status (STATUS)
- Reason (REASON)

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	Yes	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

None

Lifetime

None

Record size

- Fixed part: 2,050 bytes
- Variable part: 0 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	The record name. This is always PD.	--	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created.	--	COPY	time_t	No	--
Interval (INTERVAL)	This is always 0.	--	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host.	--	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Name of the monitored host.	--	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time when performance data was collected on the PFM - RM host.	--	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time when performance data was collected on the monitored host.	--	FIXED	string (32)	No	--
Status (STATUS)	Connection status. SUCCESS: Connected ERROR: Connection failed	--	FIXED	string (8)	No	--
Reason (REASON)	Cause when the Status field is ERROR. Connection failed: Connection failed. Authorization failed: Authorization failed. Response invalid: There was an unintended response from the server. Collection error: Collection failed. If the Status field is SUCCESS, this item is empty. Collection timeout: Timeout occurred during collection. Invalid environment(SSH_Client): Invalid environment. The file specified in SSH_Client during instance environment setup does not exist (when the PFM - RM host is running Windows and the monitored host is running UNIX). Invalid environment(Perl_Module): Invalid environment. The file specified in Perl_Module during instance environment setup is not found (when the PFM - RM host is running Windows and the monitored host is running UNIX). Invalid environment(Private_Key_File):	--	FIXED	string (128)	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Reason (REASON)	Invalid environment. The file specified in Private_Key_File during monitored host setup is not found. Note that this field is set to a null string when the value of the Status field is SUCCESS.	--	FIXED	string (128)	No	--
OS Type (OS_TYPE)	OS on the monitored host.	--	FIXED	string (16)	No	--
Version (VERSION)	OS version on the monitored host.	--	FIXED	string (32)	No	--
Processor Type (PROCESSOR_TYPE)	Type of processor on the monitored host.	--	FIXED	string (64)	No	--
Detail (DETAIL)	Details about the monitored host.	--	FIXED	string (256)	No	--
Ext1 (EXT1)#	Extension field 1	--	FIXED	string (256)	No	All
Ext2 (EXT2)#	Extension field 2	--	FIXED	string (256)	No	All

Legend:

--: Supported on all OSs of the monitored hosts.

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

System Summary (PI)

Function

The System Summary (PI) record stores performance data, taken at a specific interval, about the processors and memory in the entire system of the monitored host.

Note

- If the connection to the monitored host fails, the information cannot be collected.
- If the OS of both the PFM - RM host and the monitored host is 64-bit Windows, you can collect a maximum of 32 pieces of CPU information.
- There is no upper limit to the number of instances you can create. The maximum number of monitoring targets you can create per instance is 50.
- If the OS of both the monitored hosts is HP-UX, AIX, or Linux, the memory size allocated as the file cache is treated as the size of used physical memory area in the following fields:
  - Free Mem % (FREE_MEM_PERCENT)
  - Free Mem Mbytes (FREE_MEM_MBYTES)
  - Used Mem % (USED_MEM_PERCENT)
  - Used Mem Mbytes (USED_MEM_MBYTES)
- If the OS of the monitored host is AIX and a user other than the root user is collecting information, 0 is displayed in the following fields if that user does not belong to either the adm group or system group:
  - CPU % (CPU_PERCENT)
  - Idle % (IDLE_PERCENT)
  - System % (SYSTEM_PERCENT)
  - User % (USER_PERCENT)
  - Wait % (WAIT_PERCENT)
  - Free Swap % (FREE_SWAP_PERCENT)
  - Free Swap Mbytes (FREE_SWAP_MBYTES)
  - Used Swap % (USED_SWAP_PERCENT)
  - Used Swap Mbytes (USED_SWAP_MBYTES)
  - Total Swap Mbytes (TOTAL_SWAP_MBYTES)
  - Page Fault Counts/sec (PAGE_FAULT_COUNTS_PER_SEC)
- If the OS of the monitored host is the Workload Partition (WPAR) environment of AIX V6.1 or later, 0 is displayed in the following fields:
  - CPU % (CPU_PERCENT)
  - Idle % (IDLE_PERCENT)
  - System % (SYSTEM_PERCENT)
  - User % (USER_PERCENT)
  - Wait % (WAIT_PERCENT)
  - Free Mem % (FREE_MEM_PERCENT)

- Free Mem Mbytes (FREE_MEM_MBYTES)
- Used Mem % (USED_MEM_PERCENT)
- Used Mem Mbytes (USED_MEM_MBYTES)
- Total Mem Mbytes (TOTAL_MEM_MBYTES)
- Free Swap % (FREE_SWAP_PERCENT)
- Free Swap Mbytes (FREE_SWAP_MBYTES)
- Used Swap % (USED_SWAP_PERCENT)
- Used Swap Mbytes (USED_SWAP_MBYTES)
- Total Swap Mbytes (TOTAL_SWAP_MBYTES)
- Page Fault Counts/sec (PAGE_FAULT_COUNTS_PER_SEC)

Default and changeable values

Item	Default value	Changeable
Collection Interval	300	Y
Collection Offset	0	Y
Log	Yes	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

Legend:
Y: Changeable
N: Not changeable

ODBC key field

None

Lifetime

None

Record size

- Fixed part: 2,206 bytes
- Variable part: 0 bytes

Fields

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Record Type (INPUT_RECORD_TYPE)	The record name. This is always PI.	COPY	COPY	char (8)	No	--
Record Time (RECORD_TIME)	Time when the record was created.	COPY	COPY	time_t	No	--
Interval (INTERVAL)	Interval during which the information is collected.	COPY	FIXED	ulong	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Interval (INTERVAL)	[Units: seconds] If the data is summarized in historical reports, the last value stored is displayed.	COPY	FIXED	ulong	No	--
VA DeviceID (VADEVICEID)	Device ID of the monitored host.	COPY	COPY	string (256)	No	--
Target Host (TARGET_HOST)	Name of the monitored host.	COPY	FIXED	string (33)	No	--
Polling Time (POLLING_TIME)	Time when performance data was collected on the PFM - RM host.	COPY	FIXED	string (32)	No	--
Target Host Time (TARGET_HOST_TIME)	Time when performance data was collected on the monitored host.	COPY	FIXED	string (32)	No	--
Active CPUs (ACTIVE_CPUS)	Number of processors.	COPY	ADD	ulong	No	--
CPU % (CPU_PERCENT)	Processor usage rate. [Units: %] This is the average of all processors.	HILO	AVG	double	No	--
Idle % (IDLE_PERCENT)	Percentage of time the processors are idle. [Units: %] This is the average of all processors.	HILO	AVG	double	No	--
System % (SYSTEM_PERCENT)	Percentage of processor usage in kernel mode. [Units: %] This is the average of all processors.	HILO	AVG	double	No	--
User % (USER_PERCENT)	Percentage of processor usage in user mode. [Units: %] This is the average of all processors.	HILO	AVG	double	No	--
Wait % (WAIT_PERCENT)	Percentage of time the processors are waiting for I/O. [Units: %] This is the average of all processors.	HILO	AVG	double	No	Windows
Processor Queue Length (PROCESSOR_QUEUE_LENGTH)	Number of requests in the processor queue that are ready to execute and waiting for processor time. If the length of the queue continuously exceeds 2, the processor is probably busy.	HILO	AVG	double	No	UNIX
Run Queue Avg 5 min (RUN_QUEUE_AVG_5_MIN)	Average number of threads waiting in the execution queue for the past 5 minutes. In HP-UX, Solaris, and AIX, this value includes the number of I/O waiting threads. In LINUX, this value does not include the number of I/O waiting threads.	HILO	AVG	double	No	Windows
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	Windows: Rate at which the processor processed interrupt requests generated by hardware devices (for example, the	HILO	AVG	double	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	system clock, mouse, disk drivers, data communication line, and NIC). DPC (delay procedure call) interrupts are not included. If this field increases greatly when there is no system activity, a hardware problem (e.g., a low-speed device) probably exists. [Units: times/second] Unix: Rate at which interrupts are generated. [Units: times/second]	HILO	AVG	double	No	--
Effective Free Mem % (EFFECTIVE_FREE_MEM_PERCENT)	Percentage of physical memory available to applications. [Units: %]	HILO	AVG	double	No	Windows, AIX, HP-UX, Solaris
Effective Free Mem Mbytes (EFFECTIVE_FREE_MEM_MBYTES)	Amount of physical memory available to applications. [Units: MB]	HILO	AVG	double	No	Windows, AIX, HP-UX, Solaris
Free Mem % (FREE_MEM_PERCENT)	Percentage of physical memory that is unused. [Units: %]	HILO	AVG	double	No	--
Free Mem Mbytes (FREE_MEM_MBYTES)	Amount of unused physical memory. [Units: MB]	HILO	AVG	double	No	--
Used Mem % (USED_MEM_PERCENT)	Percentage of physical memory used. [Units: %]	HILO	AVG	double	No	--
Used Mem Mbytes (USED_MEM_MBYTES)	Amount of used physical memory. [Units: MB]	HILO	AVG	double	No	--
Total Mem Mbytes (TOTAL_MEM_MBYTES)	Amount of physical memory. [Units: MB]	COPY	ADD	double	No	--
Free Swap % (FREE_SWAP_PERCENT)	Windows: Percentage of virtual memory that is unused. [Units: %] UNIX: Percentage of swap area that is unused. [Units: %]	HILO	AVG	double	No	--
Free Swap Mbytes (FREE_SWAP_MBYTES)	Windows: Amount of unused virtual memory. [Units: MB] Unix: Amount of unused swap space. [Units: MB]	HILO	AVG	double	No	--
Used Swap % (USED_SWAP_PERCENT)	Windows: Percentage of virtual memory used. [Units: %] Unix: Percentage of swap space used.	HILO	AVG	double	No	--

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Used Swap % (USED_SWAP_PERCENT)	[Units: %]	HILO	AVG	double	No	--
Used Swap Mbytes (USED_SWAP_MBYTES)	Windows: Size of area committed for virtual memory. [Units: MB] Unix: Size of swap space. [Units: MB]	HILO	AVG	double	No	--
Total Swap Mbytes (TOTAL_SWAP_MBYTES)	Windows: Amount of virtual memory. [Units: MB] UNIX: Amount of swap area. [Units: MB]	COPY	ADD	double	No	--
Page Fault Counts/sec (PAGE_FAULT_COUNTS_PER_SEC)	Frequency of page faults. [Units: faults/second]	HILO	AVG	double	No	HP-UX, Linux
Page Scan Counts/sec (PAGE_SCAN_COUNTS_PER_SEC)	Frequency of page scans. [Units: scans/second]	HILO	AVG	double	No	Windows, Linux, Solaris
Page-In Counts/sec (PAGE_IN_COUNTS_PER_SEC)	Rate of page-in operations. [Units: operations/second]	HILO	AVG	double	No	Linux
Page-Out Counts/sec (PAGE_OUT_COUNTS_PER_SEC)	Rate of page-out operations. [Units: operations/second]	HILO	AVG	double	No	Linux
Page-In Pages/sec (PAGE_IN_PAGES_PER_SEC)	Rate at which pages are paged in. [Units: pages/second]	HILO	AVG	double	No	AIX
Page-Out Pages/sec (PAGE_OUT_PAGES_PER_SEC)	Rate at which pages are paged out. [Units: pages/second]	HILO	AVG	double	No	AIX
Paging Pages/sec (PAGING_PAGES_PER_SEC)	Rate at which pages were being paged in and out when a page fault occurred. [Units: pages/second] This is the total of the Page-In Pages/sec and Page-Out Pages/sec fields. If this value continuously exceeds 5, lack of memory might be causing a system bottleneck.	HILO	AVG	double	No	UNIX
Pool Nonpaged KBytes (POOL_NONPAGED_KBYTES)	Amount of physical memory allocated for executing system component tasks for which page-outs could not be performed. [Units: KB] If this value continuously increases even though server processing is not becoming busier, a process might have a memory leak.	HILO	AVG	double	No	UNIX

PFM - View name (PFM - Manager name)	Description	Smry rule	Grpg rule	Format	Delta	Not sprtd on
Swap-In Counts/sec (SWAP_IN_COUNTS_PER_SEC)	Frequency of swap-in operations. [Units: operations/second]	HILO	AVG	double	No	Windows, AIX, Linux
Swap-Out Counts/sec (SWAP_OUT_COUNTS_PER_SEC)	Frequency of swap-out operations. [Units: operations/second]	HILO	AVG	double	No	Windows, AIX, Linux
Swap-In Pages/sec (SWAP_IN_PAGES_PER_SEC)	Frequency of page loading by swap-in operations. [Units: pages/second]	HILO	AVG	double	No	Windows, AIX
Swap-Out Pages/sec (SWAP_OUT_PAGES_PER_SEC)	Frequency of page retrieval by swap-out operations. [Units: pages/second]	HILO	AVG	double	No	Windows, AIX
Ext1 (EXT1)#	Extension field 1	HILO	AVG	double	No	All
Ext2 (EXT2)#	Extension field 2	HILO	AVG	double	No	All

Legend:

--: Supported on all OSs of the monitored hosts.

All: Not supported on any OS of the monitored hosts.

Smry rule: Summary rule

Grpg rule: Grouping rule

Not sprtd on: Not supported on

#

This field is not used for operations.

8 Messages

This chapter describes the format of the PFM - RM for Platform messages, lists the destinations to which messages are output, shows which messages are output to the Windows event log and syslog, and describes the messages in detail.

8.1 Message format

This section explains the format of messages issued by PFM - RM for Platform. It also describes the notations used in this manual to explain the messages.

8.1.1 Format of output messages

This section explains the format of the messages issued by PFM - RM for Platform.

Each message consists of a message ID, followed by a message text. The message format is as follows:

```
KAVLnnnnn-Y message-text
```

The message ID is composed of the following elements:

`K`

Identifier of the system.

`AVL`

Indicates a PFM - RM for Platform message.

nnnnn

Message number. The message numbers for PFM - RM for Platform are in the 17,000 series (`17`*xxx)*.

Y

Type of message:

- `E`: Error
  The processing has been cancelled.
- `W`: Warning
  The processing resumes after the message has been output.
- `I`: Information
  The system is providing the user with information.
- `Q`: Query
  The system is prompting the user to enter a response.

The following are the correspondences between the message type and the Windows event log type:

`-E`

- Level: Error
- Description: Error message

`-W`

- Level: Warning
- Description: Warning message

`-I`

- Level: Information
- Description: Additional information message

`-Q`

(Not output)

The following are the correspondences between the message type and the syslog priority level:

`-E`

- Level: `LOG_ERR`
- Description: Error message

`-W`

- Level: `LOG_WARNING`
- Description: Warning message

`-I`

- Level: `LOG_INFO`
- Description: Additional information message

`-Q`

(Not output)

8.1.2 Format of message explanations

This section describes the format used to explain messages in this manual.

The part of a message text that is shown in italics represents a variable; the actual wording in the message will depend on the circumstances. The manual lists the messages in the order of the message IDs. The following illustrates the format of a message explanation:

message-ID

message-text

Explanation of the message

S:

Explains the processing performed by the system.

O:

Explains the action the operator should take when the message is displayed.

Reference note

When the system administrator is contacted by the operator, the system administrator should collect log information and conduct initial checking in accordance with the procedures explained in *9. Error Handling Procedures*.

When you conduct initial checking to determine the cause of a problem, examine all applicable log information, such as the log information for the OS (Windows event log or syslog) and the log information output by PFM - RM for Platform. The log information enables you to understand the details of the processing that was underway when the problem occurred and to take appropriate action. You should also

make a record of the operations that led up to the problem and evaluate whether the problem is likely to recur.

8.2 Message output destinations

This section shows the output destinations of the messages issued by PFM - RM for Platform.

Whether a message is output to a destination shown in the table below is indicated by *Y* or --:

Legend:

Y: Message is output to the destination.
--: Message is not output to the destination.
Win. event log: Windows event log
stdout: Standard output
stderr: Standard error

Table 8–1: PFM - RM for Platform message output destinations

Message ID	Output destination							
	Win. event log	syslog	Common message log	stdout	stderr	JP1 system event#1	Agent event#2	Trace log of Remote Monitor Collector service
KAVL17000	Y	Y	Y	--	--	--	--	--
KAVL17001	Y	Y	Y	--	--	--	--	--
KAVL17002	Y	Y	Y	--	--	--	--	--
KAVL17003	Y	Y	Y	--	--	--	--	--
KAVL17004	Y	Y	Y	--	--	--	--	--
KAVL17005	Y	Y	Y	--	--	--	--	--
KAVL17006	Y	Y	Y	--	--	--	--	--
KAVL17007	Y	Y	Y	--	--	--	--	--
KAVL17008	Y	Y	Y	--	--	--	--	--
KAVL17009	Y	Y	Y	--	--	--	--	--
KAVL17010	--	--	Y	--	--	--	--	--
KAVL17011	--	--	Y	--	--	Y	Y	--
KAVL17012	--	--	Y	--	--	--	--	--
KAVL17013	--	--	Y	--	--	--	--	--
KAVL17014	--	--	Y	--	--	--	--	--
KAVL17015	--	--	Y	--	--	--	--	--
KAVL17016	--	--	Y	--	--	--	--	--
KAVL17017	--	--	Y	--	--	--	--	--
KAVL17018	--	--	--	--	--	--	--	Y
KAVL17019	--	--	Y	--	--	--	--	--
KAVL17020	--	--	Y	--	--	--	--	--
KAVL17021	--	--	Y	--	--	--	--	--

Message ID	Output destination							
	Win. event log	syslog	Common message log	stdout	stderr	JP1 system event#1	Agent event#2	Trace log of Remote Monitor Collector service
KAVL17022	--	--	Y	--	--	--	--	--
KAVL17023	--	--	Y	--	--	--	--	--
KAVL17024	--	--	Y	--	--	--	--	--
KAVL17025	--	--	Y	--	--	--	--	--
KAVL17026	--	--	Y	--	--	--	--	--
KAVL17027	Y	Y	Y	--	--	--	--	--
KAVL17028	Y	Y	Y	--	--	--	--	--
KAVL17029	--	--	Y	--	--	--	--	--
KAVL17030	--	--	Y	--	--	--	--	--
KAVL17031	--	--	Y	--	--	--	--	--
KAVL17032	--	--	Y	--	--	--	--	--
KAVL17033	--	--	Y	--	--	--	--	--
KAVL17034	--	--	Y	--	--	--	--	--
KAVL17035	--	--	Y	--	--	--	--	--
KAVL17036	--	--	Y	--	--	--	--	--

#1

A JP1 system event notifies JP1/IM of a change in the agent status. For details about JP1 system events, see the chapter that describes the monitoring of operations linked with the integrated manager product (JP1/IM) in the *Job Management Partner 1/Performance Management User's Guide*.

The following table shows the programs that are required in order to issue JP1 system events.

Table 8–2: Programs required in order to issue JP1 system events

Host type	Prerequisite program	Version
PFM - Manager host	PFM - Manager	09-00 or later
PFM - Web Console host	PFM - Web Console	08-00 or later
PFM - RM host	PFM - RM for Platform	09-00 or later
	PFM - Manager or PFM - Base	09-00 or later
	JP1/Base	09-00 or later

#2

An agent event notifies PFM - Manager of a change in the agent status. For details about agent events, see the chapter that describes event display in the *Job Management Partner 1/Performance Management User's Guide*.

The following table shows the programs that are required in order to issue agent events.

Table 8–3: Programs required in order to issue agent events

Host type	Prerequisite program	Version
PFM - Manager host	PFM - Manager	09-00 or later
PFM - Web Console host	PFM - Web Console	08-00 or later
PFM - RM host	PFM - RM for Platform	09-00 or later
	PFM - Manager or PFM - Base	09-00 or later

8.3 List of messages output to the Windows event log and syslog

This section lists the messages that PFM - RM for Platform outputs to the Windows event log and to syslog.

If the OS is Windows, the Windows event log is displayed in the application log in the Event Viewer window.

> **Reference note**
>
> To open the Event Viewer window, from the Windows **Start** menu, choose **Administrative Tools**, and then **Event Viewer**.

For any event issued by PFM - RM for Platform, the identifier `PFM-RMPlatform` is displayed in the **Source** column of the Event Viewer window.

If the OS is UNIX, syslog means are output to the syslog file.

For details about the storage location of the syslog file, see the syslog daemon configuration file (default is `/etc/syslogd.conf`).

The following table lists the messages that PFM - RM for Platform outputs to the Windows event log and to syslog.

Table 8–4: Messages output to the Windows event log and syslog

Message ID	Windows event log		syslog	
	Event ID	Type	Facility	Level
KAVL17000-I	17000	Information	LOG_DAEMON	LOG_INFO
KAVL17001-E	17001	Error	LOG_DAEMON	LOG_ERR
KAVL17002-I	17002	Information	LOG_DAEMON	LOG_INFO
KAVL17003-E	17003	Error	LOG_DAEMON	LOG_ERR
KAVL17004-E	17004	Error	LOG_DAEMON	LOG_ERR
KAVL17005-E	17005	Error	LOG_DAEMON	LOG_ERR
KAVL17006-E	17006	Error	LOG_DAEMON	LOG_ERR
KAVL17007-E	17007	Error	LOG_DAEMON	LOG_ERR
KAVL17008-E	17008	Error	LOG_DAEMON	LOG_ERR
KAVL17009-E	17009	Error	LOG_DAEMON	LOG_ERR
KAVL17027-E	17027	Error	LOG_DAEMON	LOG_ERR
KAVL17028-E	17028	Error	LOG_DAEMON	LOG_ERR

8.4 Messages

This section explains the messages issued by PFM - RM for Platform and the actions to be taken.

KAVL17000-I

Remote Monitor Collector has stopped. (host=*host-name*, service=*service-ID*)

The Remote Monitor Collector service terminated normally.

S:

Terminates the Remote Monitor Collector service processing.

KAVL17001-E

Remote Monitor Collector failed to start.

Startup of the Remote Monitor Collector service failed.

S:

Terminates the Remote Monitor Collector service processing.

O:

Check the immediately preceding message that has been output to the common message log and take appropriate action according to that message.

KAVL17002-I

Remote Monitor Collector started. (host=*host-name*, service=*service-ID*)

Startup of the Remote Monitor Collector service has been completed.

S:

Starts Remote Monitor Collector's performance data collection processing.

KAVL17003-E

Remote Monitor Collector stopped abnormally.

The Remote Monitor Collector terminated abnormally.

S:

Terminates the Remote Monitor Collector service processing.

O:

Check the immediately preceding message that has been output to the common message log and take appropriate action according to that message.

KAVL17004-E

An attempt to read the service startup information file has failed.

An attempt to read the service startup initialization file failed during startup of the Remote Monitor Collector service.

S:

Terminates the Remote Monitor Collector service processing.

O:

Check whether the service startup initialization file (`jpcagt.ini`) exists under the following directory:

- In Windows:
  installation-folder`\agt7\agent\`*instance-name*`\`
- In UNIX:
  `/opt/jp1pc/agt7/agent/`*instance-name*`/`

KAVL17005-E

An attempt to read the target information file has failed. (Target=*monitoring-target-name*)

An attempt to read the monitoring target information file failed during startup of the Remote Monitor Collector service.

S:

Continues the Remote Monitor Collector service processing.

O:

Check for any errors with the items that were specified when the monitoring target was set up.

Check whether the monitoring target information file (*monitoring-target-name*`.ini`) exists under the following directory:

- In Windows:
  installation-folder`\agt7\agent\`*instance-name*`\targets\`
- In UNIX:
  `/opt/jp1pc/agt7/agent/`*instance-name*`/targets/`

KAVL17006-E

An error occurred in the *function-name* function. (en=*error-code*,arg1=*argument-1*, arg2=*argument-2*, arg3=*argument-3*)

An error occurred during execution of the function indicated by *function-name*.

S:

Terminates the Remote Monitor Collector service processing.

O:

Collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17007-E

A signal interrupted processing. (signal=*signal-number*)

Processing was canceled by a signal.

S:

Terminates the Remote Monitor Collector service processing.

O:

Collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17008-E

Remote Monitor Collector will now stop because an error occurred.

The Remote Monitor Collector service is being stopped because of an error.

S:

Terminates the Remote Monitor Collector service processing.

O:

Check the immediately preceding message that has been output to the common message log and take appropriate action according to that message.

KAVL17009-E

Memory allocation failed. (RecordType=*record-type*)

Memory allocation failed. If `UNKNOWN` is displayed in *record-type*, memory allocation failed for multiple record IDs.

S:

Terminates the Remote Monitor Collector service processing.

O:

Increase available memory.

KAVL17010-W

Memory allocation failed. (RecordType=*record-type*)

Memory allocation failed. If `UNKNOWN` is displayed in *record-type*, memory allocation failed for multiple record IDs.

S:

Resumes the Remote Monitor Collector service processing.

O:

Increase the available memory.

KAVL17011-W

An attempt to collect the record failed. (RecordType=*record-type*, Target=*monitoring-target-name*)

Acquisition of the record indicated by *record-type* failed.

S:

Resumes the Remote Monitor Collector service processing.

O:

If this message is repeatedly output at every monitoring interval for the same monitoring target and record type, check to make sure that the system environment of the monitoring target has been correctly set up. If this message is output occasionally, the machine might be overloaded. If the cause of the error cannot be determined, collect

maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17012-W

An invalid value or a value outside the range was specified for the property of the Remote Monitor Collector service. (property=*property-name*, value=*value-range*, Target=*monitoring-target-name*)

An invalid value or a value outside the permitted range was specified for the indicated property of the Remote Monitor Collector service.

S:

Ignores the specified value and resumes the Remote Monitor Collector service processing. The value of this item remains unchanged.

O:

Check to see if the set value causes problems. If the value is not appropriate, specify an appropriate value.

KAVL17013-W

The collector process failed to start.

Startup of the collection process failed.

S:

Resumes the Remote Monitor Collector service processing.

O:

Collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17014-W

The collector process stopped abnormally.

The collection process terminated abnormally.

S:

Resumes the Remote Monitor Collector service processing.

O:

If this message is output more than once in succession, check the monitoring target's system environment settings for any error. If the cause of the error cannot be determined, collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17015-W

A performance data file is invalid. (Target=*monitoring-target-name*)

The contents of the performance data storage file are invalid.

S:

Resumes the Remote Monitor Collector service processing.

O:

Collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17016-W

Performance data was not saved to the Store database because it is the same as previous performance data. (RecordType=*record-type*, Target=*monitoring-target-name*)

The performance data was not saved in the Store database because it was the same as the previous data.

S:

Resumes the Remote Monitor Collector service processing.

O:

Specify the record collection interval or the collection interval for the collection process in such a manner that the following condition is satisfied: record collection interval ≥ collection interval for the collection process.

If the condition record collection interval ≥ collection interval for the collection process is satisfied but this warning occurs frequently, either increase the collection interval or reduce the number of monitored hosts in the instance environment.

KAVL17017-W

The record build failed because there is no performance data. (Target=*monitoring-target-name*)

Record creation failed because there was no performance data.

S:

Resumes the Remote Monitor Collector service processing.

O:

This warning might occur immediately after startup because there is no performance data yet. If this warning continues to occur even after some time has elapsed after startup, check the following items for each OS of the monitored hosts:

If the monitored host is running Windows

- Is the monitored host running?
- Is the WMI service running on the monitored host?
- Were the following settings specified correctly when the monitoring target was set up?

  · `TargetHost`

  · `UseCommonAccount`

  · `User`

  · `Password`

  · `Domain`

  If you are using common account information, check for any errors with the following items specified in common account information (wmi):

  · `User`

  · `Password`

  · `Domain`

- Can the name be resolved by the host name (`TargetHost`) specified when the monitoring target was set up?
- Was the WMI connection setting procedure performed correctly?

If the monitored host is running UNIX

- Is the monitored host running?
- Is the SSH service running on the monitored host?
- Were the following settings specified correctly when the monitoring target was set up?
  - `TargetHost`
  - `UseCommonAccount`
  - `User`
  - `Private_Key_File`
  - `Port`

  If you are using common account information, check for any errors with the following items specified in common account information (ssh):
  - `User`
  - `Private_Key_File`
- Can the name be resolved by the host name (`TargetHost`) specified when the monitoring target was set up?
- Was the SSH connection setting procedure performed correctly?
- Were the following settings specified correctly when the instance environment was set up (only when the PFM - RM host is running in a Windows environment)?
  - `SSH_Client`
  - `Perl_Module`

If the cause of the error cannot be determined, collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17018-I

The records were successfully saved onto the Store database. (RecordType=*record-type*, count=*records-count*, Target=*monitoring-target-name*)

The records indicated in *record-type* have been stored successfully in the Store database.

S:

Resumes the Remote Monitor Collector service processing.

KAVL17019-W

The initialization of interprocess communication failed.

Preparation for communication between the Remote Monitor Collector service and the collection process failed.

S:

Resumes the Remote Monitor Collector service processing.

O:

Processing on the work file, such as open or write processing, might have failed. Check for a shortage of available disk space.

If there is no problem with the available disk space, collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17020-W

An error occurred during collection of the record. (Target=*monitoring-target-name*)

An error occurred during record collection.

S:

Resumes the Remote Monitor Collector service processing.

O:

Collect maintenance data and contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

KAVL17021-I

A collector process will restart because the system detected that it stopped.

The collection process will be restarted because the system detected termination of the process.

S:

Resumes the Remote Monitor Collector service processing.

KAVL17022-W

Account authentication failed.

Account authentication failed.

S:

Resumes the Remote Monitor Collector service processing.

O:

Check for any errors in the following items, which were specified during instance environment setup:

- `UseCommonAccount`
- `RMHost_User`
- `RMHost_Password`
- `RMHost_Domain`

If you are using common account information, check for any errors in the following items specified in the common account information (pfmhost):

- `User`
- `Password`
- `Domain`

KAVL17023-W

The user profile failed to load.

Loading of the user profile failed.

S:

Resumes the Remote Monitor Collector service processing.

O:

Check whether the following settings were specified correctly when the instance environment was set up:

- `UseCommonAccount`
- `RMHost_User`
- `RMHost_Password`
- `RMHost_Domain`

If you are using common account information, check for any errors in the following items specified in the common account information (pfmhost):

- `User`
- `Password`
- `Domain`

Additionally, check whether the user profile identified in the error message exists.

KAVL17024-W

There are no SSH client execution modules. (Instance=*instance-name*)

The setting of the SSH client execution module (`SSH_Client`) is invalid. Because the instance includes a monitored host running UNIX, specify a correct value.

S:

Resumes the Remote Monitor Collector service processing.

O:

Check whether a correct value was specified in `SSH_Client` when the instance environment was set up.

KAVL17025-W

There are no Perl execution modules. (Instance=*instance-name*)

The setting of the Perl execution module (`Perl_Module`) is invalid. Because the instance includes a monitored host running UNIX, specify a correct value.

S:

Resumes the Remote Monitor Collector service processing.

O:

Check whether a correct value was specified in `Perl_Module` when the instance environment was set up.

KAVL17026-W

There are no private keys. (Instance=*instance-name*, Target=*monitoring-target-name*)

The setting for the private key file (`Private_Key_File`) used in the SSH public key method is invalid. If the monitored host is running UNIX, specify a correct value.

S:

Resumes the Remote Monitor Collector service processing.

O:

Check for any errors in the following items that were set when the monitoring target was set up:

- `UseCommonAccount`
- `Private_Key_File`

If you are using common account information, check for any errors in the following item specified in the common account information (ssh):

- `Private_Key_File`

KAVL17027-E

Memory allocation failed.

Memory allocation failed during startup.

S:

Terminates processing the Remote Monitor Collector service.

O:

Increase the amount of free memory.

KAVL17028-E

Failed to load the common account information. (Type=*type-of-common-account-information*, Instance=*instance-name*)

An attempt to read the common account information failed during startup of the Remote Monitor Collector service.

S:

Terminates processing the Remote Monitor Collector service.

O:

Make sure that common account information has been set up.

Check for any errors in the items specified in the common account information.

After checking the above issues, use the `jpcconf acc setup` command to set up the common account information.

KAVL17029-W

Failed to load the common account information. (Type=*type-of-common-account-information*, Instance=*instance-name*)

An attempt to read the common account information failed.

S:

Continues the Remote Monitor Collector service processing.

Reads common account information again at the next collection timing.

O:

Make sure that common account information has been set up.

Check for any errors in the items specified in the common account information.

After checking the above issues, use the `jpcconf acc setup` command to set up common account information.

KAVL17030-W

Failed to add the information for the monitoring target. (Instance=*instance-name*, Target=*monitoring-target-name*)

An attempt to add monitoring target information failed.

S:

Continues the Remote Monitor Collector service processing.

Does not collect performance data for the monitoring target for which information failed to be added.

O:

Check the preceding message in the common message log, and take action according to that message.

After taking the above action, use the `jpcconf target setup` command to perform setup again.

KAVL17031-W

Failed to update the information for the monitoring target. (Instance=*instance-name*, Target=*monitoring-target-name*)

An attempt to update monitoring target information failed.

S:

Continues the Remote Monitor Collector service processing.

Collects performance data for the monitoring target based on the pre-update values.

O:

Check the preceding message in the common message log, and take action according to that message.

KAVL17032-W

Failed to load the information file for the monitoring target. (Instance=*instance-name*, Target=*monitoring-target-name*)

An attempt to read the monitoring target information file failed.

S:

Continues the Remote Monitor Collector service processing.

O:

Check for any errors in the items that were set when the monitoring target was set up.

Make sure that the monitoring target information file (*monitoring-target-name*`.ini`) exists in the following directory:

- For Windows

installation-folder\agt7\agent*instance-name*\targets\

- For UNIX
  /opt/jp1pc/agt7/agent/*instance-name*/targets/

After checking the above issues, use the `jpcconf target setup` command to perform setup again.

KAVL17033-W

Failed to load the common start information file for the component. The instance will start as an environment that cannot use common account information. (Instance=*instance-name*)

An attempt to read the common start information file for each component failed. The system starts as an environment where common account information cannot be used.

S:

Continues the Remote Monitor Collector service processing.

O:

Make sure that the common start information file for each component (`jpccomm.ini`) exists in the following directory:

- For Windows
  installation-folder\
- For UNIX
  /opt/jp1pc/

KAVL17034-E

An invalid setting to use common account information is set in an environment that cannot use common account information. (Instance=*instance-name*)

An environment where common account information cannot be used is set to use common account information.

S:

Terminates the Remote Monitor Collector service processing.

O:

Take one of the following actions:

- Change the setting so that common account information is not used.
- To use common account information, upgrade PFM - Manager or PFM - Base in the same device to a version that supports common account information. Then create the common account information.
- If backup data was restored, check the data at the restoration source, and restore the correct backup data.

KAVL17035-W

An invalid setting to use common account information is set in an environment that cannot use common account information. (Instance=*instance-name*, Target=*monitoring-target-name*)

An environment where common account information cannot be used is set to use common account information.

S:

Continues the Remote Monitor Collector service processing.

O:

Take one of the following actions:

- Change the setting so that common account information is not used.
- To use common account information, upgrade PFM - Manager or PFM - Base in the same device to a version that supports common account information. Then create common account information.
- If backup data was restored, check the data at the restoration source, and restore the correct backup data.

KAVL17036-W

An invalid value is set in the common account information. (Type=*type-of-common-account-information*, Label=*item-name*, value=*value-range*)

An invalid value is specified in the common account information.

S:

Continues the Remote Monitor Collector service processing by ignoring the specified value. The corresponding item retains the pre-change (original) value.

O:

Check for any errors in the items specified in the common account information.

After checking the above issue, use the `jpcconf acc setup` command to set up common account information.

9 Error Handling Procedures

This chapter describes how to handle errors that might occur while you are using Performance Management products. The focus of this chapter's discussion is on handling errors that occur in PFM - RM for Platform. For details about error handling for the entire Performance Management system, see the chapter that describes troubleshooting in the *Job Management Partner 1/ Performance Management User's Guide*.

9.1 Error handling procedures

This section describes the procedures for handling errors that occur while you are using Performance Management products.

Checking the event

Check the following:

- Event where the error occurred
- Message contents (if a message has been displayed)
- Log information (such as the common message log)

For details about the messages and how to respond to each message, see *8. Messages*. For details about the log information that is output by the Performance Management products, see *9.3 Log information to be collected for troubleshooting*.

Collecting data

Collect data to determine the cause of the error. For details about how to collect the necessary data, see *9.4 Data to be collected for troubleshooting* and *9.5 How to collect data for troubleshooting*.

Checking the problem

Use the collected data to check the cause of the problem. You should also isolate the problem or the affected range.

9.2 Troubleshooting

This section explains how to conduct troubleshooting while you are using Performance Management products. If an error occurs, you should first check to see if any of the events described in this section has occurred.

The following table lists and describes the principal errors that might occur in Performance Management.

Table 9–1: Troubleshooting

No.	Classification	Nature of problem	Subsection
1	Setting up or starting services	• A Performance Management program service does not start. • It takes too long for a service to start once startup is requested. • Communication is not performed properly when a program service starts immediately after a Performance Management program service has stopped. • The message `The disk capacity is insufficient` is displayed, and then the Master Store service or the Remote Monitor Store service stops. • The Remote Monitor Collector service of PFM - RM does not start. • Failure Audit (Event ID: `4625` or `4776`) is recorded in the Windows security event log.	*9.2.1*
2	Executing commands	• When the `jpctool service list` command is executed, the names of inactive services are displayed. • When the `jpctool db dump` command is executed, data other than the specified Store data is output.	*9.2.2*
3	Report definitions	• There is a time period that is not included in historical reports.	*9.2.3*
4	Alarm definitions	• The program defined for action execution does not function correctly. • An alarm event is not displayed. • Even though the alarm threshold has been exceeded, the color of the alarm icon displayed in the Display Alarm Status window of Agents remains green.	*9.2.4*
5	Collecting and managing performance data	• The size of the PFM - RM for Platform's Store database is not reduced even though the data retention period was shortened. • The message `Illegal data was detected in the Store database` is output to the common message log. • PFM - RM for Platform was started, but no performance data is being collected. • The alarm related to process monitoring is not reported as intended.	*9.2.5*

9.2.1 Troubleshooting problems with setting up or starting a service

This subsection describes how to handle problems that are related to service setup or service startup.

(1) A Performance Management program service does not start

The following describes the possible causes and the resolutions.

- PFM - Manager is not running.

  If PFM - Manager and PFM - RM for Platform are both on the same host, the PFM - RM for Platform services cannot start if PFM - Manager is not running. Check if the PFM - Manager service is running; start it if it is not

running. For details about how to start services, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

- The same port number is set for more than one Performance Management program service.

  When the same port number is set for multiple Performance Management program services, none of those Performance Management program services can be started.

  The default is for the system to assign port numbers automatically, in which case there cannot be any duplicated port numbers. If you set specific port numbers for Performance Management program services during Performance Management setup, check the port numbers that you specified. If you specified the same port number for more than one Performance Management program service, specify different port numbers. For details about how to set port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- There is an error in the settings for the Store database storage directory.

  If any of the directories listed below is set to be inaccessible or does not exist, the Remote Monitor Store service cannot start. Check the specified directory names and attribute settings and correct any errors.

  - Store database storage directory
  - Store database backup directory
  - Store database partial backup directory
  - Store database export directory
  - Store database import directory

  If you specify these directories for multiple Remote Monitor Store services, the Remote Monitor Store services cannot start. Check the specified directory settings and correct any errors.

- An unauthorized method was used to change a machine's host name.

  For details about how to rename a host on a machine, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. If you rename a host using an unauthorized method, the Performance Management program services might not start.

- An error occurred in the service control manager.

  If you execute the `jpcspm start` command in Windows, the error message `An error occurred in the Windows service control manager` might be displayed and startup of the service might fail. If this has occurred, re-execute the `jpcspm start` command. If the same event occurs frequently, edit the `jpccomm.ini` file to change the retry interval and retry count for service startup processing during execution of the `jpcspm start` command. For details about how to change the retry interval and retry count, see the chapter that describes startup and termination of Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

(2) It takes too long for a service to start once startup is requested

It might take a long time for a service to actually start once you execute the `jpcspm start` command or you start a service by choosing the **Services** icon. If this is caused by either of the reasons listed below, the time required for starting the service will be reduced for subsequent startups of the service.

- During the first startup after a new instance has been added, the indexes of the Store database are created, which might cause the services to take longer than usual to start.
- If the Store service is unable to perform normal termination processing for a reason such as a power shut-off, the indexes of the Store database are rebuilt during the next restart, which might cause the services to take longer than usual to start.

(3) Communication is not performed properly when a program service starts immediately after a Performance Management program service has stopped

Immediately after a Performance Management program service has stopped, another program service might be started using the same port that the stopped service was using. In such a case, communication might not be performed properly. You can prevent this problem by doing the following:

- Use fixed port numbers for the Performance Management program services.

  For details about how to set port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Specify a value for `TCP_TIMEWAIT`.

  In the `TCP_TIMEWAIT` value, set the connection wait time to the following default value:

  In Windows Server 2003, Windows Server 2008, and Windows Server 2012: 2 minutes

(4) The message "The disk capacity is insufficient" is displayed, and then the Master Store service or the Remote Monitor Store service stops

Data storage in the Store database is interrupted when there is not enough free space on the disk used by the Store database. In such a case, the message `The disk capacity is insufficient` is displayed and the Master Store service or the Remote Monitor Store service stops.

If this message is displayed, take one of the following actions:

- Provide sufficient disk space.

  Determine the amount of disk space required for the Store database and change the Store database storage location to a disk with sufficient available space. For details about how to determine the disk space required for the Store database, see *A. Estimating System Requirements*. For details about how to change the Store database storage location, see *3.6.1 Changing performance data storage locations*.

- Change the data retention conditions for the Store database.

  Change the data retention conditions for the Store database by adjusting the maximum data capacity. For details about how to change the data retention conditions for the Store database, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

If the Master Store service or the Remote Monitor Store service will not start after you have taken these actions, an unrecoverable logical conflict has occurred in the Store database. In such a case, restore the Store database from a backup, and then start the Master Store service or the Remote Monitor Store service. If no backup is available, initialize the Store database, and then start the Master Store service or the Remote Monitor Store service. To initialize the Store database, you must delete all the following files from the storage directory for the Store database:

- Files with the extension `.DB`
- Files with the extension `.IDX`

For details about the storage directory for the Store database, see *3.6.1 Changing performance data storage locations*.

(5) The Remote Monitor Collector service of PFM - RM does not start

If the PFM - RM host is running Windows, startup of the Remote Monitor Collector service might fail during PFM - RM startup, and one of the following messages might be displayed in the Windows event log when Windows is restarted:

- The *Service Name* service hung on starting.
- *Service Name* service hung on startup.

Because this problem is caused by a timeout in Windows service control manager, it tends to occur when PFM - Manager's communication load is high and a response from PFM - Manager takes time. This problem occurs when all of the following conditions are satisfied:

- JP1/PFM - Manager's communication load is high.
  For example, many copies of PFM - RM are being started concurrently.
- In Windows **Services** applet, the startup type is set to **Automatic** for PFM - RM services.
- The OS is restarted.

To avoid this problem, take either of the following steps:

- When starting a service at the time the OS is restarted, start it by executing the jpcspm start command instead of starting it from Windows service control manager.
- Shorten the PFM - RM startup time by using the setting described below for the PFM - RM host.
  This setting shortens the reconnection processing during startup of the PFM - RM service if PFM - Manager cannot be connected to. In this case, the probability of the PFM - RM service starting in a stand-alone mode increases.

  To shorten the startup time of PFM - RM, change [Agent Collector *x* Section][#] in the startup information file (jpccomm.ini) and the NS Init Retry Count label of [Agent Store *x* Section][#] from NS Init Retry Count =2 to NS Init Retry Count =1.

  #
  The PFM - RM product ID is entered for *x*. For details about product IDs, see *B. List of Identifiers*. If multiple copies of PFM - RM are installed on the same host, specify an NS Init Retry Count label value for each product ID.

  The startup information file (jpccomm.ini) is stored in the following directory:

  If the PFM - RM host is a physical host
  installation-folder\jpccomm.ini

  If the PFM - RM host is a logical host
  environment-directory[#]\jp1pc\jpccomm.ini

  #
  Indicates the directory on the shared disk specified when the logical host was created.

(6) Failure Audit (Event ID: 4625 or 4776) is recorded in the Windows security event log.

When the monitored host is running Windows, Failure Audit (Event ID: 4625 or 4776) might be recorded in the Windows security event log.

PFM - RM for Platform makes a WMI connection to the monitored host by using the user name and password specified in the account information[#1] when the monitoring target was set up. However, WMI also tries to connect to the monitored host by using the process-executing account information[#2] (in which a user name and password were specified when the instance environment was set up), resulting in this problem. Even when Failure Audit (Event ID: 4625 or 4776) is displayed in the Windows security event log, there is no problem if performance information has been collected.

To avoid this problem, take the following steps:

1. Create account information having the same user name and password on the PFM - RM host and the monitored host.
2. Specify the user name and password (in the account information created in step 1) in the setting items for the instance environment and the setting items for the monitoring target as described below.
   - `RMHost_User`#2 setting item in the account information for the instance environment: *User name*
   - `RMHost_Password`#2 setting item in the account information for the instance environment: *Password*
   - `User`#1 setting item in the account information for the monitoring target: *User name*
   - `Password`#1 setting item in the account information for the monitoring target: *Password*

   For details about how to specify these settings, see *3.1.4 Setup procedure for the Windows edition*.

#1: This is a setting item (`User` or `Password`) in common account information (wmi) when common account information is used.

#2: This is a setting item (`User` or `Password`) in common account information (pfmhost) when common account information is used.

9.2.2 Troubleshooting problems with command execution

This subsection describes how to handle problems that are related to command execution.

(1) When the jpctool service list command is executed, the names of inactive services are displayed

The following describes the possible causes and the resolutions.

- 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 has been uninstalled. Execute the `jpctool service delete` command to delete the service information. For details about how to delete service information, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
- The machine's host name was changed without deleting Performance Management program service information.

  If a machine's host name was changed without deleting Performance Management program service information, the service information corresponding to the service IDs that were associated with the previous host name remains in the database that the Master Manager service manages. Execute the `jpctool service delete` command to delete service information. For details about how to delete service information and how to rename hosts, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) When the jpctool db dump command is executed, data other than the specified Store data is output

If you execute the `jpctool db dump` command more than once with the same export file name specified for the same Master Store service or Remote Monitor Store service, the subsequent output results will overwrite the initial output results. Specify a different export file name each time you execute the `jpctool db dump` command for the same Master Store service or Remote Monitor Store service. For details about how to export the Store database, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*.

9.2.3 Troubleshooting problems with report definitions

This subsection describes how to handle problems that are related to report definitions for Performance Management.

(1) There is a time period that is not included in historical reports

If the current time of the system on which PFM - RM for Platform is installed is changed to a future time, historical information from the time at which the change was made to the specified time is not stored. Therefore, the status of the monitoring target during that time period is not displayed in historical reports.

9.2.4 Troubleshooting problems with alarm definitions

This subsection describes how to handle problems that are related to alarm definitions.

(1) The program defined for action execution does not function correctly

The following describes a possible cause and the resolution.

- PFM - Manager or the Action Handler service at the target host is not running.

  Actions cannot be executed when PFM - Manager or the Action Handler service at the target host is inactive. To execute actions, make sure that PFM - Manager and the Action Handler service are running at the target host.

(2) An alarm event is not displayed

The following describes a possible cause and the resolution.

- PFM - Manager is not running.

  When PFM - Manager is inactive, the system cannot issue alarm events from PFM - RM for Platform correctly. To monitor alarm events, make sure that PFM - Manager is running.

(3) Even though the alarm threshold has been exceeded, the color of the alarm icon displayed in the Display Alarm Status window of Agents remains green

Possible causes of this problem, and the corrective step to take, are shown below:

- An alarm table that uses Japanese was bound in an environment where the `LANG` environment variable of the PFM - Manager host and the PFM - RM host is not set to Japanese

  In this case, alarms that use Japanese are not correctly evaluated. Set the `LANG` environment variable of the PFM - Manager host and the PFM - RM host to Japanese. You can check the setting of the `LANG` environment variable by checking the common message log to see whether the latest service startup message is output in Japanese or English.

  If the PFM - Manager host uses an English environment, changing it to a Japanese environment while the current setting is in effect will corrupt the existing alarm definitions, making them undeletable. Therefore, take the following steps:

  1. If you need alarm tables that use Japanese in the alarm definitions, export all of them from PFM - Web Console.

     For exporting, you cannot use the `jpctool alarm export` command.

     For details about how to export alarm tables, see the chapter that describes exporting of alarm tables in the *Job Management Partner 1/Performance Management User's Guide*.
  2. Delete all alarm tables that use Japanese in the alarm definitions.

3. Stop PFM - Manager.
4. Change the `LANG` environment variable of PFM - Manager host to Japanese.
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 the alarm tables.

   For details about how to import alarm tables, see the chapter that describes importing of alarm tables in the *Job Management Partner 1/Performance Management User's Guide*.

For other notes on environments where multiple languages coexist, see the chapter that describes notes on environments where multiple languages coexist in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

9.2.5 Troubleshooting problems with collection and management of performance data

This subsection describes how to handle problems that are related to collection and management of Performance Management performance data.

(1) The size of the PFM - RM for Platform's Store database is not reduced even though the data retention period was shortened

If the Store database has reached its maximum size but shortening the data retention period does not reduce the file size, you need to shorten the retention period, back up the Store database, and then restore the database.

For details about how to specify the data retention period, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/Performance Management User's Guide*. For details about how to back up and restore the Store database, see the chapter that describes backup and restore processing in the *Job Management Partner 1/Performance Management User's Guide*.

(2) The message "Illegal data was detected in the Store database" is output to the common message log

An inconsistency might have occurred in the Store database due to an unexpected service stop or machine shutdown. Take one of the following actions:

- If you have backed up the Store database, restore it.
- If you have not backed up the Store database, stop the Remote Monitor Store service, delete the corresponding database files (`*.DB` and `*.IDX` files), and then restart the service.

(3) PFM - RM for Platform was started, but no performance data is being collected

If the Status field value in the PD record is `ERROR`, take appropriate action based on the Reason field value.

The following describes the items to be checked for each Reason field value.

(a) Connection failed: Connection to the monitored host failed.

When the monitored host is running Windows

- Is the monitored host running?
- Is the WMI service running on the monitored host?
- Were the settings for the following specified correctly when the monitoring target was set up?[#1]
  - `TargetHost`
- Can the name be resolved by the host name (`TargetHost`) that was specified when the monitoring target was set up?
- Were the following WMI connection setup procedures performed correctly?
  - DCOM setting at the PFM - RM host
  - WMI namespace setting at the monitored host
  - Firewall setting at the monitored host
- If there is a firewall between PFM - RM for Platform and the monitoring target, is the firewall passage port set appropriately?

When the monitored host is running UNIX

- Is the monitored host running?
- Is the SSH service running on the monitored host?
- Were the following settings specified correctly when the monitored host was set up?[#1]
  - `Target Host`
  - `UseCommonAccount`[#2]
  - `User`[#3]
  - `Private_Key_File`[#3]
  - `Port`
- Can the name be resolved by the host name (`TargetHost`) that was specified when the monitoring target was set up?
- Were the settings for the following items specified correctly when the instance environment was set up?[#4] (This applies only when the PFM - RM host is running Windows.)
  - `SSH_Client`
  - `Perl_Module`
- Was the SSH connection setup procedure performed correctly?
- If there is a firewall between PFM - RM for Platform and the monitoring target, is the firewall passage port set appropriately?

#1

To check the items that have been set up, execute the `jpcconf target setup` command. If you are using common account information, execute the `jpcconf acc display` command to check the setting items. Alternatively, in PFM - Web Console, from the Remote Monitor Collector service of PFM - RM for Platform, view the Remote Monitor Configuration property to check the settings.

#2

This item is displayed when both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

#3

If you are using common account information, the values of `User` and `Private_Key_File` are the respective values that are specified in `User` and `Private_Key_File` in common account information (ssh).

#4

To check the items that have been set up, execute the `jpcconf inst setup` command. Alternatively, in PFM - Web Console, from the Remote Monitor Collector service of PFM - RM for Platform, view the Remote Monitor Configuration property to check the settings.

(b) Authorization failed: Authorization of the monitored host failed.

The items to be checked in Windows are described below. This error is not applicable to UNIX.

When the monitored host is running Windows

- Were the following settings specified correctly when the monitoring target was set up?[#1]
  - `UseCommonAccount`[#2]
  - `User`[#3]
  - `Password`[#3]
  - `Domain`[#3]
- Were the following WMI connection setup procedures performed correctly?
  - DCOM setting on the PFM - RM host
  - DCOM setting on the monitored host

#1

To check the settings, execute the `jpcconf target setup` command. If you are using common account information, execute the `jpcconf acc display` command to check the setting items. Alternatively, use PFM - Web Console to check the settings by displaying the Remote Monitor Configuration properties from the Remote Monitor Collector service of PFM - RM for Platform.

#2

This item is displayed when both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

#3

If you are using common account information, the values of `User`, `Password`, and `Domain` are the respective values that are specified in `User`, `Password`, and `Domain` in common account information (wmi).

(c) Collection timeout: Performance data collection did not end within the specified time

The items to be checked are shown below:

- In the instance environment, is the collection interval of the collection process for the monitored host too short?
  The collection interval of the collection process means the `Interval` setting in the instance environment. If this interval is short, either reduce the number of monitoring targets in the instance environment or lengthen the collection interval of the collection process.
- Has the monitored host been started?
- Were settings specified correctly when the monitored host was set up?[#]
- Was the WMI connection setting procedure followed correctly?
- Was the SSH connection setting procedure followed correctly?

- Is the PFM - RM host or the monitored host under a heavy system load?

If the cause of the error cannot be determined, collect maintenance data and contact the system administrator.

#

To check the items that have been set up, execute the `jpcconf target setup` command. Alternatively, in PFM - Web Console, from the Remote Monitor Collector service of PFM - RM for Platform, view the Remote Monitor Configuration property to check the settings.

(d) Invalid environment (SSH_Client): The file specified in SSH_Client when the instance environment was set up does not exist (when the PFM - RM host is running Windows and the monitored host is running UNIX)

The item to be checked when the PFM - RM host is running Windows and the monitored host is running UNIX is shown below. This error is not applicable when the monitored host is running Windows or when the PFM - RM host is running UNIX.

- Was the following setting specified correctly when the instance environment was set up?#
  SSH_Client

#

To check the item that has been set up, execute the `jpcconf inst setup` command. Alternatively, in PFM - Web Console, from the Remote Monitor Collector service of PFM - RM for Platform, view the Remote Monitor Configuration property to check the setting.

(e) Invalid environment (Perl_Module): The file specified in Perl_Module when the instance environment was set up does not exist (when the PFM - RM host is running Windows and the monitored host is running UNIX)

The item to be checked when the PFM - RM host is running Windows and the monitored host is running UNIX is shown below. This error is not applicable when the monitored host is running Windows or when the PFM - RM host is running UNIX.

- Was the following setting specified correctly when the instance environment was set up?#
  Perl_Module

#

To check the item that has been set up, execute the `jpcconf inst setup` command. Alternatively, in PFM - Web Console, from the Remote Monitor Collector service of PFM - RM for Platform, view the Remote Monitor Configuration property to check the setting.

(f) Invalid environment (Private_Key_File): The file specified in Private_Key_File when the monitored host was set up does not exist

The environment where the message `The file specified in Private_Key_File when the monitored host was set up does not exist` is output differs according to the version of PFM - RM for Platform, as follows:

- When the version of PFM - RM for Platform is from 09-50 to 10-00: The message is output if the PFM - RM host is running Windows, and the monitored host is running UNIX.
- When the version of PFM - RM for Platform is 10-50 or later: The message is output if the PFM - RM host is running Windows or UNIX, and the monitored host is running UNIX.

The items below are checked when the monitored host is running UNIX. This error is not applicable when the monitored host is running Windows.

- Were the following items specified correctly when the monitored host was set up?[#1]

  · `UseCommonAccount`[#2]

  · `Private_Key_File`[#3]

#1

To check the item that has been set up, execute the `jpcconf target setup` command. If you are using common account information, execute the `jpcconf acc display` command to check the setting items.

Alternatively, in PFM - Web Console, from the Remote Monitor Collector service of PFM - RM for Platform, view the Remote Monitor Configuration property to check the setting.

#2

This item is displayed when both the version of PFM - RM for Platform and the version of the prerequisite program (PFM - Manager or PFM - Base) in the same device as PFM - RM for Platform are 10-50 or later.

#3

If you are using common account information, the value of `Private_Key_File` is the value that is specified in `Private_Key_File` in common account information (ssh).

(g) Values other than those described above

- Collect maintenance data and contact the system administrator.
- If the monitored host is running Windows, check the application event log and take the appropriate corrective action.

  To use PFM - RM for Platform to collect performance data for the records listed below, PFM - RM for Platform must be set up so that objects can be monitored on the performance console.[#] The table below lists the objects corresponding to each record, the source (service) names that are output to the event log, and the performance extension DLLs.

  #

  You can use **Performance** to check the object name that corresponds to each record. If there is no corresponding object, specify the settings according to the procedure provided in Microsoft Knowledge Base by Microsoft so that the objects can be monitored.

  Table 9–2: Objects corresponding to each record, the source (service) names that are output to the event log, and the performance extension DLLs

No.	Category	Record name (record ID)	Object name	Source (service) name that is output to the event log	Performance extension DLL
1	Disk	Logical Disk Overview (`PI_LDSK`)	`LogicalDisk`	`WinMgmt`	`perfdisk.dll`
2		Physical Disk Overview (`PI_PDSK`)	`PhysicalDisk`		
3	Network-related	Network Interface Overview (`PI_NET`)	`Network Interface`		`perfctrs.dll`
4	OS in general (such as processors and memory)	System Overview (`PI`)	`Memory`		`perfos.dll`
5			`System`		
6			`Processor`		

No.	Category	Record name (record ID)	Object name	Source (service) name that is output to the event log	Performance extension DLL
7	OS in general (such as processors and memory)	Processor Overview (PI_CPU)	Processor	WinMgmt	perfos.dll

If the name WinMgmt is recorded in the application event log, PFM - RM for Platform might not function correctly or the records corresponding to that source (service) might not be collected. If the application event log contains the events shown in the table below, either reinstall the source (service) or eliminate the cause of the error that is disclosed in Microsoft Knowledge Base, or contact the developer of the source (service), and then repair the environment so that the application event logs are not recorded.

The following table shows examples of application event logs when PFM - RM for Platform is not functioning correctly or the records for the source (service) cannot be collected.

Table 9–3: Examples of application event logs when records are not collected successfully

No.	Event ID	Source (service) name	Event log information
1	37	WinMgmt	WMI ADAP 0x0 was unable to read the *file-name* performance library due to an unknown problem in the library.
2	41		WMI ADAP did not create object index *n* for the performance library *service-name* because the value was not found by the 009 subkey.
3	61		WMI ADAP was unable to process the *file-name* performance library due to a time violation in the open function.

- If the monitoring target is running UNIX, check whether the df command can be correctly executed, then take the appropriate recovery step.

  If the monitoring target is running UNIX, PFM - RM for Platform needs to run in a state in which the df command can be executed normally and the information in the mounted remote file system can be referenced. If you specify Y for the setting Disk_Category of the instance environment when the df command cannot be executed normally and the remote file system does not return a response, the Remote Agent service will not be able to collect performance data correctly. In this case, take the following actions:

  1. Change the setting Disk_Category of the instance environment to N.
  2. Execute either of the following commands to stop the df process on the remote host specified as the monitoring target:
     - kill -TERM *df-process-ID*
     - kill *df-process-ID*
  3. Correctly mount the remote file system by taking the appropriate action, such as restarting the NFS daemon.
  4. Return the setting Disk_Category of the instance environment to Y.

(4) Alarms related to process monitoring are not reported as intended

Note the following when you are monitoring the process operation status of a monitored host that is running UNIX: An error alarm might be reported even though the monitoring target process is not stopped, and then a normal alarm might be reported at the following collection time.

In a UNIX environment, when a process generates child processes, copies of these processes are created, and as a result duplicate copies of the same processes might appear to exist. Therefore, keep in mind that the number of processes increases when a process that generates child processes is the monitoring target. Specifically, an error alarm can be

reported if process information is collected at the time the number of processes increases, and a normal alarm can then be reported if process information is collected at the time the number of processes returns to 1.

To avoid this phenomenon, take the following steps:

- If the maximum number of concurrently existing child processes that will be generated by the monitoring target process is clear, specify the result of the formula shown below for the upper threshold of the number of monitoring target processes. Here, *m* indicates the maximum number of active processes and *n* indicates the maximum number of concurrently existing child processes per process.

  $m \times (1 + n)$

  If the calculation result exceeds 65,535, specify `65535`.
- If the maximum number of concurrently existing child processes that will be generated by the monitoring target process is unclear, specify `65535` for the upper threshold of the number of monitoring target processes.

If the process operation status information could not be collected from the OS, the number of monitoring target processes might become 0 and an alarm might be reported. To prevent this alarm, from the Alarms window, open the New Alarm Table > Main Information window or the Edit > Main Information window. Then in **Advanced settings**, select **Report alarm when the following damping condition is reached** and specify `2` **occurrence(s) during/Interval(s)**.

9.2.6 Troubleshooting other problems

We recommend that you check the existing circumstances when other errors occur. If a message is output, check the details of the message. For details about the log information that is output by Performance Management, see *9.3 Log information to be collected for troubleshooting*.

If you cannot resolve an error by taking the steps described in this section, or if an error occurs that is not described here, collect the data needed to investigate the error and contact the system administrator.

For details about the data you need to collect and how to collect it, see *9.4 Data to be collected for troubleshooting* and *9.5 How to collect data for troubleshooting*.

9.3 Log information to be collected for troubleshooting

When an error occurs in Performance Management, you need to check the log information and investigate the problem. The following five types of log information are output during operation of Performance Management:

- System log
- Common message log
- Operation status log
- Trace log
- Agent log

This section describes each type of log information.

9.3.1 Types of log information to be collected

(1) System log

The system log contains log information that reports the system status and errors that have occurred. This log information is output to the following file:

In Windows

Event log file

In UNIX

syslog file

For details about the output formats, see the chapter that describes log information in the manual *Job Management Partner 1/Performance Management Reference*.

Notes about logical host operation

In addition to the system log for Performance Management, you might need the log information for the cluster software in order to check such information as Performance Management control by the cluster software.

(2) Common message log

The common message log contains log information that reports the system status and errors that have occurred. The information output to this log is more detailed than the system log information. For details about the name and size of the file to which the common message log information is output, see *9.3.2 Log files and directories to check*. For details about the output formats, see the chapter that describes log information in the manual *Job Management Partner 1/Performance Management Reference*.

Notes about logical host operation

When Performance Management is under logical host operation, the common message log is output to the shared disk. Because a log file on the shared disk is inherited together with the system during failover, messages are recorded in the same log file.

(3) Operation status log

The operation status log is the log information that is output by PFM - Web Console. For details about the name and size of the file to which the operation status log information is output, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*. For details about the output formats, see the chapter that describes log information in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Trace log

The trace log is the log information that is collected in order to investigate the details of an error and determine the processing time required by each process when an error occurs. The trace log is output to a log file for each service of the Performance Management programs.

Notes about logical host operation

When Performance Management is under logical host operation, the common message log is output to the shared disk. Because a log file on the shared disk is inherited together with the system during failover, messages are recorded in the same log file.

(5) Agent log

The agent log is the log information for processing related to record collection. It is output by PFM - RM for Platform. In the event of an error, the agent log is collected in order to obtain detailed information about the processing. For details about the agent log, see *9.3.2(3) Agent log*.

Format

The agent log is output in the following format:

```
yyyy/mm/dd hh:mm:ss.sss inf1 inf2 inf3 Message
```

The following table describes each item that is output.

Table 9–4: Items in the agent log

No.	Item	Description
1	*yyyy*/*mm*/*dd*	Date the log was output (year/month/day)
2	*hh*:*mm*:*ss*.*sss*	Local time the log was output (hour:minute:second.millisecond)
3	*inf1* to *inf3*	Maintenance information
4	*Message*	Message

Note

Do not change the time at the PFM - RM host or the update date and time in the agent log file. If this information is changed, the agent log might not be output correctly because the output of the agent log uses information about the last update date and time of the log file.

9.3.2 Log files and directories to check

This subsection describes the log information that is output from Performance Management programs. For details about the name and size of the file to which the operation status log information is output, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

(1) Common message log

This subsection describes the common message log, which is one of the types of log information for Performance Management.

The following table lists the output sources, the log file names, and the amount of disk space used for Windows.

Table 9–5: File names of the common message log (for Windows)

No.	Type of log information	Output source	File name	Disk space used[#1] (kilobytes)
1	Common message log	Performance Management	*installation-folder*`\log\jpclog{01|02}`[#2]	2,048 (**x** 2)
2			*installation-folder*`\log\jpclogw{01|02}`[#2]	2,048 (**x** 2)
3	Common message log (for logical host operation)	Performance Management for logical host operation	*environment-folder*[#3] `\jp1pc\log\jpclog{01|02}`[#2]	2,048 (**x** 2)
4			*environment-folder*[#3] `\jp1pc\log\jpclogw{01|02}`[#2]	2,048 (**x** 2)

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 2,048 (**x** 2) indicates that a maximum of two log files, each with a size of 2,048 kilobytes, can be created. In this case, the total available disk space must be 4,096 kilobytes.

#2

The value `01` or `02` is appended to the file name of the common message log.

Sequential file method (`jpclog`)

Log information is first output to the log file whose name ends with `01`. When the maximum log file size is reached, the suffix at the end of the log file name is changed from `01` to `02`, and a new log file with the suffix `01` is created. Log information is then output to the new `01` log file. If a log file with a name ending in `02` already exists, that log file will be overwritten when the `01` suffix is changed to `02`. The most recent log information is always output to the log file with a `01` suffix.

Wrap-around file method (`jpclogw`)

Log information is first output to the log file whose name ends with `01`. When the maximum log file size is reached, a new log file with the suffix `02` is created. Log information is then output to the new `02` log file. If a log file with a name ending in `02` already exists, all data is deleted from that log file, and then log information is output from the beginning of the file. Thereafter, the log files are used alternately.

For details about how to output log information to log files, see the chapter that describes detection of Performance Management failures in the *Job Management Partner 1/Performance Management User's Guide*.

#3

The environment folder is on the shared disk that was specified when the logical host was created.

The following table lists the output sources, the log file names, and the amount of disk space used for UNIX.

Table 9–6: File names of the common message log (for UNIX)

No.	Type of log information	Output source	File name	Disk space used#1 (kilobytes)
1	Common message log	Performance Management	`/opt/jp1pc/log/jpclog{01|02}`#2	2,048 (**x** 2)
2			`/opt/jp1pc/log/jpclogw{01|02}`#2	2,048 (**x** 2)
3	Common message log (for logical host operation)	Performance Management for logical host operation	*environment-directory*#3 `/jp1pc/log/jpclog{01|02}`#2	2,048 (**x** 2)
4			*environment-directory*#3 `/jp1pc/log/jpclogw{01|02}`#2	2,048 (**x** 2)

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 2,048 (**x** 2) indicates that a maximum of two log files, each with a size of 2,048 kilobytes, can be created. In this case, the total available disk space must be 4,096 kilobytes.

#2

The value `01` or `02` is appended to the file name of the common message log.

Sequential file method (`jpclog`)

Log information is first output to the log file whose name ends with `01`. When the maximum log file size is reached, the suffix at the end of the log file name is changed from `01` to `02`, and a new log file with the suffix `01` is created. Log information is then output to the new `01` log file. If a log file with a name ending in `02` already exists, that log file will be overwritten when the `01` suffix is changed to `02`. The most recent log information is always output to the log file with a `01` suffix.

Wrap-around file method (`jpclogw`)

Log information is first output to the log file whose name ends with `01`. When the maximum log file size is reached, a new log file with the suffix `02` is created. Log information is then output to the new `02` log file. If a log file with a name ending in `02` already exists, all data is deleted from that log file, and then log information is output from the beginning of the file. Thereafter, the log files are used alternately.

For details about how to output log information to the log files, see the chapter that describes detection of Performance Management failures in the *Job Management Partner 1/Performance Management User's Guide*.

#3

The environment directory is on the shared disk that was specified when the logical host was created.

(2) Trace log

This subsection describes the trace log, which is one of the types of log information for Performance Management.

The following table lists the output sources and the storage folder names for Windows.

Table 9–7: Names of trace log storage folders (for Windows)

No.	Type of log information	Output source	Folder name
1	Trace log	Action Handler service	*installation-folder*`\bin\action\log\`
2		Performance Management command	*installation-folder*`\tools\log\`

No.	Type of log information	Output source	Folder name
3	Trace log	Remote Monitor Collector service	*installation-folder*\agt7\agent*instance-name*\log\
4		Remote Monitor Store service	*installation-folder*\agt7\store*instance-name*\log\
5		Status Server service	*installation-folder*\bin\statsvr\log\
6	Trace log (for logical host operation)	Action Handler service	*environment-folder*#\jp1pc\bin\action\log\
7		Performance Management command	*environment-folder*#\jp1pc\tools\log\
8		Remote Monitor Collector service	*environment-folder*#\jp1pc\agt7\agent*instance-name*\log\
9		Remote Monitor Store service	*environment-folder*#\jp1pc\agt7\store*instance-name*\log\

#
The environment folder is on the shared disk that was specified when the logical host was created.

The following table lists the output sources and the storage directory names for UNIX.

Table 9–8: Names of trace log storage directories (for UNIX)

No.	Type of log information	Output source	Directory name
1	Trace log	Action Handler service	/opt/bin/action/log/
2		Performance Management command	/opt/jp1pc/tools/log/
3		Remote Monitor Collector service	/opt/jp1pc/agt7/agent/*instance-name*/log/
4		Remote Monitor Store service	/opt/jp1pc/agt7/store/*instance-name*/log/
5		Status Server service	/opt/jp1pc/bin/statsvr/log/
6	Trace log (for logical host operation)	Action Handler service	*environment-directory*#/jp1pc/bin/action/log/
7		Performance Management command	*environment-directory*#/jp1pc/tools/log/
8		Remote Monitor Collector service	*environment-directory*#/jp1pc/agt7/agent/*instance-name*/log/
9		Remote Monitor Store service	*environment-directory*#/jp1pc/agt7/store/*instance-name*/log/

#
The environment directory is on the shared disk that was specified when the logical host was created.

(3) Agent log

This subsection describes the agent log of PFM - RM for Platform, which is one of the types of log information for Performance Management.

The following table lists the output sources, output targets, log file names, and disk space used for Windows.

Table 9–9: Agent log files (for Windows)

No.	Type of log information	Output source	Output target	File name	Default disk space used[#1] (megabytes)
1	Normal log	PFM - RM for Platform	*installation-folder* `\agt7\agent\` *instance-name* `\log\`	`collect_core_`*nn*[#2]	3 (**x** 4)[#3]
2				`collect_`*nn*[#2]	
3				`timer_core_`*nn*[#2]	
4				`timer_`*nn*[#2]	
5				`target_`*monitoring-target-name*`_`*nn*[#2]	
6	Normal log (for logical host operation)	PFM - RM for Platform	*environment-folder*[#4]`\jp1pc\agt7\agent\` *instance-name* `\log\`	`collect_core_`*nn*[#2]	3 (**x** 4)[#3]
7				`collect_`*nn*[#2]	
8				`timer_core_`*nn*[#2]	
9				`timer_`*nn*[#2]	
10				`target_`*monitoring-target-name*`_`*nn*[#2]	

#1

You can use the following methods to check and change the maximum file size for the agent log:

- `jpcconf inst` command
- Remote Monitor Configuration property in the PFM - Web Console window

For details about how to change the maximum file size with the `jpcconf inst` command, see *3.6.2 Updating an instance environment*.

#2

The agent log uses the sequential method. First, log information is output to a log file with a file name ending with `01`. When the size of the log file reaches the maximum limit, the end of the log file name changes from `01` to `02`, and a new log file with a file name ending with `01` is created. After that, log information is output to the log file with the file name ending with `01`. If a log file with a file name ending with `02` or higher already exists, that file is overwritten. The latest log data is always output to a log file with a file name ending with `01`.

In the file name, *nn* indicate a number from `01` to `04`.

#3

The value in parentheses is the number of log files. For example, 3 (**x** 4) indicates that a maximum of four log files, each with a size of 3 megabytes, can be created. In this case, the total available disk space must be 12 megabytes.

Use the following formula to estimate the amount of disk space used by agent logs per instance. The units are megabytes.

(`4` + *number-of-monitored-hosts*) **x** `4` **x** *Log_Size-value-specified-for-the-instance-environment*

#4

The environment folder is on the shared disk that was specified when the logical host was created.

The following table lists the output sources, output targets, log file names, and disk space used for UNIX.

Table 9–10: Agent log files (for UNIX)

No.	Type of log information	Output source	Output target	File name	Default disk space used[#1] (megabytes)
1	Normal log	PFM - RM for Platform	`/opt/jp1pc/agt7/agent/` *instance-name*`/log/`	`collect_`*nn*[#2]	3 (**x** 4)[#3]
2				`timer_`*nn*[#2]	
3				`target_`*monitoring-target-name*`_`*nn*[#2]	

No.	Type of log information	Output source	Output target	File name	Default disk space used[#1] (megabytes)
4	Normal log (for logical host operation)	PFM - RM for Platform	*environment-directory*[#4]`/jp1pc/agt7/agent/`*instance-name*`/log/`	`collect_`*nn*[#2]	3 (**x** 4)[#3]
5				`timer_`*nn*[#2]	
6				`target_`*monitoring-target-name*`_`*nn*[#2]	

#1

You can use the following methods to check and change the maximum file size for the agent log:

- `jpcconf inst` command
- Remote Monitor Configuration property in the PFM - Web Console window

For details about how to change the maximum file size with the `jpcconf inst` command, see *3.6.2 Updating an instance environment*.

#2

The agent log uses the sequential method. First, log information is output to a log file with a file name ending with `01`. When the size of the log file reaches the maximum limit, the end of the log file name changes from `01` to `02`, and a new log file with a file name ending with `01` is created. After that, log information is output to the log file with the file name ending with `01`. If a log file with a file name ending with `02` or higher already exists, that file is overwritten. The latest log data is always output to a log file with a file name ending with `01`.

In the file name, *nn* indicate a number from `01` to `04`.

#3

The value in parentheses is the number of log files. For example, 3 (**x** 4) indicates that a maximum of four log files, each with a size of 3 megabytes, can be created. In this case, the total available disk space must be 12 megabytes.

Use the following formula to estimate the amount of disk space used by agent logs per instance. The units are megabytes.

(`2` + *number-of-monitored-hosts*) **x** `4` **x** *Log_Size-value-specified-for-the-instance-environment*

#4

The environment directory is on the shared disk that was specified when the logical host was created.

9.4 Data to be collected for troubleshooting

This section describes the data that needs to be collected when an error has occurred.

Performance Management provides commands for collecting the needed data in the batch mode. Use the `jpcras` command to collect PFM - RM for Platform data. The tables in the following subsections indicate the data that can be collected by the `jpcras` command.

Note

The data collected by the `jpcras` command depends on options you specify when you execute the command. For details about the command's options and the data that is collected, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Notes about logical host operation

The following notes apply to logical host operation:

- During logical host operation, Performance Management log information is stored on the shared disk. If the shared disk is online, you can use the `jpcras` command to also collect the log information on the shared disk in the batch mode.
- To investigate problems during failover, you need the information existing before and after the failover. This means that you need information from both the executing system and the standby system.
- When Performance Management runs on a logical host, its startup and termination are controlled by the cluster software. Therefore, you need information about the cluster software in order to investigate a Performance Management that is running on a logical host. Compare the cluster software operation and the Performance Management operation.

9.4.1 Data to be collected from a Windows environment

(1) Log information about the OS

The following table lists the log information about the OS that needs to be collected.

Table 9–11: Log information about the OS (for Windows)

No.	Type of information	Overview	Default file name	Collection by the jpcras command
1	System log	Windows event log	--	Y
2		WMI log	*system-folder*`\system32\WBEM\Logs\*`#	Y
3	Process information	List of processes	--	Y
4	System file	`hosts` file	*system-folder*`\system32\drivers\etc\hosts`	Y
5		`services` file	*system-folder*`\system32\drivers\etc\services`	Y
6	OS information	System information	--	Y
7		Network status	--	Y
8		Host name	--	Y

No.	Type of information	Overview	Default file name	Collection by the jpcras command
9	OS information	Windows firewall information	--	Y
10	Dump information (in Windows Server 2003)	Dr. Watson log file	*system-drive*\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwtsn32.log# *system-drive*\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dump#	Y
11	Dump information (in Windows Server 2008 or Windows Server 2012)	Problem report and solution log file	*user-mode-process-dump-output-folder**program-name*.*process-ID*.dmp Example: jpcagt7.exe.2420.dmp	N

Legend:

Y: Can be collected

N: Cannot be collected

--: Not applicable

#

If you have set the log files to be output to a different folder, collect the data from the applicable folder.

(2) Information about Performance Management

The following table lists the Performance Management information that needs to be collected. In the case of a network connection error, you must also collect applicable files from the machine at the connection destination.

Table 9–12: Information about Performance Management (for Windows)

No.	Type of information	Overview	Default file name	Collection by the jpcras command
1	Common message log	Message log output from Performance Management (sequential file method)	*installation-folder*\log\jpclog{01|02}#1	Y
2		Message log output from Performance Management (wrap-around file method)	*installation-folder*\log\jpclogw{01|02}#1	Y
3	Configuration information	Each configuration information file	--	Y
4		Output results of the jpctool service list command	--	Y
5	Version information	Product version	--	Y
6		Historical information	--	Y
7	Database information	Remote Monitor Store service	• *installation-folder*\agt7\store*instance-name*\STPD	Y

No.	Type of information	Overview	Default file name	Collection by the jpcras command
7	Database information	Remote Monitor Store service	• *installation-folder*\agt7\store*instance-name**following-files-under-STPI-folder* ・*.DB ・*.IDX	Y
8	Trace log	Trace information for each service of the Performance Management program	--[#2]	Y
9	Agent log	Normal log of the processing related to record collection by PFM - RM for Platform	• *installation-folder*\agt7\agent*instance-name*\log\collect_{01|02|03|04}[#4] • *installation-folder*\agt7\agent*instance-name*\log\timer_{01|02|03|04}[#4] • *installation-folder*\agt7\agent*instance-name*\log\target_*monitoring-target-name*_{01|02|03|04}[#4]	Y
10	Work data	Work data during performance data collection	• *installation-folder*\agt7\agent*instance-name*\targets* • *installation-folder*\agt7\agent*instance-name*\groups*	Y
11	Install log[#3]	Message log during installation	• %TEMP%\pfm_inst.log[#5] • *system-folder*\TEMP\HCDINST*.LOG	N
12	Language environment information for system account	Language environment information for system account	• *installation-folder*\agt7\agent*instance-name*\log\system_lang.log	Y

Legend:

Y: Can be collected

N: Cannot be collected

--: Not applicable

#1

For details about how to output log information to the log files, see the chapter that describes detection of Performance Management failures in the *Job Management Partner 1/Performance Management User's Guide*.

#2

For details about the trace log storage folder, see *9.3.2(2) Trace log*.

#3

Collect this log information if installation fails. %TEMP% indicates the folder that is set in TEMP when the set command is executed at the command prompt.

#4

For details about the agent log output method and the storage folder, see *9.3.2 Log files and directories to check*.

#5

This applies to Windows Server 2003 only.

(3) Software information

The following table lists the types of information that must be collected by the various software when you want to use PFM - RM for Platform to collect performance data.

Table 9–13: Software information

No.	Type of information	Overview	Acquiring command	Collection by the jpcras command
1	PuTTY	SSH client (plink) version information	plink.exe -V#1	Y
2	ActivePerl	Perl module (perl) version information	perl.exe -V#2	Y

Legend:

Y: Can be collected

#1

Specify the -V option for the absolute path name of the plink.exe command specified in SSH_Client when the instance environment was set up. Note that the command will not be executed in the following cases:

- SSH_Client is not specified.
- No file exists in the path specified in SSH_Client.
- The file name specified in SSH_Client is not plink.exe.

#2

Specify the -V option for the absolute path name of the perl.exe command specified in Perl_Module when the instance environment was set up. Note that the command will not be executed in the following cases:

- Perl_Module is not specified.
- No file exists in the path specified in Perl_Module.
- The file name specified in Perl_Module is not perl.exe.

(4) Operation information

You need the following information about the operation that was underway when an error occurred:

- Details of the operation
- Time the error occurred
- Machine configuration (such as the version of each OS, host name, and configuration of PFM - Manager and PFM - RM for Platform)
- Whether the problem is repeatable
- Performance Management user name used during logon, if the user has logged on from PFM - Web Console
- Any arguments specified in a command, if the problem occurred during command execution

(5) Error information on screen displays

Obtain a hardcopy of the following information:

- The window operation when the application error occurred
- The error message dialog box (including the contents of detailed information if displayed)
- The Command Prompt window or the Administrator Console window, if the error occurred during command execution

(6) User-mode process dump (in Windows Server 2008 or Windows Server 2012)

In a Windows Server 2008 or Windows Server 2012 environment, if a Performance Management process is stopped by an application error, collect a user-mode process dump.

(7) Collecting a problem report (in Windows Server 2008 or Windows Server 2012)

In a Windows Server 2008 or Windows Server 2012 environment, if a Performance Management process is stopped by an application error, collect a problem report.

(8) Other information

You also need the following information:

- The contents of **System** and **Application** in the Event Viewer window of Windows
- The contents of **System Information**, which is displayed by choosing **Accessories**, and then **System Tools**

9.4.2 Data to be collected from a UNIX environment

(1) Log information about the OS

The following table lists the log information about the OS that needs to be collected.

Table 9–14: Log information about the OS (for UNIX)

No.	Type of information	Overview	Default file name	Collection by the jpcras command
1	System log	syslog	--	Y#
2	Process information	List of processes	--	Y
3	System file	`hosts` file	`/etc/hosts`	Y
4		`services` file	`/etc/services`	Y
5	OS information	Patch information	--	Y
6		Kernel information	--	Y
7		Version information	--	Y
8		Network status	--	Y
9		Environment variable	--	Y
10		Host name	--	Y
11	Dump information	`core` file	--	Y

Legend:
Y: Can be collected
--: Not applicable

#

If the system is set to output to a path and file name that are not the default, the information cannot be collected. Use an appropriate method to collect the data.

(2) Information about Performance Management

The following table lists the Performance Management information that needs to be collected. In the case of a network connection error, you must also collect applicable files from the machine at the connection destination.

Table 9–15: Information about Performance Management (for UNIX)

No.	Type of information	Overview	Default file name	Collection by the jpcras command
1	Common message log	Message log output from Performance Management (sequential file method)	`/opt/jp1pc/log/jpclog{01|02}`#1	Y
2		Message log output from Performance Management (wrap-around file method)	`/opt/jp1pc/log/jpclogw{01|02}`#1	Y
3	Configuration information	Each configuration information file	--	Y
4		Output results of the `jpctool service list` command	--	Y
5	Version information	Product version	--	Y
6		Historical information	--	Y
7	Database information	Remote Monitor Store service	• `/opt/jp1pc/agt7/store/`*instance-name*`/*.DB` • `/opt/jp1pc/agt7/store/`*instance-name*`/*.IDX`	Y
8	Trace log	Trace information for each service of the Performance Management program	--#2	Y
9	Agent log	Normal log of the processing related to record collection by PFM - RM for Platform	• `/opt/jp1pc/agt7/agent/`*instance-name*`/log/collect_{01|02|03|04}`#3 • `/opt/jp1pc/agt7/agent/`*instance-name*`/log/timer_{01|02|03|04}`#3 • `/opt/jp1pc/agt7/agent/`*instance-name*`/log/target_`*monitoring-target-name*`_{01|02|03|04}`#3	Y
10	Work data	Work data during performance data collection	• `/opt/jp1pc/agt7/agent/`*instance-name*`/targets/*` • `/opt/jp1pc/agt7/agent/`*instance-name*`/groups/*`	Y
11	Install log#4	Standard log of Hitachi Program Product Installer	• `/etc/.hitachi/.hitachi.log` • `/etc/.hitachi/.hitachi.log{01|02|03|04|05}` • `/etc/.hitachi/.install.log`	N

No.	Type of information	Overview	Default file name	Collection by the jpcras command
11	Install log#4	Standard log of Hitachi Program Product Installer	• `/etc/.hitachi/.install.log{01|02|03|04|05}`	N

Legend:

Y: Can be collected

N: Cannot be collected

--: Not applicable

#1

For details about how to output log information to the log files, see the chapter that describes detection of Performance Management failures in the *Job Management Partner 1/Performance Management User's Guide*.

#2

For details about the trace log storage directory, see *9.3.2 Log files and directories to check*.

#3

For details about the agent log output method and the storage directory, see *9.3.2 Log files and directories to check*.

#4

Collect this log information if installation fails.

(3) Operation information

You need the following information about the operation that was underway when the error occurred:

- Details of the operation
- Time the error occurred
- Machine configuration (such as the version of each OS, host name, and configuration of PFM - Manager and PFM - RM for Platform)
- Whether the problem is repeatable
- Performance Management user name used during logon, if the user has logged on from PFM - Web Console
- Any arguments specified in a command, if the problem occurred during command execution

(4) Error information on screen displays

Obtain a hardcopy of the following information:

- The window operation when the application error occurred
- The messages output to the console, if the error occurred during command execution

9.5 How to collect data for troubleshooting

This section describes how to collect data in the event of an error.

9.5.1 How to collect data in a Windows environment

(1) Collecting dump information (in Windows Server 2008 or Windows Server 2012)

To collect dump information in a Windows Server 2008 or Windows Server 2012 environment:

1. Open Task Manager.
2. Select the **Processes** tab.
3. Right-click the name of the process for which a dump is to be collected and choose **Create Dump File**.
   A dump file is stored in the following folder:

   ```
   system-drive\Users\user-name\AppData\Local\Temp
   ```

4. Collect the dump files from the folder identified in step 3.
   If you have changed the setting of the environment variable so that dump files are output to a different folder than the one described in step 3, collect the dump files from that alternate folder.

(2) Executing the data collection command

Use the `jpcras` command to collect data needed to determine the cause of an error. Note that an OS user with Administrator permissions must perform the procedure described below.

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 command extensions of the command interpreter:

   ```
   cmd /E:ON
   ```

3. Execute the `jpcras` command, with the data to be collected and the data storage folder to be used specified.
   The following `jpcras` command stores all the available information in the `c:\tmp\jpc\agt` folder:

   ```
   jpcras c:\tmp\jpc\agt all all
   ```

When you execute the `jpcras` command, the `jpctool service list -id * -host *` command is executed internally in order to obtain a list of PFM services and to check their activity status. If there is a firewall between the host where the command is executed and the host for the Performance Management system or if the system configuration is large, it might take a while for the `jpctool service list -id * -host *` command to execute. In such a case, you can suppress execution of the `jpctool service list -id * -host *` command, thus reducing the command execution time, by specifying `1` in the `JPC_COLCTRLNOHOST` environment variable.

For details about the `jpcras` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Note on executing a command in a Windows Server 2008 or Windows Server 2012 environment

If the user account control functionality (UAC) is enabled in the operating system, the user account control dialog box might appear during command execution. If this dialog box appears, click the **Continue** button to continue data collection. Clicking the **Cancel** button will cancel data collection.

(3) Executing a data collection command (operation on a logical host)

Performance Management information for logical host information is on the shared disk and must be collected in both the executing system and the standby system.

Use the `jpcras` command to collect data needed to determine the cause of an error. Note that an OS user with Administrator permissions must perform the procedure described below.

To execute the data collection command for logical host operation:

1. Place the shared disk online.

   Information about the logical host is stored on the shared disk. At the executing node, make sure that the shared disk is online, and then collect the information.

2. Execute the `jpcras` command in both the executing system and the standby system, with the data to be collected and the data storage folder to be used specified.

   The following `jpcras` command stores all the available information in the `c:\tmp\jpc\agt` folder:

   ```
   jpcras c:\tmp\jpc\agt all all
   ```

   Executing the `jpcras` command without the `lhost` argument specified collects all the Performance Management information on the physical and logical hosts at that node. If there is a Performance Management in the logical host environment, the log files on the shared disk are acquired.

   If the `jpcras` command is executed at a node where the shared disk is offline, files will not be acquired from the shared disk, but the command will terminate normally without resulting in an error.

   Note

   Execute the data collection command at both the executing node and the standby node to collect information. To examine an event before and after failover, you need the information from both systems (executing and standby).

   For details about the `jpcras` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

3. Collect information about the cluster software.

   This information is needed to determine whether the problem occurred in the cluster software or in Performance Management. Collect the information that provides control requests, such as startup and termination of Performance Management from the cluster software, and their results.

(4) Collecting the Windows event log

In the Windows Event Viewer window, collect the content of **System** and **Applications**.

(5) Checking information about the operation

Check and save information about the operation that was underway when the error occurred. The following lists the information that you need to check and save:

- Details of the operation
- Time the error occurred
- Machine configuration (such as the version of each OS, host name, and configuration of PFM - Manager and PFM - RM for Platform)
- Whether the problem is repeatable
- Performance Management user name used during logon, if the user has logged on from PFM - Web Console
- Any arguments specified in a command, if the problem occurred during command execution

(6) Collecting error information on screen displays

Obtain a hardcopy of the following information:

- The window operation when the application error occurred
- The error message dialog box
  If there is detailed information, also make a hardcopy of that information.
- The Command Prompt window or the Administrator Console window, if the error occurred during command execution
  To print the Command Prompt window or the Administrator Console window, specify the following settings for the Command Prompt Properties window:
  - **Edit options** on the **Options** page
    Select **Quick Edit Mode**.
  - **Layout** page
    For **Screen buffer size**, set **Height** to `500`.

(7) Collecting other information

Collect other necessary information.

- Content of **Accessories** > **System Tools** > **System Information**

9.5.2 How to collect data in a UNIX environment

(1) Executing the data collection command

Use the `jpcras` command to collect data needed to determine the cause of an error. Note that an OS user with `root` user permissions must perform the procedure described below.

To execute the data collection command:

1. Log on to the host where the service subject to this data collection is installed.
2. Execute the `jpcras` command with the data to be collected and the data storage directory to be used specified.

The following `jpcras` command stores all the available information in the `/tmp/jpc/agt` directory:

```
jpcras /tmp/jpc/agt all all
```

The data collected by the data collection command is compressed and stored in the specified directory by the `tar` and `compress` commands. The file name is as follows:

```
jpcrasYYMMDD#.tar.Z
```

#: *YYMMDD* is replaced with the year, month, and day.

When you execute the `jpcras` command, the `jpctool service list -id * -host *` command is executed internally in order to obtain a list of PFM services and to check their activity status. If there is a firewall between the host where the command is executed and the host for the Performance Management system or if the system configuration is large, it might take a while for the `jpctool service list -id * -host *` command to execute. In such a case, you can suppress execution of the `jpctool service list -id * -host *` command, thus reducing the command execution time, by specifying 1 in the `JPC_COLCTRLNOHOST` environment variable.

For details about the `jpcras` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(2) Executing the data collection command (for logical host operation)

Performance Management information for logical host information is on the shared disk and must be collected in both the executing system and the standby system. Use the `jpcras` command to collect data needed to determine the cause of an error. Note that an OS user with the `root` user permissions must perform the procedure described below.

To execute the data collection command for logical host operation:

1. Mount the shared disk.

   Information about the logical host is stored on the shared disk. At the executing node, make sure that the shared disk is mounted, and then collect the information.

2. Execute the `jpcras` command in both the executing system and the standby system, with the data to be collected and the data storage directory to be used specified.

   The following `jpcras` command stores all the available information in the `/tmp/jpc/agt` directory:

   ```
   jpcras /tmp/jpc/agt all all
   ```

   The data collected by the data collection command is compressed and stored in the specified directory by the `tar` and `compress` commands. The file name is as follows:

   ```
   jpcrasYYMMDD#.tar.Z
   ```

   #: *YYMMDD* is replaced with the year, month, and day.

   Executing the `jpcras` command without the `lhost` argument specified collects all the Performance Management information on the physical and logical hosts at that node. If there is a Performance Management in the logical host environment, the log files on the shared disk are acquired.

   If the `jpcras` command is executed at a node where the shared disk is not mounted, files will not be acquired from the shared disk, but the command will terminate normally without resulting in an error.

Note

Execute the data collection command at both the executing node and the standby node to collect information. To examine an event before and after failover, you need the information from both systems (executing and standby).

For details about the `jpcras` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

3. Collect information about the cluster software.

   This information is needed to determine whether the problem occurred in the cluster software or in Performance Management. Collect the information that provides control requests, such as startup and termination of Performance Management from the cluster software, and their results.

(3) Checking information about the operation

Check and save information about the operation that was underway when the error occurred. The following lists the information that you should check and save:

- Details of the operation
- Time the error occurred
- Machine configuration (such as the version of each OS, host name, and configuration of PFM - Manager and PFM - RM for Platform)
- Whether the problem is repeatable
- Performance Management user name used during logon, if the user has logged on from PFM - Web Console
- Any arguments specified in a command, if the problem occurred during command execution

(4) Collecting error information on screen displays

Collect the following error information:

- The messages that were output to the console, if the error occurred during command execution

9.6 Detecting problems within Performance Management

You can detect Performance Management errors by using JP1/Base, an integrated system monitoring product, to monitor the Performance Management log files. Performance Management also provides the status management function for checking the status of each service of PFM - Manager and PFM - RM for Platform in the event of an error. This function enables the system administrator to quickly detect an error, obtain the accurate status of the service that caused the error, and take appropriate action to recover the error.

Performance Management provides the health check function for detecting Performance Management errors. This function monitors the operating status of PFM - RM for Platform and PFM - RM host and displays the monitoring results on PFM - Web Console as changes in the operating status of PFM - RM for Platform. The automatic PFM service restart function enables the PFM service to be restarted automatically if the PFM service has stopped abnormally for some reason.

Use of the status management function that enables you to check the detailed status of Performance Management services is a prerequisite for using the health check function to monitor the operating status of PFM - RM for Platform and for using the automatic PFM service restart function to restart the PFM service automatically. Therefore, the target PFM - RM for Platform's version must support the status management function, and the status management function must be enabled. There are no prerequisite conditions for monitoring the operating status of the host. You can also use JP1/Base (integrated system monitoring product) to monitor the Performance Management log files in order to detect Performance Management errors. The system administrator can then detect a failure, identify the cause, and take appropriate action for recovery. For details about detection of Performance Management failures, see the chapter that describes detection of Performance Management failures in the *Job Management Partner 1/Performance Management User's Guide*.

9.7 Recovering from Performance Management system errors

If the Performance Management server fails, you must restore it from backup files to its normal status before the failure. For details about how to restore the status that existed before a failure, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

Appendixes

A. Estimating System Requirements

Before building a system, check whether the machine to be used is powerful enough to run PFM - RM for Platform.

A.1 Memory requirements

The memory requirements depend on the setup conditions and on the conditions under which PFM - RM for Platform will be used. The formula for estimating the memory requirements is available in the *Release Notes*.

A.2 Disk space requirements

The required disk space depends on the number of records to be used to store performance data.

To estimate the disk space required by PFM - RM for Platform, you must estimate the disk space required by the entire system and the disk space required by the Store database. The formulas for estimating these requirements are available in the *Release Notes*.

B. List of Identifiers

To operate PFM - RM for Platform or to extract performance data from the Store database of PFM - RM for Platform, identifiers might be required so that the system can identify PFM - RM for Platform. The following table shows the PFM - RM for Platform identifiers.

Table B–1: Identifiers of PFM - RM for Platform

Identifier	Name	Usage	Description
`7`	Product ID	Commands, etc.	The product ID is part of the service ID. The service ID is required when you use commands to check the configuration of the Performance Management system and when you back up performance data. For details about service IDs, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
`RMPlatform` or `agt7`	Service key		This identifier is needed in order to use commands to start and stop PFM - RM for Platform. For details about service keys, see the naming rules provided in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
`RM Platform`	Product name	Display in GUI, etc.	The product name identifies the product and is used to display information in the PFM - Web Console windows.
`pcm7`	Help ID	Help	This is the identifier for the PFM - RM for Platform Help.
`RMPLATFORM`	Product type identifier	ODBC	The product type identifier is needed in order to use SQL statements to extract data. For details, see the chapter that describes operation analysis linked with ODBC-based application programs in the *Job Management Partner 1/Performance Management User's Guide*.

C. List of Processes

This appendix describes the functions of the PFM - RM for Platform processes.

Note

These processes and the number of processes also apply to a PFM - RM for Platform that runs on a logical host.

C.1 List of Processes (for Windows)

The following table lists and describes the processes of PFM - RM for Platform. The value in parentheses following each process name is the number of processes that can run concurrently.

Table C–1: Processes of PFM - RM for Platform (in Windows)

Process name (number of processes)	Function
`jpcagt7.exe` (*n*)	Process of the Remote Monitor Collector service. One process is started for each instance of PFM - RM for Platform.
`jpcsto.exe` (*n*)	Process of the Remote Monitor Store service. One process is started for each instance of PFM - RM for Platform.
`jpc7collect.exe` (*n*)#1	Collection process. One process is started for each instance of PFM - RM for Platform.
`stpqlpr.exe` (1)#2	Process for executing Store database backup and export.
`jpc7corecollect32.exe` (1)#3	Core collection process (32-bit edition)
`jpc7corecollect64.exe` (1)#3	Core collection process (64-bit edition)

#1

Child process of the `jpcagt7.exe` process

#2

Child process of the `jpcsto.exe` process

#3

Child process of the `jpc7collect.exe` process. The `jpc7collect.exe` process starts `jpc7corecollect32.exe` in a 32-bit environment and `jpc7corecollect64.exe` in a 64-bit environment.

C.2 List of processes (for UNIX)

The following table lists and describes the processes of PFM - RM for Platform. The value in parentheses following each process name is the number of processes that can run concurrently.

Table C–2: Processes of PFM - RM for Platform (in UNIX)

Process name (number of processes)	Function
`jpcagt7` (*n*)	Process of the Remote Monitor Collector service. One process is started for each instance of PFM - RM for Platform.
`jpcsto` (*n*)	Process of the Remote Monitor Store service. One process is started for each instance of PFM - RM for Platform.

Process name (number of processes)	Function
`jpc7collect` (*n*)[#1]	Collection process. One process is started for each instance of PFM - RM for Platform.
`stpqlpr` (1)[#2]	Process for executing Store database backup and export.

#1

Child process of the `jpcagt7` process

#2

Child process of the `jpcsto` process

D. List of Port Numbers

This appendix describes the port numbers used by PFM - RM for Platform.

For details about the port numbers for PFM - Manager and PFM - Base, and the firewall passage directions, see the appendix in the manual *Job Management Partner 1/Performance Management Reference*.

You can change port numbers as appropriate to your system environment. For details about how to change port numbers, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. The TCP/IP protocol is used.

Note

Performance Management supports static NAT (Basic NAT), which performs one-to-one address conversion. It does not support dynamic NAT or NAPT (IP Masquerade, NAT+), which include a port conversion function.

D.1 Port numbers for PFM - RM for Platform

The following table shows the port numbers used by PFM - RM for Platform.

Table D–1: Port numbers used by PFM - RM for Platform

Port number	Service name	Parameter	Usage
Automatic#1	Remote Monitor Collector service	`jp1pcagt7`[*nnn*]#2	Used to bind alarms and acquire real-time reports.
	Remote Monitor Store service	`jp1pcsto7`[*nnn*]#2	Used to record performance data and acquire historical reports.

#1

If you execute the `jpcconf port define` command, a port number not being used at that time is automatically allocated and displayed. If you do not execute the `jpcconf port define` command, a port number not being used by the system is automatically allocated each time the service is restarted.

#2

If multiple instances are created, a sequence number (*nnn*) is assigned to the second and subsequent instances that are created. No sequence number is assigned to the first instance that is created.

D.2 Firewall passage directions

This subsection describes the firewall passage directions for PFM - RM for Platform.

(1) Setting the firewall passage directions

If there is a firewall between PFM - Manager and PFM - RM for Platform, you must set fixed port numbers for all services of PFM - Manager and PFM - RM for Platform.

The following table shows the firewall passage directions.

Table D–2: Firewall passage directions (between PFM - Manager and PFM - RM for Platform)

Service name	Parameter	Passage direction
Remote Monitor Collector service	`jp1pcagt7`[*nnn*]#	PFM - RM for Platform ⬅ PFM - Manager

Service name	Parameter	Passage direction
Remote Monitor Store service	`jp1pcsto7`[*nnn*]#	PFM - RM for Platform ⬅ PFM - Manager

Legend:

⬅ : Direction in which communication (connection) begins, from the right-hand item to the left-hand item.

#

If multiple instances are created, a sequence number (*nnn*) is assigned to the second and subsequent instances that are created. No sequence number is assigned to the first instance that is created.

When communication (connection) begins, the service receiving the connection request (pointed to by the arrow) uses the port number indicated in Table *D-1 Port numbers used by PFM - RM for Platform* as the reception port. The service sending the connection request uses an available port as assigned by the OS as the transmission port. The range of port numbers used depends on the OS.

Set the firewall so that the transmission port used temporarily by PFM - Manager can pass through the reception port of PFM - RM for Platform.

Note

If you execute the `jpctool db dump` or `jpctool service list` command at the PFM - RM for Platform host, specify the `proxy` option so that communication is established via PFM - Manager. Alternatively, between each PFM - RM host, set port numbers in the directions shown in the table below so that communication can pass through the firewall. For details about the `proxy` option of the `jpctool db dump` and `jpctool service list` commands, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Table D–3: Firewall passage directions (between each PFM - RM host)

Service name	Parameter	Passage direction
Remote Monitor Collector service	`jp1pcagt7`[*nnn*]#	PFM - RM ⬅ ➡ PFM - RM
Remote Monitor Store service	`jp1pcsto7`[*nnn*]#	

Legend:

⬅ ➡ : Direction in which communication (connection) begins, from the left-hand item to the right-hand item or from the right-hand item to the left-hand item.

#

If multiple instances are created, a sequence number (*nnn*) is assigned to the second and subsequent instances that are created. No sequence number is assigned to the first instance that is created.

In order to collect information from the monitored host, WMI is used for communications when the monitored host is running Windows, and SSH is used for communications when the monitored host is running UNIX. Therefore, if you place a firewall between PFM - RM for Platform and the monitored host, you must specify the settings so that communication passes through the firewall as follows:

- PFM - RM for Platform (Remote Monitor Collector service) ➡ monitored host

  Note

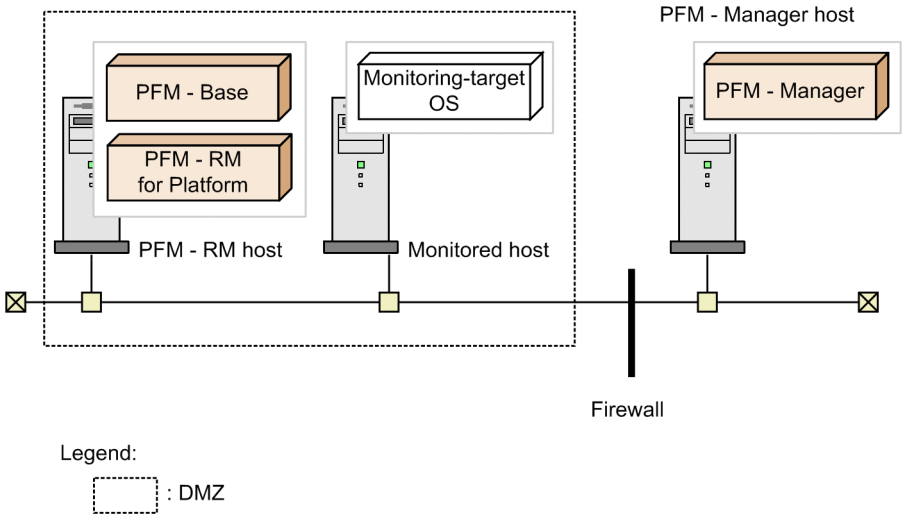
  ➡ : Direction in which communication (connection) begins, from the left-hand item to the right-hand item.

(a) When the monitored host is running Windows

WMI uses DCOM. Because DCOM uses dynamic port allocation, the port used for DCOM must pass through the firewall. For details about the setup method, see the firewall product documentation or contact the firewall product developer.

Usage with a firewall is not suitable because one WMI and DCOM request cannot be separated from another WMI and DCOM request. The following figure shows the recommended configuration.

Figure D–1: Example of an acceptable configuration for passing through a firewall with the port used in DCOM



(b) When the monitored host is running UNIX

Specify the settings so that the port number specified in the settings for the monitoring target of PFM - RM for Platform is used to pass through the firewall.

The table below shows the values that can be specified for the port number, which is a monitoring target setting. For details about the monitoring target settings, see *3.2.4 Setup procedure for the UNIX edition*.

Table D–4: Port numbers permitted for the monitoring target setting

Setting item	Description	Permitted value	Default value
Port	Port number of the SSH server on the monitored host	From 1 to 65,535	`22`

(2) Setting the firewall passage directions (when a logical host is used for operation)

If you place a firewall between PFM - Manager and PFM - RM for Platform, you must set fixed port numbers for all services of PFM - Manager and PFM - RM for Platform.

The following table shows the firewall passage directions.

Table D–5: Firewall passage directions (between PFM - Manager and PFM - RM for Platform (for logical host operation)

Service name	Parameter	Passage direction
Remote Monitor Collector service (logical host)	`jp1pcagt7`[*nnn*]#	PFM - RM for Platform (logical host) ← PFM - Manager
Remote Monitor Store service (logical host)	`jp1pcsto7`[*nnn*]#	

Legend:

⬅ : Direction in which communication (connection) begins, from the right-hand item to the left-hand item.

#

If multiple instances are created, a sequence number (*nnn*) is assigned to the second and subsequent instances that are created. No sequence number is assigned to the first instance that is created.

When communication (connection) begins, the service receiving the connection request (pointed to by the arrow) uses the port number indicated in Table *D-1 Port numbers used by PFM - RM for Platform* as the reception port. The service sending the connection request uses an available port assigned by the OS as the transmission port. The range of port numbers used depends on the OS.

Set the firewall so that the transmission port used temporarily by PFM - Manager can pass to the reception port of the logical host of PFM - RM for Platform.

(3) Setting the firewall passage directions (when the health check function is used)

If PFM - RM for Platform is to monitor the operating status of a monitored host using the health check function, you must specify the settings so that ICMP communication passes through the firewall.

The following table shows the firewall passage directions.

Table D–6: Firewall passage directions (between PFM - RM for Platform and a monitored host)

Service name	Communication protocol	Passage direction
Remote Monitor Collector service	ICMP echo request/ICMP echo response	PFM - RM host ⬅ ➡ monitored host

Legend:

⬅ ➡ : Direction in which communication (connection) begins, from the left-hand item to the right-hand item or from the right-hand item to the left-hand item.

E. Properties of PFM - RM for Platform

This appendix describes the properties of the following services and agents of PFM - RM for Platform that are displayed in PFM - Web Console:

- Remote Monitor Store service
- Remote Monitor Collector service
- Remote agents and group agents

E.1 List of properties of the Remote Monitor Store service

The following table lists and describes the properties of the Remote Monitor Store service of PFM - RM for Platform.

Table E–1: List of properties of the Remote Monitor Store service of PFM - RM for Platform

Directory name	Property name	Description
--	First Registration Date	Displays the first date and time the service was recognized by PFM - Manager.
	Last Registration Date	Displays the most recent date and time the service was recognized by PFM - Manager.
General	--	Stores information such as host names and directories. You cannot change properties stored in this directory.
	Directory	Displays the name of the current directory where the service is running.
	Host Name	Displays the name of the physical host where the service is running.
	Process ID	Displays the service's process ID.
	Physical Address	Displays the IP address and port number of the host where the service is running when the IPv6 communication facility is disabled.
	Physical Address (IPv4)	Displays the IP address (IPv4) of the host where the service is running when the IPv6 communication facility is enabled.
	Physical Address (IPv6)	Displays the IP address (IPv6) of the host where the service is running when the IPv6 communication facility is enabled.

Directory name		Property name	Description
General		Port Number	Displays the port number being used by the service that is running when the IPv6 communication facility is enabled.
		User Name	Displays the name of the user that executed the service process.
		Time Zone	Displays the time zone in which the service is used.
System		--	Stores information about the OS where the service is running. You cannot change properties stored in this directory.
		CPU Type	Displays the CPU type.
		Hardware ID	Displays the hardware ID.
		OS Type	Displays the OS type.
		OS Name	Displays the OS name.
		OS Version	Displays the OS version.
Network Services		--	Stores information about the Performance Management communication common library. You cannot change properties stored in this folder.
		Build Date	Displays the creation date of the Remote Monitor Store service.
		INI File	Displays the name of the directory containing the jpcns.ini file.
Network Services	Service	--	Stores information about the service. You cannot change properties stored in this folder.
		Description	Displays the host name in the following format: *instance-name_host-name*
		Local Service Name	Displays the service ID.
		Remote Service Name	Displays the service ID of the Master Manager service at the connection-target PFM - Manager host.
		EP Service Name	Displays the service ID of the Correlator service at the connection-target PFM - Manager host.
Retention		--	Specifies the data retention period when using Store version 1.0. Because the Remote Monitor Store service is not

Directory name		Property name	Description
Retention		--	support by Store version 1.0, you cannot change the properties stored in this directory.
		Product Interval - Minute Drawer	Displays the retention period for records of the PI record type that are collected every minute. The permitted value is fixed at Day.
		Product Interval - Hour Drawer	Displays the retention period for records of the PI record type that are collected hourly. The permitted value is fixed at Day.
		Product Interval - Day Drawer	Displays the retention period for records of the PI record type that are collected daily. The permitted value is fixed at 2Days.
		Product Interval - Week Drawer	Displays the retention period for records of the PI record type that are collected weekly. The specifiable value is fixed at Week.
		Product Interval - Month Drawer	Displays the retention period for records of the PI record type that are collected monthly. The permitted value is fixed at Month.
		Product Interval - Year Drawer	Displays the retention period for records of the PI record type that are collected yearly. The permitted value is fixed at Year.
Retention Ex		--	Sets the data retention period for Store version 2.0. For details, see the chapter that describes management of operation monitoring data in the *Job Management Partner 1/ Performance Management User's Guide*.
Retention Ex	Product Interval - *record-ID-of-PI-record-type*	--	Sets the retention period for records of the PI record type.
		Period - Minute Drawer (Day)	Specifies the retention period for records of the PI record type that are collected every minute. You can specify from 0 to 366 days in 1-day increments.
		Period - Hour Drawer (Day)	Sets the retention period for records of the PI record type that are collected hourly. The permitted value is an integer in the range from 0 to 366 (days).

Directory name		Property name	Description
Retention Ex	Product Interval - *record-ID-of-PI-record-type*	Period - Day Drawer (Week)	Sets the retention period for records of the PI record type that are collected daily. The permitted value is an integer in the range from 0 to 266 (weeks).
		Period - Week Drawer (Week)	Sets the retention period for records of the PI record type that are collected weekly. The permitted value is an integer in the range from 0 to 266 (weeks).
		Period - Month Drawer (Month)	Sets the retention period for records of the PI record type that are collected monthly. The permitted value is an integer in the range from 0 to 60 (months).
		Period - Year Drawer (Year)	Sets the retention period for records of the PI record type that are collected yearly. The permitted value is from 10 (fixed).
	Product Detail - *record-ID-of-PD-record-type*	Period (Day)	Sets the retention period for records of the PD record type for each record ID. The permitted value is an integer in the range from 0 to 366 (days).
Disk Usage		--	Stores the amount of disk space being used by each database. The property stored in this directory displays the disk usage in effect when the property is displayed. You cannot change properties stored in this directory.
		Product Interval	Displays the amount of disk space used by records of the PI record type.
		Product Detail	Displays the amount of disk space used by records of the PD record type.
		Product Alarm	Displays the amount of disk space used by records of the PA record type. PFM - RM for Platform does not use this property.
		Product Log	Displays the amount of disk space used by records of the PL record type. PFM - RM for Platform does not use this property.
		Total Disk Usage	Displays the amount of disk space used by the entire database.
Configuration		--	Displays the properties of the Remote Monitor Store service.

Directory name	Property name	Description
Configuration	Store Version	Displays the version of the Store database.
Multiple Manager Configuration	Primary Manager	Displays the host name of the monitoring manager specified as the primary manager for multiple monitoring. You cannot change this property.
	Secondary Manager	Displays the host name of the monitoring manager specified as the secondary manager for multiple monitoring. You cannot change this property.

Legend:
--: Not applicable

E.2 List of properties of the Remote Monitor Collector service

The following table lists and describes the properties of the Remote Monitor Collector service of PFM - RM for Platform.

Table E–2: List of properties of the Remote Monitor Collector service of PFM - RM for Platform

Directory name	Property name	Description
--	First Registration Date	Displays the first date and time the service was recognized by PFM - Manager.
	Last Registration Date	Displays the most recent date and time the service was recognized by PFM - Manager.
	Data Model Version	Displays the version of the data model.
General	--	Stores information such as host names and directories. You cannot change properties stored in this directory.
	Directory	Displays the name of the current directory where the service is running.
	Host Name	Displays the name of the physical host on which the service runs.
	Process ID	Displays the process ID of the service.
	Physical Address	Displays the IP address and port number of the host where the service is running when the IPv6 communication facility is disabled.
	Physical Address (IPv4)	Displays the IP address (IPv4) of the host where the service is running when the IPv6

Directory name		Property name	Description
General		Physical Address (IPv4)	communication facility is enabled.
		Physical Address (IPv6)	Displays the IP address (IPv6) of the host where the service is running when the IPv6 communication facility is enabled.
		Port Number	Displays the port number being used by the service that is running when the IPv6 communication facility is enabled.
		User Name	Displays the name of the user that executed the service process.
		Time Zone	Displays the time zone in which the service is being used.
System		--	Stores information about the OS where the service is running. You cannot change properties stored in this directory.
		CPU Type	Displays the CPU type.
		Hardware ID	Displays the hardware ID.
		OS Type	Displays the OS type.
		OS Name	Displays the OS name.
		OS Version	Displays the OS version.
Network Services		--	Stores information about the Stores information Performance Management communication common library. You cannot change properties stored in this directory.
		Build Date	Displays the creation date of the Remote Monitor Collector service.
		INI File	Displays the name of the directory containing the jpcns.ini file.
Network Services	Service	--	Stores information about the service. You cannot change properties stored in this directory.
		Description	Displays the host name in the following format: *instance-name_host-name*
		Local Service Name	Displays the service ID.

Directory name		Property name	Description
Network Services	Service	Remote Service Name	Displays the service ID of the Remote Monitor Store service to which the Remote Monitor Collector service is connected.
		EP Service Name	Displays the service ID of the Correlator service on the connection-target PFM - Manager host.
		AH Service Name	Displays the service ID of the Action Handler service on the connection-target PFM - Manager host.
JP1 Event Configurations		--	Specifies the condition for issuing JP1 events.
		Services	Specifies whether Yes or No was selected for the list items in the Remote Monitor Collector service, Remote Monitor Store service, Action Handler service, and Status Server service to issue a JP1 system event for each service.
		JP1 Event Send Host	Specifies the connection-target event server name of JP1/Base. You can only specify an event server that is running on the logical host or physical host of the same machine as that on which the Action Handler service is running. You can specify from 0 to 255 bytes of single-byte alphanumeric characters, including periods (.) or hyphens (-). If you specify a value that is outside the permitted range, it is treated as if the specification was omitted. If the value is omitted, the host where the Action Handler service is running is used as the event-issuing host. If localhost is specified, it is assumed that you mean the physical host.
		Monitoring Console Host	This property specifies the PFM - Web Console host to be started when the service that browses it is automatically executed by the startup of the JP1/IM - Manager monitor. You can specify from 0 to 255 bytes of single-byte alphanumeric characters, including periods (.) or hyphens (-). If you specify a value that is outside the permitted range, it is treated as if the specification was omitted.

Directory name		Property name	Description
JP1 Event Configurations		Monitoring Console Host	If the value is omitted, the connection-target PFM - Manager host is assumed.
		Monitoring Console Port	Specifies the port number (http request port number) on which the PFM - Web Console is to be started. You can specify from 1 to 65535. If you specify a value that is outside the permitted range, it is treated as if the specification was omitted. If the value is omitted, 20358 is set.
JP1 Event Configurations	Alarm	JP1 Event Mode	Specifies whether to issue a JP1 system event or a JP1 user event when the alarm status changes. • JP1 User Event: Issues a JP1 user event. • JP1 System Event: Issue a JP1 system event.
Detail Records		--	Stores the properties of records of the PD record type. The record IDs of the collected records are displayed in boldface type.
Detail Records	*record-ID*#1	--	Stores the properties of a record.
		Description	Displays a description of the record. You cannot change this property.
		Log	Displays Yes or No, indicating whether records are to be recorded in the Store database of PFM - RM for Platform. No is always displayed here.
		Log (ITSLM)	Displays Yes or No, indicating whether records are to be recorded in the Store database of PFM - RM for Platform from JP1/ITSLM - Manager when JP1/ITSLM - Manager is linked. If JP1/ITSLM - Manager is not linked, this property is fixed at No. You cannot change this property.
		Monitoring (ITSLM)	Displays Yes or No, based on the setting in JP1/ITSLM - Manager, indicating whether records are to be sent to JP1/ITSLM - Manager when JP1/ITSLM - Manager is linked. If JP1/ITSLM - Manager is not linked, this property is fixed at No. You cannot change this property.

Directory name		Property name	Description
Detail Records	*record-ID*[#1]	Collection Interval[#2]	Specifies the data collection interval. The permitted value is from 0 to 2,147,483,647 seconds in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.
		Collection Offset[#2]	Specifies the offset value (in seconds) for starting data collection. This value must be in the range from 0 to 32,767 seconds but cannot exceed the value specified for Collection Interval. The data collection logging time does not depend on the Collection Offset value and is the same as the Collection Interval.
		Sync Collection With[#2]	Displays the records whose collection is to be synchronized, in *record-type*, *record-ID* format.
		Over 10 Sec Collection Time	Displays record collection time only when historical data collection takes priority over real-time report display processing[#3]. Whether the collection of records takes 10 seconds or longer is displayed as Yes or No. • Yes: Sometimes takes 10 seconds or longer. • No: Takes less than 10 seconds. You cannot change this property.
		LOGIF	Specifies the conditions for storing records in the database. Only records that satisfy the conditions are stored in the database. The system displays the conditional expression (character string) that was created in the LOGIF Expression Editor window, which is displayed by clicking **LOGIF** in the lower frame of the properties window for the service that is displayed on PFM - Web Console's **Services** page.
Interval Records		--	Stores the properties of records of the PI record type. The record IDs of the collected records are displayed in boldface type.
Interval Records	*record-ID*[#1]	--	Stores the properties of a record.

Directory name		Property name	Description
Interval Records	*record-ID*[#1]	Description	Displays a description of the record. You cannot change this property.
		Log	Displays Yes or No indicating whether records are to be recorded in the Store database of PFM - RM for Platform. No is always displayed here.
		Log (ITSLM)	Displays Yes or No, indicating whether records are to be recorded in the Store database of PFM - RM for Platform from JP1/ITSLM - Manager when JP1/ITSLM - Manager is linked. If JP1/ITSLM - Manager is not linked, this property is fixed at No. You cannot change this property.
		Monitoring (ITSLM)	Displays Yes or No, based on the setting in JP1/ITSLM - Manager, indicating whether records are to be sent to JP1/ITSLM - Manager when JP1/ITSLM - Manager is linked. If JP1/ITSLM - Manager is not linked, this property is fixed at No. You cannot change this property.
		Collection Interval	Specifies the data collection interval. The permitted value is from 0 to 2,147,483,647 seconds in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.
		Collection Offset	Specifies the offset value (in seconds) for starting data collection. This value must be in the range from 0 to 32,767 seconds but cannot exceed the value specified for Collection Interval. The data collection logging time does not depend on the Collection Offset value and is the same as the Collection Interval.
		Over 10 Sec Collection Time	Displays record collection time only when historical data collection takes priority over real-time report display processing[#3]. Whether the collection of records takes 10 seconds or longer is displayed as Yes or No. • Yes: Sometimes takes 10 seconds or longer.

Directory name		Property name	Description
Interval Records	*record-ID*#1	Over 10 Sec Collection Time	• No: Takes less than 10 seconds. You cannot change this property.
		LOGIF	Specifies the conditions for storing records in the database. Only records that satisfy the conditions are stored in the database. The system displays the conditional expression (character string) that was created in the LOGIF Expression Editor window, which is displayed by clicking **LOGIF** in the lower frame of the properties window for the service that is displayed on PFM - Web Console's **Services** page.
Log Records		--	Stores the properties of records of the PL type. PFM - RM for Platform does not use this property.
Monitoring Targets		--	Stores the properties of the monitored host that is monitored by PFM - RM for Platform.
Monitoring Targets	*monitoring-target-name*	--	Displays a description of the monitoring target. As many descriptions are displayed as there are monitoring targets.
		Target Name	Displays the name of the monitoring target. You cannot change this property.
		Target Host	Displays the name of the monitored host. You cannot change this property.
Health Check Configurations		Health Check for Target Hosts	Specifies whether to poll monitored hosts. This property applies to all monitored hosts in an instance.
Restart Configurations		--	Specifies the conditions for automatically restarting the PFM service.
		Restart when Abnormal Status	Specifies whether to automatically restart a service when the Status Server service cannot normally acquire the status of the Action Handler service, Remote Monitor Collector service, and Remote Monitor Store service.
		Restart when Single Service Running	Specifies whether to automatically restart a service when only the Remote Monitor

Directory name		Property name	Description
Restart Configurations		Restart when Single Service Running	Store service or Remote Monitor Collector service has started.
Restart Configurations	Remote Monitor Collector	Auto Restart	Specifies whether to use the auto restart function on the Remote Monitor Collector service.
		Auto Restart - Interval (Minute)	Specifies the interval at which to check the operation status of a service when the auto restart function is used. You can specify from 1 to 1,440 minutes in 1-minute increments.
		Auto Restart - Repeat Limit	Specifies the number of continuous retries, as an integer from 1 to 10, when the auto restart function is used.
		Scheduled Restart	Select Yes or No from the list items to indicate whether the scheduled restart function will be used on the Remote Monitor Collector service.
		Scheduled Restart - Interval	Specifies the restart interval, as an integer from 1 to 1000, when the scheduled restart function is used.
		Scheduled Restart - Interval Unit	Select Day, Week, or Month from the item list to indicate the unit for the restart interval when the scheduled restart function is used.
		Scheduled Restart - Origin - Year	Specifies the year when a restart will be executed, as an integer from 1971 to 2035.
		Scheduled Restart - Origin - Month	Specifies the month when a restart will be executed, as an integer from 1 to 12.
		Scheduled Restart - Origin - Day	Specifies the day when a restart will be executed, as an integer from 1 to 31.
		Scheduled Restart - Origin - Hour	Specifies the time (hour) when a restart will be executed, as an integer from 0 to 23.
		Scheduled Restart - Origin - Minute	Specifies the time (minutes) when a restart will be executed, as an integer from 0 to 59.
	Remote Monitor Store	Auto Restart	Specifies whether to use the auto restart function on the Remote Monitor Store service.
		Auto Restart - Interval (Minute)	Specifies the interval at which to check the operation status of a service when the auto restart

Directory name		Property name	Description
Restart Configurations	Remote Monitor Store	Auto Restart - Interval (Minute)	function is used. You can specify from 1 to 1,440 minutes in 1-minute increments.
		Auto Restart - Repeat Limit	Specifies the number of continuous retries, as an integer from 1 to 10, when the auto restart function is used.
		Scheduled Restart	Select Yes or No from the item list to indicate whether the scheduled restart function will be used on the Remote Monitor Store service.
		Scheduled Restart - Interval	Specifies the restart interval, as an integer from 1 to 1000, when the scheduled restart function is used.
		Scheduled Restart - Interval Unit	Select Day, Week, or Month from the item list to indicate the unit for the restart interval when the scheduled restart function is used.
		Scheduled Restart - Origin - Year	Specifies the year when a restart will be executed, as an integer from 1971 to 2035.
		Scheduled Restart - Origin - Month	Specifies the month when a restart will be executed, as an integer from 1 to 12.
		Scheduled Restart - Origin - Day	Specifies the day when a restart will be executed, as an integer from 1 to 31.
		Scheduled Restart - Origin - Hour	Specifies the time (hour) when a restart will be executed, as an integer from 0 to 23.
		Scheduled Restart - Origin - Minute	Specifies the time (minutes) when a restart will be executed, as an integer from 0 to 59.
	Action Handler	Auto Restart	Specifies whether to use the auto restart function on the Action Handler service.
		Auto Restart - Interval (Minute)	Specifies the interval at which to check the operation status of a service when the auto restart function is used. You can specify from 1 to 1,440 minutes in 1-minute increments.
		Auto Restart - Repeat Limit	Specifies the number of continuous retries, as an integer from 1 to 10, when the auto restart function is used.
		Scheduled Restart	Select Yes or No from the item list to indicate whether the scheduled restart function will

Directory name		Property name	Description
Restart Configurations	Action Handler	Scheduled Restart	be used on the Action Handler service.
		Scheduled Restart - Interval	Specifies the restart interval, as an integer from 1 to 1000, when the scheduled restart function is used.
		Scheduled Restart - Interval Unit	Select Day, Week, or Month from the item list to indicate the unit for the restart interval when the scheduled restart function is used.
		Scheduled Restart - Origin - Year	Specifies the year when a restart will be executed, as an integer from 1971 to 2035.
		Scheduled Restart - Origin - Month	Specifies the month when a restart will be executed, as an integer from 1 to 12.
		Scheduled Restart - Origin - Day	Specifies the day when a restart will be executed, as an integer from 1 to 31.
		Scheduled Restart - Origin - Hour	Specifies the time (hour) when a restart will be executed, as an integer from 0 to 23.
		Scheduled Restart - Origin - Minute	Specifies the time (minutes) when a restart will be executed, as an integer from 0 to 59.
ITSLM Connection Configuration		--	Displays information about the JP1/ITSLM - Manager that is linked.
ITSLM Connection Configuration	ITSLM Connection	--	Displays information about the connection-target JP1/ITSLM - Manager.
		ITSLM Host	Displays the host name of the connected JP1/ITSLM - Manager. This property is not displayed when JP1/ITSLM - Manager is not connected.
		ITSLM Port	Displays the port number of the connected JP1/ITSLM - Manager. This property is not displayed when JP1/ITSLM - Manager is not connected.
	MANAGE ITSLM CONNECTION	--	Specifies whether to terminate the connection to JP1/ITSLM - Manager.
		DISCONNECT ITSLM CONNECTION	Specifies from the item list the host name of the JP1/ITSLM - Manager whose connection is to be terminated. If a blank character is specified from the item list, no action is taken. Only a blank character is

Directory name		Property name	Description
ITSLM Connection Configuration	MANAGE ITSLM CONNECTION	DISCONNECT ITSLM CONNECTION	displayed in the item list if JP1/ITSLM - Manager is not connected.
Multiple Manager Configuration		Primary Manager	Displays the host name of the manager specified as the primary manager for multiple monitoring. You cannot change this property.
		Secondary Manager	Displays the host name of the manager specified as the secondary manager for multiple monitoring. You cannot change this property.
Remote Monitor Configuration		--	Stores the setting properties specific to PFM - RM for Platform.
Remote Monitor Configuration	Remote Monitor	--	Displays an overview of the Remote Monitor Collector service.
		Product	Displays 7 as the product ID.
		Instance	Displays the instance name specified in the jpcconf inst setup command.
		UseCommonAccount	Displays the value of UseCommonAccount, which was specified when the instance environment was set up. Not Supported is displayed in environments where common account information is not supported. You cannot change this property. This property is supported only when the PFM - RM host is running Windows.
		Interval	Displays the value of Interval, which was specified when the instance environment was set up. You can change this property.
		Std_Category	Displays the value of StdCategory, which was specified when the instance environment was set up. You can change this property.
		Disk_Category	Displays the value of DiskCategory, which was specified when the instance environment was set up. You can change this property.
		Network_Category	Displays the value of NetworkCategory, which

Directory name		Property name	Description
Remote Monitor Configuration	Remote Monitor	Network_Category	was specified when the instance environment was set up. You can change this property.
		Ps_Category	Displays the value of PsCategory specified when the instance environment was set up. You can change this property.
		RMHost_User	• Displays the value of RMHost_User, which was specified when the instance environment was set up. You can change this property.#4 • Displays the value of User in common account information (pfmhost) when Y is specified for UseCommonAccount in an environment where common account information can be used. This property is supported only when the PFM - RM host is running Windows.
		RMHost_Password	**** (fixed) is displayed. You cannot change this property. This property is supported only when the PFM - RM host is running Windows.
		RMHost_Domain	• Displays the value of RMHost_Domain, which was specified when the instance environment was set up. You can change this property.#4 • Displays the value of Domain in common account information (pfmhost) when Y is specified for UseCommonAccount in an environment where common account information can be used. You cannot change this property. This property is supported only when the PFM - RM host is running Windows.
		SSH_Client	Displays the value specified in SSH_Client when the instance environment was set up. You can change this property.

Directory name		Property name	Description
Remote Monitor Configuration	Remote Monitor	SSH_Client	This property is supported only when the PFM - RM host is running Windows. You must specify this property when the monitored host is running UNIX.
		Perl_Module	Displays the value specified in Perl_Module when the instance environment was set up. You can change this property. This property is supported only when the PFM - RM host is running Windows. You must specify this property when the monitored host is running UNIX.
		Log_Size	Displays the value of Log_Size, which was specified when the instance environment was set up. You can change this property.

Legend:

--: Not applicable

#1

The directory name shows the record ID without the database ID. For details about the record ID of each record, see *7. Records*.

#2

If Sync Collection With is displayed, Collection Interval and Collection Offset are not displayed.

#3

For details, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

#4

To apply the new values, restart the Remote Monitor Collector service.

E.3 List of properties of remote agents and group agents

The following table lists and describes the properties of remote agents and group agents of PFM - RM for Platform.

Table E–3: List of properties of remote agents and group agents of PFM - RM for Platform

Directory name	Property name	Description	Remote agent	Group agent
--	First Registration Date	Displays the first date and time the service was recognized by PFM - Manager.	D	D
	Last Registration Date	Displays the most recent date and time the service was recognized by PFM - Manager.	D	D
	Data Model Version	Displays the version of the data model.	D	D

Directory name		Property name	Description	Remote agent	Group agent
Remote Monitoring		--	Stores the properties of the remote agent or group agent.	D	D
		Agent Type	Displays the type of Agent: • Remote Agent: For remote agent • Group Agent: For group agent	D	D
		Remote Monitor Name	Displays the service ID of PFM - RM for Platform.	D	D
		Target Name	Displays the name of the monitoring target.	D	N
		Target Host	Displays the name of the monitored host.	D	N
		Group Name	Displays the group name.	N	D
		Primary Host	Displays the primary host name.	N	D
		Grouping Targets	Displays a list of target names that are to be summarized.	N	D
Detail Records		--	Stores the properties of records of the PD record type. The record IDs of the collected records are displayed in boldface type.	D	D
Detail Records	*record-ID*[#1]	--	Stores the properties of a record.	D	D
		Description	Displays a description of the record.	D	D
		Log[#2, #3]	Displays Yes or No indicating whether records are to be recorded in the Store database of PFM - RM for Platform. If this value is set to Yes and Collection Interval is set to a value greater than 0, records are recorded into the database.	U	U
		Log (ITSLM)[#2, #3]	Displays Yes or No indicating whether records are to be recorded in the Store database of PFM - RM for Platform from JP1/ITSLM - Manager. If this value is set to Yes and Collection Interval is set to a value greater than 0, the record is recorded into the database. You cannot change this property.	D	D

Directory name		Property name	Description	Remote agent	Group agent
Detail Records	*record-ID*[#1]	Monitoring (ITSLM)	Displays Yes or No, based on the setting in JP1/ITSLM - Manager, indicating whether records are to be sent to JP1/ITSLM - Manager. You cannot change this property.	D	D
		Collection Interval[#4]	Specifies the data collection interval. The permitted value is from 0 to 2,147,483,647 seconds in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.	D[#5]	D[#5]
		Collection Offset[#4]	Specifies the offset value (in seconds) for starting data collection. This value must be in the range from 0 to 32,767 seconds but cannot exceed the value specified for Collection Interval. The data collection logging time does not depend on the Collection Offset value and is the same as the Collection Interval.	D[#5]	D[#5]
		Sync Collection With[#4]	Displays the records whose collection is to be synchronized, in *record-type*,*record-ID* format.	D	D
		Over 10 Sec Collection Time	Displays record collection time only when historical data collection takes priority over real-time report display processing[#6]. Whether the collection of records takes 10 seconds or longer is displayed as Yes or No. • Yes: Sometimes takes 10 seconds or longer. • No: Takes less than 10 seconds. You cannot change this property.	D	D
		Realtime Report Data Collection Mode	Displays report data collection mode only when historical data collection takes priority over real-time report display processing[#6].	U	U

Directory name		Property name	Description	Remote agent	Group agent
Detail Records	*record-ID*[#1]	Realtime Report Data Collection Mode	Specify either of the following real-time report display modes: • Reschedule: Reschedule mode • Temporary Log: Temporary log mode If you specify Yes for Over 10 Sec Collection Time, you must specify Temporary Log (temporary log mode) for this property.	U	U
		LOGIF	Specifies the conditions for storing records in the database. Only records that satisfy the conditions are stored in the database. The system displays the conditional expression (character string) that was created in the LOGIF Expression Editor window, which is displayed by clicking **LOGIF** in the lower frame of the properties window for the service that is displayed on PFM - Web Console's **Services** page.	D[#5]	D[#5]
Interval Records		--	Stores the properties of records of the PI record type. The record IDs of the collected records are displayed in boldface type.	D	D
Interval Records	*record-ID*[#1]	--	Stores the properties of a record.	D	D
		Description	Displays a description of the record. You cannot change this property.	D	D
		Log[#3]	Displays Yes or No indicating whether records are to be recorded in the Store database of PFM - RM for Platform. If this value is set to Yes and Collection Interval is set to a value greater than 0, records are recorded in the database.	U	U
		Log (ITSLM)[#3]	Displays Yes or No indicating whether records are to be recorded in the Store database of PFM - RM for Platform from JP1/ITSLM - Manager. If this	D	D

Directory name		Property name	Description	Remote agent	Group agent
Interval Records	*record-ID*[#1]	Log (ITSLM)[#3]	value is set to Yes and Collection Interval is set to a value greater than 0, the record is recorded into the database. You cannot change this property.	D	D
		Monitoring (ITSLM)	Displays Yes or No, based on the setting in JP1/ITSLM - Manager, indicating whether records are to be sent to JP1/ITSLM - Manager. You cannot change this property.	D	D
		Collection Interval	Specifies the data collection interval. The permitted value is from 0 to 2,147,483,647 seconds in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.	D[#5]	D[#5]
		Collection Offset	Specifies the offset value (in seconds) for starting data collection. This value must be in the range from 0 to 32,767 seconds but cannot exceed the value specified for Collection Interval. The data collection logging time does not depend on the Collection Offset value and is the same as the Collection Interval.	D[#5]	D[#5]
		Over 10 Sec Collection Time	Displays record collection time only when historical data collection takes priority over real-time report display processing[#6]. Whether the collection of records takes 10 seconds or longer is displayed as Yes or No. • Yes: Sometimes takes 10 seconds or longer. • No: Takes less than 10 seconds. You cannot change this property.	D	D
		Realtime Report Data Collection Mode	Displays report data collection mode only when historical data collection	U	U

Directory name		Property name	Description	Remote agent	Group agent
Interval Records	*record-ID*[#1]	Realtime Report Data Collection Mode	takes priority over real-time report display processing[#6]. Specify either of the following real-time report display modes: • Reschedule: Reschedule mode • Temporary Log: Temporary log mode If you specify Yes for Over 10 Sec Collection Time, you must specify Temporary Log (temporary log mode) for this property.	U	U
		LOGIF	Specifies the conditions for storing records in the database. Only records that satisfy the conditions are stored in the database. The system displays the conditional expression (character string) that was created in the LOGIF Expression Editor window, which is displayed by clicking **LOGIF** in the lower frame of the properties window for the service that is displayed on PFM - Web Console's **Services** page.	D[#5]	D[#5]
Log Records		--	Stores the properties of records of the PL type. PFM - RM for Platform does not use this property.	D	D
Remote Monitor Configuration		--	Stores the setting properties specific to the monitoring target.	D	N
Remote Monitor Configuration	Target	--	Displays an overview of the service of the remote agent.	D	N
		UseCommonAccount	Displays Y or N to indicate whether to use common account information. • Y: Use • N: Do not use Not Supported is displayed in environments where common account information is not supported. You cannot change this property.	D	D

Directory name		Property name	Description	Remote agent	Group agent
Remote Monitor Configuration	Target	TargetType	Displays the method to be used for connecting to the monitored host. You cannot change this property. This property is supported only when the PFM - RM host is running Windows. • wmi: WMI (when the monitored host is also running Windows) • ssh: SSH (when the monitored host is also running UNIX)	D	N
		User	• Specifies the user ID to be used for connecting to the monitored host. • Displays the value#7 specified in common account information when Y is specified for UseCommonAccount in an environment where common account information can be used. You cannot change this property.	U	N
		Password	**** (fixed) is displayed. You cannot change this property. This property is supported only when the monitored host is running Windows.	D	N
		Domain	• Specifies the domain name to which the monitored host belongs. • Displays the value of Domain in common account information (wmi) when Y is specified for UseCommonAccount in an environment where common account information can be used. You cannot change this property. This property is supported only when the monitored host is running Windows.	U	N
		Private_Key_File	• Specifies the name of the private key file that is to be used with the SSH public key method. • Displays the value of Private_Key_File in common account	U	N

Directory name			Property name	Description	Remote agent	Group agent
Remote Monitor Configuration	Target		Private_Key_File	information (ssh) when Y is specified for UseCommonAccount in an environment where common account information can be used. You cannot change this property. This property is supported only when the monitored host is running UNIX.	U	N
			Port	This is the port number of the SSH server on the monitored host. This property is supported only when the monitored host is running UNIX.	U	N
	Application monitoring setting		Case Sensitive	Specifies whether comparisons when evaluating monitoring condition will be case-sensitive. • Yes: Case-sensitive • No: Not case-sensitive	U	N
	Application monitoring setting	*application-name*[#8]	--	Displays the name of the application that has been added.	D	N
			Virtual Environment ID	Specifies a maximum of 63 bytes as a virtual environment identifier for specifying the range of data to be collected from the processes for PD_APP2, PD_APPC, and PD_APPD records. If this property is not specified, data is collected from all processes.	U	N
			Monitoring[01-15] Label[#9]	Specifies a maximum of 31 bytes as the name for identifying the monitoring condition. By default, Monitoring [01-15] is set. If this property is not specified, Monitoring [01-15] is set. You must specify a unique value for this property.	U	N
			Monitoring[01-15] Field[#9]	Displays the fields to be monitored. • None: Not specified • Program Name: Refers to the value in the	U	N

Directory name			Property name	Description	Remote agent	Group agent
Remote Monitor Configuration	Application monitoring setting	*application-name*#8	Monitoring[01-15] Field#9	Program Name field of the PD_APS record. • Command Line: Refers to the value in the Command Line field of the PD_APS record. • Service Name: Refers to the value in the Service Name field of the PD_ASVC record.	U	N
			Monitoring[01-15] Condition#9	Specifies a maximum of 127 bytes for the monitoring condition when using a version of PFM - RM for Platform that is earlier than 10-00. Specifies a maximum of 4,096 bytes for the monitoring condition when using version 10-00 (or later) of PFM - RM for Platform.	U	N
			Monitoring[01-15] Range#9	Specifies the lower and upper threshold values for the number of monitoring targets, connecting the two values with a hyphen (-), such as 1-2. You can specify from 0 to 65535.	U	N
	ADDITION OR DELETION A SETTING		ADD AN APPLICATION MONITORING SETTING	Specifies a maximum of 63 bytes for the name of the application to be added. You must specify a unique value for this property.	U	N
			DELETE AN APPLICATION MONITORING SETTING	Specifies the name of the application to be deleted. By default, no application name is displayed.	U	N

Legend:

--: Not applicable

U: Displayed and updatable

D: Displayed but not updatable

N: Not displayed

#1

The directory name shows the record ID without the database ID. For details about the record ID of each record, see *7. Records*.

#2

For PD_APPD, PD_APS, and PD_ASVC records, the value of this property is fixed at No. (You cannot change it to Yes.)

#3

If either of these property values are Yes, records are recorded in the Store database.

#4

If Sync Collection With is displayed, Collection Interval and Collection Offset are not displayed.

#5

The value set by PFM - RM for Platform is displayed.

#6

For details, see the chapter that describes troubleshooting in the *Job Management Partner 1/Performance Management User's Guide*.

#7

If the PFM - RM host is running Windows:

If the value of `TargetType` indicates that the monitored host is running Windows, the value of `User` in common account information (wmi) is displayed.

If the value of `TargetType` indicates that the monitored host is running UNIX, the value of `User` in common account information (ssh) is displayed.

If the PFM - RM host is running UNIX:

The value of `User` in common account information (ssh) is displayed.

#8

For the directory name, the application specified in the `ADD AN APPLICATION MONITORING SETTING` property is displayed.

#9

In the specification of `Monitoring[01-15] Label`, `Monitoring[01-15] Field`, `Monitoring[01-15] Condition`, and `Monitoring[01-15] Range`, `[01-15]` means that a number from `01` to `15` is entered there. For example, when actual property items are displayed, they would appear as `Monitoring01 Label`, `Monitoring06 Field`, `Monitoring10 Condition`, or `Monitoring15 Range`.

F. List of Directories and Files

This appendix lists the directories and files of PFM - RM for Platform.

The following shows the installation directory for Performance Management.

In Windows

You can specify any folder as the installation folder for Performance Management. The following is the default installation folder:

- In Windows Server 2003 (x64), the 64-bit edition of Windows Server 2008, and Windows Server 2012
  system-drive`\Program Files (x86)\Hitachi\jp1pc`
- All other cases
  system-drive`\Program Files\Hitachi\jp1pc`

In UNIX

The installation directory for Performance Management is `/opt/jp1pc/`.

F.1 List of folders and files (for Windows)

The following table lists the folders and files for the Windows edition of PFM - RM for Platform.

Table F–1: List of folders and files for PFM - RM for Platform (for Windows)

Folder name	File name	Description
installation-folder\	--	Installation folder or environment folder
	`instagt7.ini`	Intermediate file for internal processing
installation-folder`\agt7\`	--	Base folder of PFM - RM for Platform
	`insrules.dat`	Intermediate file for internal processing
	`jpcagtras.bat`	Maintenance data collection program
	`PATCHLOG.TXT`	Intermediate file for internal processing
	`readme.txt`	Readme text
	`version.txt`	Version information
installation-folder`\agt7\agent\`	--	Base folder of the Remote Monitor Collector service
	`agtlist.ini`	Intermediate file for internal processing
	`GARULES.DAT`	Grouping rule description file (master)
	`jpcagt.ini.instmpl`	Intermediate file for internal processing

Folder name	File name	Description
installation-folder\agt7\agent\	jpcagt7.exe	Executable program of the Remote Monitor Collector service
	target.ini.tmpl	Template file for setting the monitoring target
	group.ini.tmpl	Template file for setting the group agent
	targetrules.dat	Monitoring target creation rule file
installation-folder\agt7\agent*instance-name*\	--	Base folder of the Remote Monitor Collector service. Files under this folder are created for each instance.
	GARULES.DAT	Grouping rule description file
	grouplist.ini	List of groups
	jpcagt.ini	Service startup initialization file of Remote Monitor Collector
	jpcagt.ini.model	Sample of a service startup initialization file of Remote Monitor Collector
	status.dat	Intermediate file for internal processing
	suspended.dat	Monitoring suspension information file
	targetlist.ini	List of monitoring targets
	tstatuses.dat	Virtual Agent status information[#1]
installation-folder\agt7\agent*instance-name*\groups\	--	Folder for the group agent
	group-name.ini	Group agent settings file
installation-folder\agt7\agent*instance-name*\log\	--	Storage folder for the internal log file of the Remote Monitor Collector service (for each instance)
	collect_core_*nn*[#2]	Internal log file
	collect_*nn*[#2]	
	timer_core_*nn*[#2]	
	timer_*nn*[#2]	
	target_*monitoring-target-name*_*nn*[#2]	
	• msglog01 • msglog02	

Folder name	File name	Description
installation-folder\agt7\agent*instance-name*\log\	• nslog01 • nslog02	Internal log file
installation-folder\agt7\agent*instance-name*\targets\	--	Folder for the remote agent
	monitoring-target-name.ini	Monitoring target settings file
	monitoring-target-name.ini.model	Sample of a monitoring target settings file
	*monitoring-target-name*_jpcapp	Application definition file
	*monitoring-target-name*_suspended.dat	Monitoring suspension information file
	corecollect.stderr	Result of collection process (stderr)
	corecollect.stdout	Result of collection process (stdout)
installation-folder\agt7\agent*instance-name*\targets*monitoring-target-name*\	--	Work folder
	records.dat	Performance information file
	records.stdout	Performance information file[#3]
	records.stderr_*NNNN*[#4]	Error information collection file
	common.stdout_*NNNN*[#4]	Result of a common command (stdout)
	common.stderr_*NNNN*[#4]	Result of a common command (stderr)
	os.stdout_*NNNN*[#4]	Result of an OS-specific command (stdout)
	os.stderr_*NNNN*[#4]	Result of an OS-specific command (stderr)
	wmi.out_*NNNN*[#4]	wmi performance information file
installation-folder\agt7\bin\	--	Command storage folder
	jpc7collect.exe	Collection process
	jpcagt7hcc.dll	HCCLib common library
	jpc7corecollect32.exe	Collection child process (32-bit edition)
	jpc7corecollect64.exe	Collection child process (64-bit edition)
	jpcagt7hcc64.dll	HCCLib common library (64-bit edition)
installation-folder\agt7\dat\	--	Data storage directory for collection processes

Folder name	File name	Description
installation-folder\agt7\dat\	common.dat	Storage file for common execution commands
	cmd2rec	File creation script for record information
	cmd2rec_common	File creation script for record information (common to all OSs)
	cmd2rec_*OS*	File creation script for record information (for each OS)
	OS.dat	Execution command storage file for each category (for each OS)
installation-folder\agt7\lib\	--	Storage folder for libraries
	jpcagt7msg.dll	Message catalog file
installation-folder\agt7\store\	--	Base folder of the Remote Monitor Store service
	STDICT.DAT	Data model definition file
	STRULES.DAT	
	stolist.ini	Intermediate file for internal processing
	jpcsto.ini.instmpl	
installation-folder\agt7\store*instance-name*\	--	Base folder of the Remote Monitor Store service. Files under this folder are created for each instance.
	*.DB	Performance data files
	*.IDX	Index files for performance data files
	*.LCK	Lock files for performance data files
	jpcsto.ini	Service startup initialization file of Remote Monitor Store
	jpcsto.ini.model	Sample of a service startup initialization file of Remote Monitor Store
	status.dat	Intermediate file for internal processing
	STDICT.DAT	Data model definition file
	STRULES.DAT	
installation-folder\agt7\store*instance-name*\backup\	--	Default database backup folder
installation-folder\agt7\store*instance-name*\dump\	--	Default database export folder

Folder name	File name	Description
installation-folder\agt7\store*instance-name*\import\	--	Default database import folder
installation-folder\agt7\store*instance-name*\log\	--	Internal log file storage folder for the Remote Monitor Collector service
	• msglog01 • msglog02	Internal log file
	• nslog01 • nslog02	
installation-folder\agt7\store*instance-name*\partial\	--	Default database partial backup folder
installation-folder\agt7\store*instance-name*\STPD\	--	PD record storage folder
installation-folder\agt7\store*instance-name*\STPI\	--	
installation-folder\agt7\store*instance-name*\STPL\	--	
installation-folder\log\	--	Common log folder
	jpclog*	Common logs
installation-folder\setup\	--	Setup file storage folder
	extract	Extraction folder for setup information
	jpcagt7u.Z	Archive file for PFM - RM for Platform setup (UNIX)
	jpcagt7w.EXE	Archive file for PFM - RM for Platform setup (Windows)
installation-folder\patch_files\agt7\	--	Storage folder for patch files (for agent)

Legend:

--: Not applicable

#1

Created if the health check function is enabled.

#2

nn is from 01 to 04.

#3

This folder is created temporarily.

#4

NNNN can be any value from 0002 to 0012.

The re-distribution files for Visual Studio are also installed. The following table lists and describes the re-distribution files for Visual Studio 2010 that are installed.

Table F–2: List of re-distribution files for Visual Studio 2010 that are installed in a Windows environment

OS	Folder name	File name	Description
32-bit	%Systemroot%\system32	msvcp100.dll	Microsoft Visual C++ 2010 SP1 CRT re-distribution file (for x86)
		msvcr100.dll	
64-bit	%Systemroot%\SysWOW64	msvcp100.dll	Microsoft Visual C++ 2010 SP1 CRT re-distribution file (for x86)
		msvcr100.dll	
	%Systemroot%\system32	msvcp100.dll	Microsoft Visual C++ 2010 SP1 CRT re-distribution file (for x86)
		msvcr100.dll	

F.2 List of directories and files (for UNIX)

The following table lists the directories and files for the UNIX edition of PFM - RM for Platform.

Table F–3: List of directories and files for PFM - RM for Platform (for UNIX)

Directory name	File name	Permission	Description
installation-directory/	--	755	Installation folder or environment directory
	instagt7.ini	644	Intermediate file for internal processing
installation-directory/agt7/	--	755	Base directory of PFM - RM for Platform
	insrules.dat	444	Intermediate file for internal processing
	jpcagtras	555	Maintenance data collection program
	patch_history	644	Intermediate file for internal processing
	PATCHLOG.TXT		
installation-directory/agt7/.ssh/	--	700	Directory for storing private and public key files
	agt7	600	Private key file
	agt7.pub	644	Public key file
installation-directory/agt7/agent/	--	755	Base directory of the Remote Monitor Collector service
	agtlist.ini	644	Intermediate file for internal processing
	GARULES.DAT	444	Grouping rule description file (master)

Directory name	File name	Permission	Description
installation-directory/agt7/agent/	jpcagt.ini.instmpl	444	Intermediate file for internal processing
	jpcagt7	555	Executable program of the Remote Monitor Collector service
	target.ini.tmpl	444	Template file for setting the monitoring target
	group.ini.tmpl		Template file for setting the group agent
	targetrules.dat		Monitoring target creation rule file
installation-directory/agt7/agent/*instance-name*/	--	755	Base directory of the Remote Monitor Collector service. Files under this directory are created for each instance.
	GARULES.DAT	444	Grouping rule description file
	grouplist.ini	644	List of groups
	jpcagt.ini	600	Service startup initialization file of Remote Monitor Collector
	jpcagt.ini.lck	777	Lock file for the service startup initialization file of Remote Monitor Collector (for each instance)
	jpcagt.ini.model	444	Sample of a service startup initialization file of Remote Monitor Collector
	status.dat	600	Intermediate file for internal processing
	suspended.dat	644	Monitoring suspension information file
	targetlist.ini	644	List of monitoring targets
	tstatuses.dat	600	Virtual Agent status information[#1]
installation-directory/agt7/agent/*instance-name*/groups/	--	755	Directory for the group agent
	group-name.ini	644	Group agent settings file
installation-directory/agt7/agent/*instance-name*/log/	--	777	Storage directory for the internal log file of the Remote Monitor Collector service (for each instance)
	collect_*nn*[#2]	666	Internal log file
	timer_*nn*[#2]		
	target_*monitoring-target-name*_*nn*[#2]		
	• msglog01 • msglog02		
	• nslog01 • nslog02		

Directory name	File name	Permission	Description
installation-directory/agt7/agent/*instance-name*/targets/	--	755	Directory for the remote agent
	monitoring-target-name.ini	600	Monitoring target settings file
	monitoring-target-name.ini.model	400	Sample of a monitoring target settings file
	*monitoring-target-name*_jpcapp	666	Application definition file
	*monitoring-target-name*_suspended.dat	644	Monitoring suspension information file
installation-directory/agt7/agent/*instance-name*/targets/*monitoring-target-name*/	--	755	Work directory
	records.dat	666	Performance information file
	records.stdout		
	records.stderr		Collection error information file
	records.stderr.old		Previous collection error information file
	records.stderr.old_*NNNN*#3		Older collection error information files
	common.stdout		Result of a common command (stdout)
	common.stdout.old		Result of the previous common command (stdout)
	common.stdout.old_*NNNN*#3		Result of older common commands (stdout)
	common.stderr		Result of a common command (stderr)
	common.stderr.old		Result of the previous common command (stderr)
	common.stderr.old_*NNNN*#3		Result of older common commands (stderr)
	os.stdout		Results of an OS-specific command (stdout)
	os.stdout.old		Result of the previous OS-specific command (stdout)
	os.stdout.old_*NNNN*#3		Result of older OS-specific commands (stdout)
	os.stderr		Result of an OS-specific command (stderr)
	os.stderr.old		Result of the previous OS-specific command (stderr)
	os.stderr.old_*NNNN*#3		Result of older OS-specific commands (stderr)
installation-directory/agt7/bin/	--	755	Command storage directory
	jpc7-ssh-keygen	500	SSH key creation command

Directory name	File name	Permission	Description
installation-directory/agt7/bin/	jpc7collect	555	Collection process
	libjpcagt7hcc.so	755	HCCLib common library
installation-directory/agt7/dat/	--	755	Data storage directory for collection process
	common.dat	400	Storage folder for common execution commands
	cmd2rec	500	File creation script for record information
	cmd2rec_common		File creation script for record information (common to all OSs)
	cmd2rec_*OS*		File creation script for record information (for each OS)
	OS.dat	400	Execution command storage folder by category (for each OS)
installation-directory/agt7/nls/LANG/	--	755	Message catalog storage directory (for details about the LANG directory, see Table *F-4 List of LANG directories*)
	jpcagt7msg.cat	444	Message catalog file
installation-directory/agt7/store/	--	755	Base directory of the Remote Monitor Store service
	STDICT.DAT	444	Data model definition file
	STRULES.DAT		
	stolist.ini	644	Intermediate file for internal processing
	jpcsto.ini.instmpl	444	
installation-directory/agt7/store/*instance-name*/	--	755	Base directory of the Remote Monitor Store service. Files under this directory are created for each instance.
	*.DB	644	Performance data files
	*.IDX		Index files for performance data files
	*.LCK	666	Lock files for performance data files
	jpcsto.ini	644	Service startup initialization file of Remote Monitor Store
	jpcsto.ini.model	444	Sample of a service startup initialization file of Remote Monitor Store
	status.dat	600	Intermediate file for internal processing
	STDICT.DAT	444	Data model definition file
	STRULES.DAT		
installation-directory/agt7/store/*instance-name*/backup/	--	755	Default database backup directory

Directory name	File name	Permission	Description
installation-directory/agt7/store/*instance-name*/dump/	--	777	Default database export directory
installation-directory/agt7/store/*instance-name*/import/	--	755	Default database import directory
installation-directory/agt7/store/*instance-name*/log/	--	777	Internal log file storage directory for the Remote Monitor Collector service
	• msglog01 • msglog02	666	Internal log file
	• nslog01 • nslog02		
installation-directory/agt7/store/*instance-name*/partial/	--	755	Default database partial backup directory
installation-directory/agt7/store/*instance-name*/STPD/	--		PD record storage directory
installation-directory/agt7/store/*instance-name*/STPI/	--		
installation-directory/agt7/store/*instance-name*/STPL/	--		
installation-directory/log/	--	777	Common log directory
	jpclog*	666	Common logs
installation-directory/setup/	--	755	Setup file storage directory
	extract		Extraction directory for setup information
	jpcagt7u.Z	444	Archive file for PFM - RM for Platform setup (UNIX)
	jpcagt7w.EXE		Archive file for PFM - RM for Platform setup (Windows)
installation-directory/patch_files/agt7/	--	755	Storage directory for patch files (for agent)

Legend:

--: Not applicable

#1

Created if the health check function is enabled.

#2

nn is from 01 to 04.

#3

NNNN is from 0002 to 0012.

The following table lists the LANG directories for the UNIX edition of PFM - RM for Platform.

Table F–4: List of LANG directories

Value of LANG	Description
C	English catalog

Value of LANG	Description
`ja_JP.SJIS`	Catalog for SJIS
`ja_JP.UTF-8`	Catalog for UTF-8
`ja_JP.eucJP`	Catalog for EUC
`ja_JP.ujis`	Symbolic link to `ja_JP.eucJP`
`ja_JP.utf8`	Symbolic link to `ja_JP.UTF-8`

G. Migration Procedure and Notes on Migration

To upgrade PFM - RM for Platform, perform an overwrite installation of PFM - RM for Platform.

In Windows

See *3.1 Installation and setup of the Windows edition*.

In UNIX

See *3.2 Installation and setup of the UNIX edition*.

Notes

- When you upgrade PFM - RM for Platform, do not uninstall the earlier version of PFM - RM for Platform. If you uninstall it, all the data created by the earlier version (such as performance data) will also be deleted and will no longer be available under the later version.
- When you perform an overwrite installation of the PFM - RM for Platform program, the following items are updated automatically:
  - Store database files for the Remote Monitor Store service
  - INI file
  - Instance environments for PFM - RM for Platform

H. Version Compatibility

There are different versions of the PFM - RM for Platform product as well as different versions of the data model.

Because the data model has upward compatibility, you can use report and alarm definitions created under an earlier version of the data model with a later version.

The following table shows the correspondence between versions for PFM - RM for Platform.

Table H–1: Correspondence between versions for PFM - RM for Platform

PFM - RM for Platform version	Data model version	Alarm table version for monitoring template
09-00	4.0	09.00
09-10	5.0	09.10
09-50	5.0	09.10
10-00	5.0	09.10
10-50	5.0	09.10

For details about version compatibility, see the description of version compatibility in the appendix in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

I. Outputting Action Log Data

Performance Management action logs consist of historical information whose output is linked with the alarm function for exceeded threshold values, such as system overloads.

For example, action logs are output when the PFM services start and stop, and when the status of the connection with PFM - Manager changes.

You can output action logs if the version of PFM - Manager or PFM - Base is 08-11 or later.

Action logs constitute a text file in CSV format. You can use them as analysis data by saving them periodically and processing them with a spreadsheet software program.

Output of action logs is set by `jpccomm.ini`. This appendix describes the information that is output as action logs by PFM - RM for Platform and PFM - Base and how to set output of action logs.

I.1 Types of events that are output to action logs

The table below lists and describes the types of events that are output to action logs and when the action logs are output by PFM - RM for Platform and PFM - Base. The entries in the *Type of event* column are identifiers that are used to classify the events that are output to action logs.

Table I–1: Types of events that are output to action logs

Type of event	Description	When output by PFM - RM for Platform or PFM - Base
`StartStop`	Event indicating startup or termination of software	• At startup and termination of PFM services • At startup and termination of the stand-alone mode
`ExternalService`	• Event indicating the result of communication between JP1 products and external services • Event indicating the occurrence of an abnormal communication	At a change in the status of the connection with PFM - Manager
`ManagementAction`	• Event indicating execution of an important program action • Event indicating execution of an action based on another audit category	At execution of an automatic action

I.2 Storage format of action logs

This subsection describes the storage format of the action log file.

Action log information is output to the default file (current output file). When that file becomes full, new action log information is saved in a different file (shift file).

To swap action log files:

1. Action logs are output sequentially to the current output file `jpcaudit.log`.
2. When the current output file becomes full, new operation logs are output to a shift file.

The shift file name is the current output file name to which a number is appended. Each time the current output file becomes full, the shift file is renamed to *file-name-number+1*. Therefore, an older file has a larger number at the end of the file name.

Example:

When the current output file `jpcaudit.log` becomes full, its contents are saved to the shift file `jpcaudit1.log`.

When the current output file becomes full again, the existing shift file `jpcaudit1.log` is renamed to `jpcaudit2.log` and the contents of the current output file are moved to `jpcaudit1.log`.

When the number of log files reaches its maximum value (specified in the `jpccomm.ini` file), the oldest log file is deleted.

3. The current output file is initialized and new action logs are written.

The `jpccomm.ini` file is used to specify information about whether action logs are to be output, the output destination, and the maximum number of storage files. For details about how to set the `jpccomm.ini` file, see *I.4 Action log output settings*.

I.3 Output format of action logs

Information about audit events is output to the Performance Management action logs. A separate action log file is output for each host. An action log's output destination host is as follows:

- When a service is executed
  Action logs are output to the host where the service is running.
- When a command is executed
  Action logs are output to the host that executed the command.

The following describes the output format, output destination, and output items for action logs.

(1) Output format

`CALFHM` *x*`.`*x*`,` *output-item-1=value-1*`,` *output-item-2=value-2*`, . . .,` *output-item-n=value-n*

(2) Output destination

installation-folder`\auditlog\`

You can use the `jpccomm.ini` file to change the output destination of action logs. For details about how to set the `jpccomm.ini` file, see *I.4 Action log output settings*.

(3) Output items

There are two types of output items:

Common output items

Output items common to all JP1 products that output action logs

Fixed output items

Optional items that are output by JP1 products that output action logs

(a) Common output items

The table below lists and describes the common output items and their values, including the items that are output by PFM - Manager.

Table I–2: Common output items for action logs

Output item		Value	Description
Item name	Output attribute		
Common specification identifier	--	`CALFHM`	Identifier indicating that this is the action log format
Common specification revision number	--	*x.x*	Revision number used for managing action logs
Sequence number	`seqnum`	*sequence-number*	Sequence number of action log records
Message ID	`msgid`	`KAVE`*xxxxx*−*x*	Message ID
Date and time	`date`	*YYYY*−*MM*−*DDThh*:*mm*:*ss*.*sssTZD*#	Output date, time, and time zone of an action log
Generated program name	`progid`	`JP1PFM`	Name of the program where the event occurred
Generated component name	`compid`	*service-ID*	Name of the component where the event occurred
Generated process ID	`pid`	*process-ID*	Process ID of the process where the event occurred
Generated location	`ocp:host`	• *host-name* • *IP-address*	Location where the event occurred
Event type	`ctgry`	• `StartStop` • `Authentication` • `ConfigurationAccess` • `ExternalService` • `AnomalyEvent` • `ManagementAction`	Category names used to classify the events that are output to action logs
Event result	`result`	• `Success` • `Failure` • `Occurrence`	Result of the event
Subject identification information	`subj:pid`	*process-ID*	One of the following: • Process ID that is run by the user operation • Process ID that caused the event • User name that caused the event • Identification information assigned to users on a 1:1 basis
	`subj:uid`	*account-identifier* (PFM user/JP1 user)	
	`subj:euid`	*effective-user-ID* (OS user)	

Legend:

--: None

#

T indicates a separator between date and time.

TZD is the time zone specifier. One of the following is output:

+*hh*:*mm*: Advanced from UTC by *hh*:*mm*

−*hh*:*mm*: Delayed from UTC by *hh*:*mm*

Z: Same as UTC.

(b) Fixed output items

The table below lists and describes the fixed output items and their values, including the items that are output by PFM - Manager.

Table I–3: Fixed output items for action logs

Output item		Value	Description
Item name	Output attribute		
Object information	`obj`	• *service-ID-of-PFM-RM* • *added-deleted-or-updated-user-name* (PFM user)	Operation target
	`obj:table`	*alarm-table-name*	
	`obj:table`	*alarm-name*	
Action information	`op`	• `Start` • `Stop` • `Add` • `Update` • `Delete` • `Change Password` • `Activate` (enable) • `Inactivate` (disable) • `Bind` • `Unbind`	Action that caused the event

Permissions information	`auth`	• Administrator user
		`Management`
		• General user
		`Ordinary`
		• Windows
		`Administrator`
		• UNIX
		`SuperUser`
			Permissions of the user who performed the operation

	`auth:mode`	• PFM authentication mode
		`pfm`
		• JP1 authentication mode
		`jp1`
		• OS user
		`os`
			Authentication mode of the user who performed the operation

Output source	`outp:host`	*name-of-PFM-Manager-host*	Host that output the action log
Instruction source	`subjp:host`	• *name-of-logon-host* • *name-of-executing-host* (only during execution of the `jpcalarm` command)	Host that issued the operation instruction
Free description	`msg`	*message*	Message that is output in the event of an alarm and execution of automatic action

Whether each fixed output item exists depends on the output timing. The following subsections describe the message ID and fixed output items for each output timing.

■ Startup and termination of PFM services (StartStop)

- Output host
  Host on which the corresponding service is running
- Output component
  Each service that starts and stops

A message ID and operation information are output when the PFM service starts and stops (StartStop). The following table lists and describes the message IDs and operation information that are output.

Table I–4: Message IDs and operation information that are output when a PFM service starts and stops (StartStop)

Item name	Attribute name	Value
Message ID	`msgid`	• Start: `KAVE03000-I` is output. • Stop: `KAVE03001-I` is output.
Operation information	`op`	• Start: `Start` is output. • Stop: `Stop` is output.

■ Startup and termination of the stand-alone mode (StartStop)

- Output host
  PFM - RM host
- Output component
  Remote Monitor Collector and Remote Monitor Store services

A message ID is output when the stand-alone mode starts and ends (StartStop). The following table lists and describes the message IDs that are output.

Table I–5: Message IDs that are output when the stand-alone mode starts and ends (StartStop)

Item name	Attribute name	Value
Message ID	`msgid`	• Start of the stand-alone mode: `KAVE03002-I` is output. • End of the stand-alone mode: `KAVE03003-I` is output.

Note 1

Fixed output items are not output.

Note 2

When each service of PFM - RM for Platform starts, it connects to the PFM - Manager host to register node information and to acquire the most recent alarm definition information.

If the service cannot connect to the PFM - Manager host, it starts (in the stand-alone mode) with only some of the functions enabled (such as collection of operation information). `KAVE03002-I` is then issued in order to indicate that the service has started in the stand-alone mode.

Thereafter, the service continues to attempt to connect to the PFM - Manager host at specific intervals. When the service successfully registers node information and acquires definition information, it ends the stand-alone mode and `KAVE03003-I` is issued.

Output of `KAVE03002-I` and `KAVE03003-I` in the action logs indicates that PFM - RM for Platform was running in incomplete status.

■ Change to the status of the connection to PFM - Manager (ExternalService)

- Output host
  PFM - RM host
- Output component
  Remote Monitor Collector and Remote Monitor Store services

A message ID is output when the status of the connection to PFM - Manager changes (ExternalService). The following table lists and describes the message IDs that are output.

Table I–6: Message IDs that are output when the status of the connection to PFM - Manager changes (ExternalService)

Item name	Attribute name	Value
Message ID	`msgid`	• Transmission of an event to PFM - Manager failed (queuing started): `KAVE03300-I` is output. • Re-transmission of an event to PFM - Manager was completed: `KAVE03301-I` is output.

Note 1

Fixed output items are not output.

Note 2

If transmission of an event to PFM - Manager fails, the Remote Monitor Collector service starts queuing events. Thereafter, each event is queued until the number of queued events reaches 3.

`KAVE03300-I` is output when event transmission fails and queuing starts. `KAVE03301-I` is output when connection with PFM - Manager is restored and transmission of queued events is completed.

Output of `KAVE03300-I` and `KAVE03301-I` in action logs brackets the period during which events were not transmitted to PFM - Manager in real time.

Note 3

The Remote Monitor Collector service normally sends events to PFM - Manager via the Remote Monitor Store service. If the Remote Monitor Store service is stopped for some reason, the Remote Monitor Collector service sends events to PFM - Manager directly.

`KAVE03300-I` is output when transmission of events to PFM - Manager fails. At this point, `KAVE03301-I` is not output because queuing has not started.

This action log indicates the events that were not sent to PFM - Manager.

■ Execution of automatic action (ManagementAction)

- Output host
  Host that executed the action
- Output component
  Action Handler service

When an automatic action is executed (ManagementAction), a message ID and free description item are output. The following table lists and describes the message IDs and free description items that are output.

Table I–7: Message IDs and free description items that are output during execution of an automatic action (ManagementAction)

Item name	Attribute name	Value
Message ID	`msgid`	• Creation of a command execution process was successful: `KAVE03500-I` is output. • Creation of a command execution process failed: `KAVE03501-W` is output. • Email transmission was successful:

Item name	Attribute name	Value
Message ID	msgid	KAVE03502-I is output. • Email transmission failed: KAVE03503-W is output.
Free description	msg	• Command execution: cmd=*executed-command-line* is output. • Email transmission: mailto=*destination-email-address* is output.

Note

KAVE03500-I is output when a command execution process is created successfully. Thereafter, the result of checking for command execution and the execution results are not output to the action logs.

(4) Output example

The following shows an output example of action logs:

```
CALFHM 1.0, seqnum=1, msgid=KAVE03000-I, date=2007-01-18T22:46:49.682+09:00,
progid=JP1PFM, compid=7A1host01, pid=2076,
ocp:host=host01, ctgry=StartStop, result=Occurrence,
subj:pid=2076,op=Start
```

I.4 Action log output settings

Use the jpccomm.ini file to specify settings that enable output of action logs. If you do not specify these settings, action logs will not be output. This subsection describes how to specify the action log output settings and provides details about the jpccomm.ini file.

(1) How to specify the settings

To specify the action log output settings:

1. Stop all Performance Management services on the host.
2. Use a program such as a text editor to edit the jpccomm.ini file.
3. Save the jpccomm.ini file, and then close it.

(2) Details of the jpccomm.ini file

This subsection describes the jpccomm.ini file.

(a) Storage folder

The storage folder is *PFM-Manager-installation-folder*.

(b) Format

The following information is defined in the jpccomm.ini file:

- Whether action logs are to be output

- Action log output destination
- Number of action log files to be saved
- Size of the action log file

The specification format is as follows:

```
"item-name"=value
```

The following table lists and describes the settings to be specified in the `jpccomm.ini` file.

Table I–8: Settings specified in the jpccomm.ini file and their initial values

Item	Description
`[Action Log Section]`	Specifies the section name. This item cannot be changed.
`Action Log Mode`	Specifies whether action logs are to be output. This item is mandatory. • Initial value `0` (do not output) • Permitted values `0` (do not output), `1` (output) If any other value is specified, an error message is output, in which case action logs are not output.
`Action Log Dir`	Specifies the output destination for action logs, using an absolute path. In a logical host environment, specify a directory on the shared disk. If the directory you specify is not on the shared disk, Performance Management will output action logs to each physical host that forms the basis for the logical host. If you specify a path that exceeds the maximum allowable length, or the system is unable to access the directory, an error message is output to the common log and Performance Management will not output action logs. • Initial value: Omitted • Value used when this item is omitted (default): On physical hosts: - Windows: *installation-folder*`\auditlog` - UNIX: `/opt/jp1pc/auditlog/` On logical hosts: - Windows: *environment-directory*`\jp1pc\auditlog` - UNIX: *environment-directory*`/jp1pc/auditlog` • Available values: Character strings from 1 to 185 bytes in length
`Action Log Num`	Specifies the maximum number of log files. This is the total number of current output file and shift files. • Initial value Omitted • Value assumed when the item is omitted (default) 5 • Permitted values Integer in the range from 2 to 10 If a nonnumeric character is specified, an error message is output and the value 5 (the default) is set. If the specified value is outside the permitted range, an error message is output and the integer in the range from 2 to 10 that is the closest to the specified value is set.
`Action Log Size`	Specifies the log file size in kilobytes. • Initial value Omitted

Item	Description
`Action Log Size`	• Value assumed when the item is omitted (default) 2,048 • Permitted values Integer in the range from 512 to 2,096,128 If a nonnumeric character is specified, an error message is output and a value of 2,048 (the default) is set. If the specified value is outside the permitted range, an error message is output and the integer in the range from 512 to 2,096,128 that is the closest to the specified value is set.

J. Data Sources of Records

The individual fields of the records store values acquired from Performance Management and monitoring-target programs, as well as values computed using certain formulas and these acquired values. This appendix lists the sources of field values or formulas. The sources of field values and the formulas are collectively referred to as *data sources*.

J.1 Data sources of records (when the monitored host is running Windows)

This section describes the data sources for the field values when the monitored host is running Windows.

(1) Application Process Count (PD_APPC)

The following table lists the data sources for the individual fields of the Application Process Count (`PD_APPC`) record:

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (`INPUT_RECORD_TYPE`)	--	--
Record Time (`RECORD_TIME`)	--	--
Interval (`INTERVAL`)	--	--
VA DeviceID (`VADEVICEID`)	--	--
Target Host (`TARGET_HOST`)	--	--
Polling Time (`POLLING_TIME`)	--	--
Target Host Time (`TARGET_HOST_TIME`)	*C*	`C:Win32_OperatingSystem.LocalDateTime`
Application Name (`APPLICATION_NAME`)	--	--
Monitoring Number (`MONITORING_NUMBER`)	--	--
Monitoring Label (`MONITORING_LABEL`)	--	--
Monitoring Min (`MONITORING_MIN`)	--	--
Monitoring Max (`MONITORING_MAX`)	--	--
Monitoring Count (`MONITORING_COUNT`)	--	--
Monitoring Status (`MONITORING_STATUS`)	--	--
Ext1 (`EXT1`)	--	--
Ext2 (`EXT2`)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(2) Application Process Detail (PD_APPD)

The following table lists the data sources for the individual fields of the Application Process Detail (PD_APPD) record:

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
Application Name (APPLICATION_NAME)	--	--
Monitoring Number (MONITORING_NUMBER)	--	--
Monitoring Label (MONITORING_LABEL)	--	--
Monitoring Condition (MONITORING_CONDITION)	--	--
Monitoring Field (MONITORING_FIELD)	--	--
Monitoring Min (MONITORING_MIN)	--	--
Monitoring Max (MONITORING_MAX)	--	--
Monitoring Count (MONITORING_COUNT)	--	--
Monitoring Status (MONITORING_STATUS)	--	--
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(3) Application Process Overview (PD_APS)

The following table lists the data sources for the individual fields of the Application Process Overview (PD_APS) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
PID (PID)	*C*	C:Win32_PerfFormattedData_PerfProc_Process.IDProcess
Program Name (PROGRAM_NAME)	*C*	C:Win32_Process.Name
Parent PID (PARENT_PID)	*C*	C:Win32_PerfFormattedData_PerfProc_Process.CreatingProcessID
Command Line (COMMAND_LINE)	*C*	C:Win32_Process.CommandLine
Terminal (TERMINAL)	--	--
Elapsed Time (ELAPSED_TIME)	*C*	C:Win32_PerfFormattedData_PerfProc_Process.ElapsedTime
State (STATE)	--	--
Virtual Env ID (VIRTUAL_ENV_ID)	--	--
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(4) Application Service Overview (PD_ASVC)

The following table lists the data sources for the individual fields of the Application Service Overview (PD_ASVC) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
Service Name (SERVICE_NAME)	*C*	C:Win32_Service.Name
Service Exit Code (SERVICE_EXIT_CODE)	*C*	C:Win32_Service.ServiceSpecificExitCode
Win32 Exit Code (WIN32_EXIT_CODE)	*C*	C:Win32_Service.ExitCode
Display Name (DISPLAY_NAME)	*C*	C:Win32_Service.DisplayName
State (STATE)	*C*	C:Win32_Service.State
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(5) Application Summary (PD_APP2)

The following table lists the data sources for the individual fields of the Application Summary (PD_APP2) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
Application Name (APPLICATION_NAME)	--	--
Application Status (APPLICATION_STATUS)	--	--
Application Exist (APPLICATION_EXIST)	--	--
Virtual Env ID (VIRTUAL_ENV_ID)	--	--
Case Sensitive (CASE_SENSITIVE)	--	--

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(6) Logical Disk Overview (PI_LDSK)

The following table lists the data sources for the individual fields of the Logical Disk Overview (PI_LDSK) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
ID (ID)	*C*	C:Win32_PerfRawData_PerfDisk_LogicalDisk.Name
Device Name (DEVICE_NAME)	--	--
Free Mbytes (FREE_MBYTES)	*C*	C:Win32_PerfRawData_PerfDisk_LogicalDisk.FreeMegabytes
Free Mbytes % (FREE_MBYTES_PERCENT)	*C*	C:Win32_PerfFormattedData_PerfDisk_LogicalDisk.PercentFreeSpace
Size (SIZE)	*C* ÷ 1,024 ÷ 1,024	C:Win32_Volume.Capacity
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(7) Network Interface Overview (PI_NET)

The following table lists the data sources for the individual fields of the Network Interface Overview (PI_NET) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	C	C:Win32_OperatingSystem.LocalDateTime
ID (ID)	C	C:Win32_PerfRawData_Tcpip_NetworkInterface.Name
Max Transmission Unit (MAX_TRANSMISSION_UNIT)	--	--
Rcvd Packets/sec (RCVD_PACKETS_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	C:Win32_PerfRawData_Tcpip_NetworkInterface.PacketsReceivedPersec T:Win32_PerfRawData_Tcpip_NetworkInterface.Timestamp_PerfTime TB:Win32_PerfRawData_Tcpip_NetworkInterface.Frequency_PerfTime
Sent Packets/sec (SENT_PACKETS_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	C:Win32_PerfRawData_Tcpip_NetworkInterface.PacketsSentPersec T:Win32_PerfRawData_Tcpip_NetworkInterface.Timestamp_PerfTime TB:Win32_PerfRawData_Tcpip_NetworkInterface.Frequency_PerfTime
Total Packets/sec (TOTAL_PACKETS_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	C:Win32_PerfRawData_Tcpip_NetworkInterface.PacketsPersec T:Win32_PerfRawData_Tcpip_NetworkInterface.Timestamp_PerfTime TB:Win32_PerfRawData_Tcpip_NetworkInterface.Frequency_PerfTime
Rcvd Bytes/sec (RCVD_BYTES_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	C:Win32_PerfRawData_Tcpip_NetworkInterface.BytesReceivedPersec T:Win32_PerfRawData_Tcpip_NetworkInterface.Timestamp_PerfTime TB:Win32_PerfRawData_Tcpip_NetworkInterface.Frequency_PerfTime
Sent Bytes/sec (SENT_BYTES_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	C:Win32_PerfRawData_Tcpip_NetworkInterface.BytesSentPersec T:Win32_PerfRawData_Tcpip_NetworkInterface.Timestamp_PerfTime TB:Win32_PerfRawData_Tcpip_NetworkInterface.Frequency_PerfTime
Total Bytes/sec (TOTAL_BYTES_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	C:Win32_PerfRawData_Tcpip_NetworkInterface.BytesTotalPersec T:Win32_PerfRawData_Tcpip_NetworkInterface.Timestamp_PerfTime

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Total Bytes/sec (TOTAL_BYTES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	TB:Win32_PerfRawData_Tcpip_NetworkInterface.Frequency_PerfTime
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

T: Indicates a time value.

TB: Indicates the time base value.

△ : Indicates a value obtained by subtracting *previously collected value* from *current collected value*.

--: Indicates that no field value obtained by processing performance data is set.

(8) Physical Disk Overview (PI_PDSK)

The following table lists the data sources for the individual fields of the Physical Disk Overview (PI_PDSK) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
ID (ID)	*C*	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.Name
Avg Disk Time (AVG_DISK_TIME)	(△ *C* ÷ *TB*) ÷ △ *B*	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.AvgDisksecPerTransfer B:Win32_PerfRawData_PerfDisk_PhysicalDisk.AvgDisksecPerTransfer_base TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime
Busy % (BUSY_PERCENT)	100 × △ *C* ÷ △ *T*	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.PercentDiskTime T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_Sys100NS
Read MBytes/sec (READ_MBYTES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*) ÷ 1,024 ÷ 1,024	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.DiskReadBytesPersec T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_PerfTime TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Write MBytes/sec (WRITE_MBYTES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*) ÷ 1,024 ÷ 1,024	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.DiskWriteBytesPersec T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_PerfTime TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime
Total MBytes/sec (TOTAL_MBYTES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*) ÷ 1,024 ÷ 1,024	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.DiskBytesPersec T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_PerfTime TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime
Read Counts/sec (READ_COUNTS_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.DiskReadsPersec T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_PerfTime TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime
Write Counts/sec (WRITE_COUNTS_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.DiskWritesPersec T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_PerfTime TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime
Total Counts/sec (TOTAL_COUNTS_PER_SEC)	△ C ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.DiskTransfersPersec T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_PerfTime TB:Win32_PerfRawData_PerfDisk_PhysicalDisk.Frequency_PerfTime
Queue Length (QUEUE_LENGTH)	△ *C* ÷ △ *T*	C:Win32_PerfRawData_PerfDisk_PhysicalDisk.AvgDiskQueueLength T:Win32_PerfRawData_PerfDisk_PhysicalDisk.Timestamp_Sys100NS
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

B: Indicates the base value of a counter.

C: Indicates the value of a counter.

T: Indicates a time value.

TB: Indicates the time base value.

△ : Indicates a value obtained by subtracting *previously collected value* from *current collected value*.

--: Indicates that no field value obtained by processing performance data is set.

(9) Processor Overview (PI_CPU)

The following table lists the data sources for the individual fields of the Processor Overview (PI_CPU) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
ID (ID)	*C*	C:Win32_PerfRawData_PerfOS_Processor.Name
CPU % (CPU_PERCENT)	100 × (1 - △ *C* ÷ △ *T*)	C:Win32_PerfRawData_PerfOS_Processor.PercentProcessorTime T:Win32_PerfRawData_PerfOS_Processor.Timestamp_Sys100NS
Idle % (IDLE_PERCENT)	100 × △ *C* ÷ △ *T*	C:Win32_PerfRawData_PerfOS_Processor.PercentIdleTime T:Win32_PerfRawData_PerfOS_Processor.Timestamp_Sys100NS
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Processor.InterruptsPersec T:Win32_PerfRawData_PerfOS_Processor.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Processor.Frequency_PerfTime
System % (SYSTEM_PERCENT)	100 × △ *C* ÷ △ *T*	C:Win32_PerfRawData_PerfOS_Processor.PercentPrivilegedTime T:Win32_PerfRawData_PerfOS_Processor.Timestamp_Sys100NS
User % (USER_PERCENT)	100 × △ *C* ÷ △ *T*	C:Win32_PerfRawData_PerfOS_Processor.PercentUserTime T:Win32_PerfRawData_PerfOS_Processor.Timestamp_Sys100NS
Wait % (WAIT_PERCENT)	--	--
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

T: Indicates a time value.

TB: Indicates the time base value.

△ : Indicates a value obtained by subtracting *previously collected value* from *current collected value*.

--: Indicates that no field value obtained by processing performance data is set.

(10) System Status (PD)

The following table lists the data sources for the individual fields of the System Status (PD) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
Status (STATUS)	--	--
Reason (REASON)	--	--
OS Type (OS_TYPE)	Windows (fixed)	--
Version (VERSION)	*C*	C:Win32_OperatingSystem.Version
Processor Type (PROCESSOR_TYPE)	*C*	C:Win32_ComputerSystem.SystemType
Detail (DETAIL)	*C*	C:Win32_OperatingSystem.Caption[, Win32_OperatingSystem.OtherTypeDescription][, Win32_OperatingSystem.CSDVersion]
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

--: Indicates that no field value obtained by processing performance data is set.

(11) System Summary (PI)

The following table lists the data sources for the individual fields of the System Summary (PI) record.

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Record Type (INPUT_RECORD_TYPE)	--	--
Record Time (RECORD_TIME)	--	--
Interval (INTERVAL)	--	--
VA DeviceID (VADEVICEID)	--	--
Target Host (TARGET_HOST)	--	--
Polling Time (POLLING_TIME)	--	--

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Target Host Time (TARGET_HOST_TIME)	*C*	C:Win32_OperatingSystem.LocalDateTime
Active CPUs (ACTIVE_CPUS)	Number of instances in Win32_PerfRawData_PerfOS_Processor excluding _Total	--
CPU % (CPU_PERCENT)	CPU_PERCENT of the _Total instance of the PI_CPU record	--
Idle % (IDLE_PERCENT)	IDLE_PERCENT of the _Total instance of the PI_CPU record	--
System % (SYSTEM_PERCENT)	SYSTEM_PERCENT of the _Total instance of the PI_CPU record	--
User % (USER_PERCENT)	USER_PERCENT of the _Total instance of the PI_CPU record	--
Wait % (WAIT_PERCENT)	--	--
Processor Queue Length (PROCESSOR_QUEUE_LENGTH)	*C*	C:Win32_PerfRawData_PerfOS_System.ProcessorQueueLength
Run Queue Avg 5 min (RUN_QUEUE_AVG_5_MIN)	--	--
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	INTERRUPT_COUNTS_PER_SEC of the _Total instance of the PI_CPU record	--
Effective Free Mem % (EFFECTIVE_FREE_MEM_PERCENT)	--	--
Effective Free Mem Mbytes (EFFECTIVE_FREE_MEM_MBYTES)	--	--
Free Mem % (FREE_MEM_PERCENT)	100 × FREE_MEM_MBYTES ÷ TOTAL_MEM_MBYTES	--
Free Mem Mbytes (FREE_MEM_MBYTES)	*C* ÷ 1,024 ÷ 1,024	C:Win32_PerfRawData_PerfOS_Memory.AvailableBytes
Used Mem % (USED_MEM_PERCENT)	100 × USED_MEM_MBYTES ÷ TOTAL_MEM_MBYTES	--
Used Mem Mbytes (USED_MEM_MBYTES)	TOTAL_MEM_MBYTES - FREE_MEM_MBYTES	--
Total Mem Mbytes (TOTAL_MEM_MBYTES)	*C* ÷ 1,024	C:Win32_OperatingSystem.TotalVisibleMemorySize

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Free Swap % (FREE_SWAP_PERCENT)	100 × FREE_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	--
Free Swap Mbytes (FREE_SWAP_MBYTES)	TOTAL_SWAP_MBYTES - USERD_SWAP_MBYTES	--
Used Swap % (USED_SWAP_PERCENT)	*C*	C:Win32_PerfFormattedData_PerfOS_Memory.PercentCommittedBytesInUse
Used Swap Mbytes (USED_SWAP_MBYTES)	*C* ÷ 1,024 ÷ 1,024	C:Win32_PerfRawData_PerfOS_Memory.CommittedBytes
Total Swap Mbytes (TOTAL_SWAP_MBYTES)	*C* ÷ 1,024 ÷ 1,024	C:Win32_PerfRawData_PerfOS_Memory.CommitLimit
Page Fault Counts/sec (PAGE_FAULT_COUNTS_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Memory.PageFaultsPersec T:Win32_PerfRawData_PerfOS_Memory.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Memory.Frequency_PerfTime
Page Scan Counts/sec (PAGE_SCAN_COUNTS_PER_SEC)	--	--
Page-In Counts/sec (PAGE_IN_COUNTS_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Memory.PageReadsPersec T:Win32_PerfRawData_PerfOS_Memory.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Memory.Frequency_PerfTime
Page-Out Counts/sec (PAGE_OUT_COUNTS_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Memory.PageWritesPersec T:Win32_PerfRawData_PerfOS_Memory.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Memory.Frequency_PerfTime
Page-In Pages/sec (PAGE_IN_PAGES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Memory.PagesInputPersec T:Win32_PerfRawData_PerfOS_Memory.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Memory.Frequency_PerfTime
Page-Out Pages/sec (PAGE_OUT_PAGES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Memory.PagesOutputPersec T:Win32_PerfRawData_PerfOS_Memory.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Memory.Frequency_PerfTime
Paging Pages/sec (PAGING_PAGES_PER_SEC)	△ *C* ÷ (△ *T* ÷ *TB*)	C:Win32_PerfRawData_PerfOS_Memory.PagesPersec

PFM - View name (PFM - Manager name)	Data source	
	Formula	WMI class
Paging Pages/sec (PAGING_PAGES_PER_SEC)	$\triangle C \div (\triangle T \div TB)$	T:Win32_PerfRawData_PerfOS_Memory.Timestamp_PerfTime TB:Win32_PerfRawData_PerfOS_Memory.Frequency_PerfTime
Pool Nonpaged KBytes (POOL_NONPAGED_KBYTES)	$C \div 1{,}024$	C:Win32_PerfRawData_PerfOS_Memory.PoolNonpagedBytes
Swap-In Counts/sec (SWAP_IN_COUNTS_PER_SEC)	--	--
Swap-Out Counts/sec (SWAP_OUT_COUNTS_PER_SEC)	--	--
Swap-In Pages/sec (SWAP_IN_PAGES_PER_SEC)	--	--
Swap-Out Pages/sec (SWAP_OUT_PAGES_PER_SEC)	--	--
Ext1 (EXT1)	--	--
Ext2 (EXT2)	--	--

Legend:

C: Indicates the value of a counter.

T: Indicates a time value.

TB: Indicates the time base value.

△ : Indicates a value obtained by subtracting *previously collected value* from *current collected value*.

--: Indicates that no field value obtained by processing performance data is set.

J.2 Data sources of records (when the monitored host is running UNIX)

This section explains the data sources for the field values when the monitored host is running UNIX.

(1) Application Process Count (PD_APPC)

The following table lists the data sources for the individual fields of the Application Process Count (PD_APPC) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
Application Name (APPLICATION_NAME)	--	--	--	--
Monitoring Number (MONITORING_NUMBER)	--	--	--	--
Monitoring Label (MONITORING_LABEL)	--	--	--	--
Monitoring Min (MONITORING_MIN)	--	--	--	--
Monitoring Max (MONITORING_MAX)	--	--	--	--
Monitoring Count (MONITORING_COUNT)	--	--	--	--
Monitoring Status (MONITORING_STATUS)	--	--	--	--
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(2) Application Process Detail (PD_APPD)

The following table lists the data sources for the individual fields of the Application Process Detail (PD_APPD) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
Application Name (APPLICATION_NAME)	--	--	--	--
Monitoring Number (MONITORING_NUMBER)	--	--	--	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Monitoring Label (MONITORING_LABEL)	--	--	--	--
Monitoring Condition (MONITORING_CONDITION)	--	--	--	--
Monitoring Field (MONITORING_FIELD)	--	--	--	--
Monitoring Min (MONITORING_MIN)	--	--	--	--
Monitoring Max (MONITORING_MAX)	--	--	--	--
Monitoring Count (MONITORING_COUNT)	--	--	--	--
Monitoring Status (MONITORING_STATUS)	--	--	--	--
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(3) Application Process Overview (PD_APS)

The following table lists the data sources for the individual fields of the Application Process Overview (PD_APS) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
PID (PID)	UNIX95=1 /usr/bin/ps -A -o pid	/usr/bin/ps -e -o pid	/usr/bin/ps -A -X -o pid	/bin/ps -e -o pid
Program Name (PROGRAM_NAME)	UNIX95=1 /usr/bin/ps -A -o comm	/usr/bin/ps -e -o fname	/usr/bin/ps -A -X -o comm	/bin/ps -e -o comm

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Parent PID (PARENT_PID)	UNIX95=1 /usr/bin/ps -A -o ppid	/usr/bin/ps -e -o ppid	/usr/bin/ps -A -X -o ppid	/bin/ps -e -o ppid
Command Line (COMMAND_LINE)	UNIX95=1 /usr/bin/ps -A -o args	/usr/bin/ps -e -o args	/usr/bin/ps -A -X -o args	/bin/ps -e -o args
Terminal (TERMINAL)	UNIX95=1 /usr/bin/ps -A -o tty	/usr/bin/ps -e -o tty	/usr/bin/ps -A -X -o tty	/bin/ps -e -o tty
Elapsed Time (ELAPSED_TIME)	UNIX95=1 /usr/bin/ps -A -o etime	/usr/bin/ps -e -o etime	/usr/bin/ps -A -X -o etime	/bin/ps -e -o etime
State (STATE)	UNIX95=1 /usr/bin/ps -A -o state	/usr/bin/ps -e -o s	/usr/bin/ps -A -X -o st	/bin/ps -e -o state
Virtual Env ID (VIRTUAL_ENV_ID)	--	/usr/bin/ps -e -o zone	/usr/bin/ps -A -X -o wpar	--
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(4) Application Summary (PD_APP2)

The following table lists the data sources for the individual fields of the Application Summary (PD_APP2) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
Application Name (APPLICATION_NAME)	--	--	--	--
Application Status (APPLICATION_STATUS)	--	--	--	--
Application Exist (APPLICATION_EXIST)	--	--	--	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Virtual Env ID (VIRTUAL_ENV_ID)	--	--	--	--
Case Sensitive (CASE_SENSITIVE)	--	--	--	--
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(5) Logical Disk Overview (PI_LDSK)

The following table lists the data sources for the individual fields of the Logical Disk Overview (PI_LDSK) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
ID (ID)	Mount point in /usr/bin/df -lk mount point	Mounted on in /usr/sbin/df -lk	Mounted on in /usr/bin/df -k	Mounted on in /bin/df -lkP
Device Name (DEVICE_NAME)	Device name in /usr/bin/df -lk	Filesystem in /usr/sbin/df -lk	Filesystem in /usr/bin/df -k	Filesystem in /bin/df -lkP
Free Mbytes (FREE_MBYTES)	free allocated Kb ÷ 1,024 in /usr/bin/df -lk	avail ÷ 1,024 in /usr/sbin/df -lk	Free ÷ 1,024 in /usr/bin/df -k	Available ÷ 1,024 in /bin/df -lkP
Free Mbytes % (FREE_MBYTES_PERCENT)	FREE_MBYTES ÷ SIZE × 100	FREE_MBYTES ÷ SIZE × 100	FREE_MBYTES ÷ SIZE × 100	FREE_MBYTES ÷ SIZE × 100
Size (SIZE)	total allocated Kb ÷ 1,024 in /usr/bin/df -lk	kbytes ÷ 1,024 in /usr/sbin/df -lk	1,024-blocks ÷ 1,024 in /usr/bin/df -k	1,024-blocks ÷ 1,024 in /bin/df -lkP
Ext1 (EXT1)	--	--	--	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(6) Network Interface Overview (PI_NET)

The following table lists the data sources for the individual fields of the Network Interface Overview (PI_NET) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
ID (ID)	Name in /usr/bin/netstat -i -n	Name in /usr/bin/netstat -i -n	Name in /usr/bin/netstat -i -n	Iface in /bin/netstat -i -n
Max Transmission Unit (MAX_TRANSMISSION_UNIT)	Mtu in /usr/bin/netstat -i -n	Mtu in /usr/bin/netstat -i -n	Mtu in /usr/bin/netstat -i -n	MTU in /bin/netstat -i -n
Rcvd Packets/sec (RCVD_PACKETS_PER_SEC)	Ipkts ÷ △ *collection time* in △ /usr/bin/netstat -i -n	Ipkts ÷ △ *collection time* in △ /usr/bin/netstat -i -n	Ipkts ÷ △ *collection time* in △ /usr/bin/netstat -i -n	RX-OK ÷ △ *collection time* in △ /bin/netstat -i -n
Sent Packets/sec (SENT_PACKETS_PER_SEC)	Opkts ÷ △ *collection time* in △ /usr/bin/netstat -i -n	Opkts ÷ △ *collection time* in △ /usr/bin/netstat -i -n	Opkts ÷ △ *collection time* in △ /usr/bin/netstat -i -n	TX-OK ÷ △ *collection time* in △ /bin/netstat -i -n
Total Packets/sec (TOTAL_PACKETS_PER_SEC)	RCVD_PACKETS_PER_SEC + SENT_PACKETS_PER_SEC	RCVD_PACKETS_PER_SEC + SENT_PACKETS_PER_SEC	RCVD_PACKETS_PER_SEC + SENT_PACKETS_PER_SEC	RCVD_PACKETS_PER_SEC + SENT_PACKETS_PER_SEC
Rcvd Bytes/sec (RCVD_BYTES_PER_SEC)	--	--	--	--
Sent Bytes/sec (SENT_BYTES_PER_SEC)	--	--	--	--
Total Bytes/sec (TOTAL_BYTES_PER_SEC)	--	--	--	--
Ext1 (EXT1)	--	--	--	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Ext2 (EXT2)	--	--	--	--

Legend:

△ : Indicates a value obtained by subtracting *previously collected value* from *current collected value*.

--: Indicates that no field value obtained by processing performance data is set.

(7) Physical Disk Overview (PI_PDSK)

The following table lists the data sources for the individual fields of the Physical Disk Overview (PI_PDSK) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
ID (ID)	device in /usr/bin/iostat	device in usr/bin/iostat -x 5 2	device in /usr/sbin/sar -d 5 1	Device in /usr/bin/iostat -x -k -d 5 2
Avg Disk Time (AVG_DISK_TIME)	avserv ÷ 1,000 in /usr/sbin/sar -d 5 1	svc_t ÷ 1,000 in /usr/bin/iostat -x 5 2	avserv ÷ 1,000 in /usr/sbin/sar -d 5 1	svctm ÷ 1,000 in /usr/bin/iostat -x -k -d 5 2
Busy % (BUSY_PERCENT)	%busy in /usr/sbin/sar -d 5 1	%b in /usr/bin/iostat -x 5 2	%busy in /usr/sbin/sar -d 5 1	%util in /usr/bin/iostat -x -k -d 5 2
Read MBytes/sec (READ_MBYTES_PER_SEC)	--	kr/s ÷ 1,024 in /usr/bin/iostat -x 5 2	--	rkB/s ÷ 1,024 in /usr/bin/iostat -x -k -d 5 2
Write MBytes/sec (WRITE_MBYTES_PER_SEC)	--	kw/s ÷ 1,024 in /usr/bin/iostat -x 5 2	--	wkB/s ÷ 1,024 in /usr/bin/iostat -x -k -d 5 2
Total MBytes/sec (TOTAL_MBYTES_PER_SEC)	blks/s × 2 ÷ 1,024 in /usr/sbin/sar -d 5 1	READ_MBYTES_PER_SEC + WRITE_MBYTES_PER_SEC	Kbs/s in /usr/sbin/sar -d 5 1	READ_MBYTES_PER_SEC + WRITE_MBYTES_PER_SEC

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Read Counts/sec (READ_COUNTS_PER_SEC)	--	r/s in /usr/bin/iostat -x 5 2	--	r/s in /usr/bin/iostat -x -k -d 5 2
Write Counts/sec (WRITE_COUNTS_PER_SEC)	--	w/s in /usr/bin/iostat -x 5 2	--	w/s in /usr/bin/iostat -x -k -d 5 2s
Total Counts/sec (TOTAL_COUNTS_PER_SEC)	r+w ÷ s in /usr/sbin/sar -d 5 1	READ_COUNTS_PER_SEC + WRITE_COUNTS_PER_SEC	r+w ÷ s in /usr/sbin/sar -d 5 1	READ_COUNTS_PER_SEC + WRITE_COUNTS_PER_SEC
Queue Length (QUEUE_LENGTH)	avque in /usr/sbin/sar -d 5 1	actv in /usr/bin/iostat -x 5 2	avque in /usr/sbin/sar -d 5 1	avgqu-sz in /usr/bin/iostat -x -k -d 5 2
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(8) Processor Overview (PI_CPU)

The following table lists the data sources for the individual fields of the Processor Overview (PI_CPU) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	/usr/bin/date -u +%Y-%m-%dT%H:%M:%SZ	/usr/bin/date -u +%Y-%m-%dT%H:%M:%SZ	/usr/bin/date -u +%Y-%m-%dT%H:%M:%SZ	/bin/date -u +%Y-%m-%dT%H:%M:%SZ
ID (ID)	cpu in /usr/sbin/sar -M -u 5 1	CPU in /usr/bin/mpstat -p 5 2	cpu in /usr/sbin/sar -u -P ALL 5 1	CPU in /usr/bin/mpstat -P ALL 5 1 or /usr/bin/mpstat -A 5 1
CPU % (CPU_PERCENT)	SYSTEM_PERCENT + USER_PERCENT	SYSTEM_PERCENT + USER_PERCENT	SYSTEM_PERCENT + USER_PERCENT	SYSTEM_PERCENT + USER_PERCENT
Idle % (IDLE_PERCENT)	%idle in /usr/sbin/sar -u -M 5 1	idl in /usr/bin/mpstat -p 5 2	Idle% in /usr/sbin/sar -u -P ALL 5 1	%idle in /usr/bin/mpstat -P ALL 5 1

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Idle % (IDLE_PERCENT)	%idle in /usr/sbin/sar -u -M 5 1	idl in /usr/bin/mpstat -p 5 2	Idle% in /usr/sbin/sar -u -P ALL 5 1	or /usr/bin/mpstat -A 5 1
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	--	intr in /usr/bin/mpstat -p 5 2	int in /usr/bin/mpstat 5 1	intr/s in /usr/bin/mpstat -P ALL 5 1 or /usr/bin/mpstat -A 5 1
System % (SYSTEM_PERCENT)	%sys in /usr/sbin/sar -u -M 5 1	sys in /usr/bin/mpstat -p 5 2	sys% in /usr/sbin/sar -u -P ALL 5 1	%sys (%system) in /usr/bin/mpstat -P ALL 5 1 or %sys in /usr/bin/mpstat -A 5 1
User % (USER_PERCENT)	%usr in /usr/sbin/sar -u -M 5 1	usr in /usr/bin/mpstat -p 5 2	usr% in /usr/sbin/sar -u -P ALL 5 1	%user + %nice in /usr/bin/mpstat -P ALL 5 1 or %usr + %nice in /usr/bin/mpstat -A 5 1
Wait % (WAIT_PERCENT)	%wio in /usr/sbin/sar -u -M 5 1	wt in /usr/bin/mpstat -p 5 2	wio% in /usr/sbin/sar -u -P ALL 5 1	%iowait in /usr/bin/mpstat -P ALL 5 1 or /usr/bin/mpstat -A 5 1
Ext1 (EXT1)	--	--	physc in /usr/sbin/sar -u -P ALL 5 1	user% in /usr/bin/mpstat -P ALL 5 1 or %usr in /usr/bin/mpstat -A 5 1
Ext2 (EXT2)	--	--	%entc in /usr/sbin/sar -u -P ALL 5 1	nice% in /usr/bin/mpstat -P ALL 5 1 or /usr/bin/mpstat -A 5 1

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(9) System Status (PD)

The following table lists the data sources for the individual fields of the System Status (PD) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ	date -u +%Y-%m-%dT%H:%M:%SZ
Status (STATUS)	--	--	--	--
Reason (REASON)	--	--	--	--
OS Type (OS_TYPE)	HP-UX (fixed)	SunOS (fixed)	AIX (fixed)	Linux (fixed)
Version (VERSION)	uname -r	uname -r	uname -v "." uname -r	uname -r
Processor Type (PROCESSOR_TYPE)	uname -m	uname -p	uname -p	uname -p
Detail (DETAIL)	uname -a	uname -a	uname -a	uname -a
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

--: Indicates that no field value obtained by processing performance data is set.

(10) System Summary (PI)

The following table lists the data sources for the individual fields of the System Summary (PI) record.

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Record Type (INPUT_RECORD_TYPE)	--	--	--	--
Record Time (RECORD_TIME)	--	--	--	--
Interval (INTERVAL)	--	--	--	--
VA DeviceID (VADEVICEID)	--	--	--	--
Target Host (TARGET_HOST)	--	--	--	--
Polling Time (POLLING_TIME)	--	--	--	--
Target Host Time (TARGET_HOST_TIME)	/usr/bin/date -u +%Y-%m-%dT%H:%M:%SZ	/usr/bin/date -u +%Y-%m-%dT%H:%M:%SZ	/usr/bin/date -u +%Y-%m-%dT%H:%M:%SZ	/bin/date -u +%Y-%m-%dT%H:%M:%SZ
Active CPUs (ACTIVE_CPUS)	Number of CPUs displayed in /usr/sbin/sar -M -u 5 1	Number of CPUs displayed in /usr/bin/mpstat -p 5 2	Number of CPUs displayed in /usr/sbin/sar -u -P ALL 5 1	Number of CPUs displayed in /usr/bin/mpstat -P ALL 5 1

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
CPU % (CPU_PERCENT)	CPU_PERCENT in the _Total instance of the PI_CPU record	CPU_PERCENT in the _Total instance of the PI_CPU record	CPU_PERCENT in the _Total instance of the PI_CPU record	CPU_PERCENT in the _Total instance of the PI_CPU record
Idle % (IDLE_PERCENT)	IDLE_PERCENT in the _Total instance of the PI_CPU record	IDLE_PERCENT in the _Total instance of the PI_CPU record	IDLE_PERCENT in the _Total instance of the PI_CPU record	IDLE_PERCENT in the _Total instance of the PI_CPU record
System % (SYSTEM_PERCENT)	SYSTEM_PERCENT in the _Total instance of the PI_CPU record	SYSTEM_PERCENT in the _Total instance of the PI_CPU record	SYSTEM_PERCENT in the _Total instance of the PI_CPU record	SYSTEM_PERCENT in the _Total instance of the PI_CPU record
User % (USER_PERCENT)	USER_PERCENT in the _Total instance of the PI_CPU record	USER_PERCENT in the _Total instance of the PI_CPU record	USER_PERCENT in the _Total instance of the PI_CPU record	USER_PERCENT in the _Total instance of the PI_CPU record
Wait % (WAIT_PERCENT)	WAIT_PERCENT in the _Total instance of the PI_CPU record	WAIT_PERCENT in the _Total instance of the PI_CPU record	WAIT_PERCENT in the _Total instance of the PI_CPU record	WAIT_PERCENT in the _Total instance of the PI_CPU record
Processor Queue Length (PROCESSOR_QUEUE_LENGTH)	--	--	--	--
Run Queue Avg 5 min (RUN_QUEUE_AVG_5_MIN)	Second value in load average of /usr/bin/uptime	Second value in load average of /usr/bin/uptime	Second value in load average of /usr/bin/uptime	Second value in load average of /bin/uptime
Interrupt Counts/sec (INTERRUPT_COUNTS_PER_SEC)	device interrupts ÷ △ *collection time* in △ /usr/bin/vmstat -s	INTERRUPT_COUNTS_PER_SEC in the _Total instance of the PI_CPU record	INTERRUPT_COUNTS_PER_SEC in the _Total instance of the PI_CPU record	INTERRUPT_COUNTS_PER_SEC in the _Total instance of the PI_CPU record
Effective Free Mem % (EFFECTIVE_FREE_MEM_PERCENT)	--	--	--	(EFFECTIVE_FREE_MEM_MBYTES ÷ TOTAL_MEM_MBYTES) × 100
Effective Free Mem Mbytes (EFFECTIVE_FREE_MEM_MBYTES)	--	--	--	-/+ buffer / cache in free of free -m
Free Mem % (FREE_MEM_PERCENT)	100 × FREE_MEM_MBYTES ÷ TOTAL_MEM_MBYTES	100 × FREE_MEM_MBYTES ÷ TOTAL_MEM_MBYTES	100 × FREE_MEM_MBYTES ÷ TOTAL_MEM_MBYTES	100 × FREE_MEM_MBYTES ÷ TOTAL_MEM_MBYTES
Free Mem Mbytes (FREE_MEM_MBYTES)	free × PAGESIZE ÷ (1,024 × 1,024) in memory of /usr/bin/vmstat 5 2	freemem × PAGESIZE ÷ (1,024 × 1,024) in /usr/sbin/sar -r 5 1	free pages × PAGESIZE ÷ (1,024 × 1,024) in /usr/bin/vmstat -v	Mem in free of /usr/bin/free -m
Used Mem % (USED_MEM_PERCENT)	100 × USED_MEM_MBYTES ÷	100 × USED_MEM_MBYTES ÷	100 × USED_MEM_MBYTES ÷	100 × USED_MEM_MBYTES ÷

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Used Mem % (USED_MEM_PERCENT)	TOTAL_MEM_MBYTES	TOTAL_MEM_MBYTES	TOTAL_MEM_MBYTES	TOTAL_MEM_MBYTES
Used Mem Mbytes (USED_MEM_MBYTES)	TOTAL_MEM_MBYTES - FREE_MEM_MBYTES	TOTAL_MEM_MBYTES - FREE_MEM_MBYTES	TOTAL_MEM_MBYTES - FREE_MEM_MBYTES	Mem in used of /usr/bin/free -m
Total Mem Mbytes (TOTAL_MEM_MBYTES)	Total pages on system × PAGESIZE ÷ (1,024 × 1,024) in /sbin/crashconf | grep system:	Memory size in /usr/sbin/prtconf | grep Memory	memory pages × PAGESIZE /(1,024 × 1,024) in /usr/bin/vmstat -v	Mem in total of /usr/bin/free -m
Free Swap % (FREE_SWAP_PERCENT)	100 × FREE_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	100 × FREE_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	100 × FREE_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	100 × FREE_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES
Free Swap Mbytes (FREE_SWAP_MBYTES)	dev in Mb_FREE of /usr/sbin/swapinfo -m	free × 512 ÷ (1,024 × 1,024) in /usr/sbin/swap -l	FREE PAGES × PAGESIZE ÷ (1,024 × 1,024) in /usr/sbin/pstat -s	Swap in free of /usr/bin/free -m
Used Swap % (USED_SWAP_PERCENT)	100 × USED_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	100 × USED_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	100 × USED_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES	100 × USED_SWAP_MBYTES ÷ TOTAL_SWAP_MBYTES
Used Swap Mbytes (USED_SWAP_MBYTES)	dev in Mb_USED of /usr/sbin/swapinfo -m	TOTAL_SWAP_MBYTES - FREE_SWAP_MBYTES	USED PAGES × PAGESIZE ÷ (1,024 × 1,024) in /usr/sbin/pstat -s	Swap in used of /usr/bin/free -m
Total Swap Mbytes (TOTAL_SWAP_MBYTES)	dev in Mb_AVAIL of /usr/sbin/swapinfo -m	blocks × 512 ÷ (1,024 × 1,024) in /usr/sbin/swap -l	(USED PAGES + FREE PAGES) × PAGE SIZE ÷ (1,024 × 1,024) in /usr/sbin/pstat -s	Swap in total of /usr/bin/free -m
Page Fault Counts/sec (PAGE_FAULT_COUNTS_PER_SEC)	--	(minor (as) faults + major faults + copy-on-write faults) ÷ △ *collection time* in △ /usr/bin/vmstat -s	faults/s in /usr/sbin/sar -r 5 1	--
Page Scan Counts/sec (PAGE_SCAN_COUNTS_PER_SEC)	pages scanned for page out ÷ △ *collection time* in	--	pages examined by clock ÷ △ *collection time* in	--

PFM - View name (PFM - Manager name)	Data source			
	HP-UX	Solaris	AIX	Linux
Page Scan Counts/sec (PAGE_SCAN_COUNTS_PER_SEC)	△ /usr/bin/vmstat -s	--	△ /usr/bin/vmstat -s	--
Page-In Counts/sec (PAGE_IN_COUNTS_PER_SEC)	page ins ÷ △ *collection time* in △ /usr/bin/vmstat -s	page ins ÷ △ *collection time* in △ /usr/bin/vmstat -s	page ins ÷ △ *collection time* in △ /usr/bin/vmstat -s	--
Page-Out Counts/sec (PAGE_OUT_COUNTS_PER_SEC)	page outs ÷ △ *collection time* in △ /usr/bin/vmstat -s	page outs ÷ △ *collection time* in △ /usr/bin/vmstat -s	page outs ÷ △ *collection time* in △ /usr/bin/vmstat -s	--
Page-In Pages/sec (PAGE_IN_PAGES_PER_SEC)	pages paged in ÷ △ *collection time* in △ /usr/bin/vmstat -s	pages paged in ÷ △ *collection time* in △ /usr/bin/vmstat -s	--	pages paged in ÷ △ *collection time* in △ /usr/bin/vmstat -s
Page-Out Pages/sec (PAGE_OUT_PAGES_PER_SEC)	pages paged out ÷ △ *collection time* in △ /usr/bin/vmstat -s	pages paged out ÷ △ *collection time* in △ /usr/bin/vmstat -s	--	pages paged out ÷ △ *collection time* in △ /usr/bin/vmstat -s
Paging Pages/sec (PAGING_PAGES_PER_SEC)	--	--	--	--
Pool Nonpaged KBytes (POOL_NONPAGED_KBYTES)	--	--	--	--
Swap-In Counts/sec (SWAP_IN_COUNTS_PER_SEC)	swpin/s in /usr/sbin/sar -w 5 1	swpin/s in /usr/sbin/sar -w 5 1	--	--
Swap-Out Counts/sec (SWAP_OUT_COUNTS_PER_SEC)	swpot/s in /usr/sbin/sar -w 5 1	swpot/s in /usr/sbin/sar -w 5 1	--	--
Swap-In Pages/sec (SWAP_IN_PAGES_PER_SEC)	pages swapped in ÷ △ *collection time* in △ /usr/bin/vmstat -s	pages swapped in ÷ △ *collection time* in △ /usr/bin/vmstat -s	--	pswpin/s in /usr/bin/sar -w 5 1
Swap-Out Pages/sec (SWAP_OUT_PAGES_PER_SEC)	pages swapped out ÷ △ *collection time* in △ /usr/bin/vmstat -s	pages swapped out ÷ △ *collection time* in △ /usr/bin/vmstat -s	--	pswpout/s in /usr/bin/sar -w 5 1
Ext1 (EXT1)	--	--	--	--
Ext2 (EXT2)	--	--	--	--

Legend:

△ : Indicates a value obtained by subtracting *previously collected value* from *current collected value*.

--: Indicates that no field value obtained by processing performance data is set.

K. Linkage to JP1/ITSLM

Linkage to JP1/ITSLM can enhance the operation status monitoring performed by PFM - RM for Platform.

To make it easier to monitor on JP1/ITSLM, PFM - RM for Platform provides PFM - Manager with default monitoring items for JP1/ITSLM.

The table below shows the default monitoring items that PFM - RM for Platform provides to PFM - Manager.

For multi-instance records, records matching the value specified for the key are collected. To see the key used for the collection target, check the collection result for each record.

For `Effective Free Memory`, 0 is output in Windows, AIX, HP-UX, and Solaris. For `Network Bytes`, `0` is output in UNIX.

Table K–1: Default monitoring items PFM - RM for Platform provides to PFM - Manager

Display name in JP1/ITSLM	Explanation	Record (record ID)	Key (PFM-Manager name)	Field name
`CPU Usage`	Process's CPU usage (%)	System Summary (`PI`)	--	`CPU_PERCENT`
`Available Memory`	Total size of unused physical memory (megabytes)	System Summary (`PI`)	--	`FREE_MEM_MBYTES`
`Effective Free Memory`	Size of unused physical memory that applications can actually use (megabytes)	System Summary (`PI`)	--	`EFFECTIVE_FREE_MEM_MBYTES`
`Logical Disk Free Size`	Size of unused area (megabytes)	Logical Disk Overview (`PI_LDSK`)	ID (`ID`)	`FREE_MBYTES`
`Disk Busy %`	Percentage of time the disk was busy when a loading or writing request was received (%)	Physical Disk Overview (`PI_PDSK`)	ID (`ID`)	`BUSY_PERCENT`
`Network Bytes`	Rate at which data is sent or received through the network interface (bytes/second)	Network Interface Overview (`PI_NET`)	ID (`ID`)	`TOTAL_BYTES_PER_SEC`
`Network Packets`	Rate at which packets are sent or received through the network interface (packets/second)	Network Interface Overview (`PI_NET`)	ID (`ID`)	`TOTAL_PACKETS_PER_SEC`

Legend:
--: Not applicable

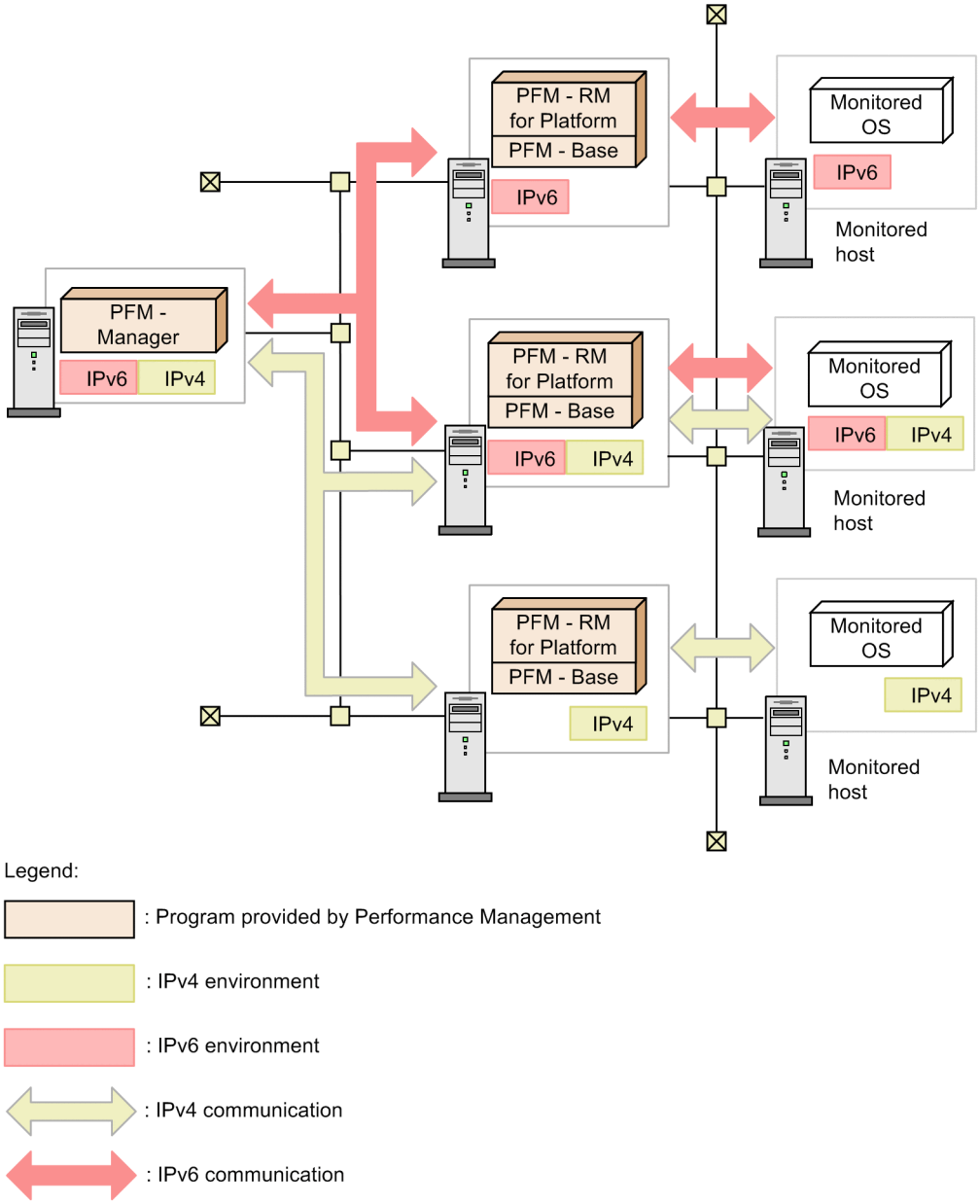
To implement these default monitoring items in PFM - Manage, you must copy the setup file and execute the setup command. For details, see *3.1.4 Setup procedure for the Windows edition* or *3.2.4 Setup procedure for the UNIX edition*.

L. Communication in IPv4 and IPv6 Environments

Performance Management supports both IPv4 and IPv6 network environments. Therefore, you can run Performance Management even in a network environment where IPv4 and IPv6 coexist.

However, this applies only when the OS of the hosts on which PFM - RM for Platform and PFM - Manager are installed is Windows Server 2008 R2, Windows Server 2012, or Linux.

Figure L–1: Scope to which communication in IPv4 and IPv6 environments applies



To enable communication in an IPv6 environment, you must execute the `jpcconf ipv6 enable` command. For details about this command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*. For details about the conditions and timing for executing the `jpcconf ipv6 enable` command, see the chapter that describes an example of a network configuration that includes an IPv6 environment in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

M. Version Changes

M.1 Changes in 10-50

Note: The changes include the functions that were added between version 10-00 and version 10-50.

- The following OSs are now supported:
  - Linux 5 (x64)
  - Linux 5 Advanced Platform (x64)
- The timing of performance data collection by the collection process was changed.
- The following OSs are now supported as monitoring targets:
  - CentOS 6 (x64)
  - CentOS 6 (x86)
  - Oracle Linux 6 (x64)
  - Oracle Linux 6 (x86)
  - Solaris 11 (SPARC)
  - SuSE Linux 11 (x64)
  - SuSE Linux 11 (x86)
- The common account information function is now supported.
- The unit used in the formula for estimating the agent log size was changed from kilobytes to megabytes.
- Information about the number of agent log files that can be collected per instance was added.
- `Over 10 Sec Collection Time` was added as a property related to the performance data collection conditions for each record.
- The following messages were added:
  `KAVL17028-E`, `KAVL17029-W` to `KAVL17033-W`, `KAVL17034-E`, `KAVL17035-W`, `KAVL17036-W`
- The following messages were changed:
  `KAVL17005-E`, `KAVL17017-W`, `KAVL17022-W`, `KAVL17023-W`, `KAVL17026-W`
- The following files were added to agent logs:
  - `collect_core_`*nn*
  - `timer_core_`*nn*
- The agent log output method was changed from the wrap-around method to a sequential method.
- A formula for estimating the amount of disk space used by agent logs per instance was added.
- The following properties for multiple monitoring were added:
  - `Primary Manager`
  - `Secondary Manager`
- `Realtime Report Data Collection Mode` was added as a property that is used when historical data collection takes priority over real-time report display processing.
- The following files were added:
  - `suspended.dat`

- *monitoring-target-name*_suspended.dat

M.2 Changes in 10-00

- The following OSs are now supported:
  - HP-UX 11i V2 (IPF)
  - Solaris 9 (SPARC)
  - AIX 5L V5.3
  - Red Hat Enterprise Linux(R) AS 4 (IPF)
  - Red Hat Enterprise Linux(R) AS 4 (AMD64 & Intel EM64T)
  - Red Hat Enterprise Linux(R) ES 4 (AMD64 & Intel EM64T)
  - Red Hat Enterprise Linux(R) AS 4 (x86)
  - Red Hat Enterprise Linux(R) ES 4 (x86)
- The following collection processes were added to enable WMI collection processing according to the OS type:
  - jpc7corecollect32.exe (32-bite edition)
  - jpc7corecollect64.exe (64-bit edition)
- If the OS of the host where PFM - RM for Platform is installed is Windows Server 2008 R2, Windows Server 2012, or Linux, PFM - RM for Platform can collect performance data even in an IPv6 environment.
- The following default monitoring items are now availablefor PFM - Manager, making it possible for PFM - RM for Platform to link to JP1/ITSLM:
  - CPU_PERCENT
  - FREE_MEM_MBYTES
  - EFFECTIVE_FREE_MEM_MBYTES
  - FREE_MBYTES
  - BUSY_PERCENT
  - TOTAL_BYTES_PER_SEC
  - TOTAL_PACKETS_PER_SEC
- A function was added for monitoring a monitored host in a UNIX environment from a PFM - RM host in a Windows environment.
- A function was added for specifying collection of process operation status information by executing the jpcprocdef create command.
- An explanation was added about software and packages that must be installed when the monitored host is running UNIX.
- An explanation was added about the operation for distributing a public key to the monitored host by executing the ssh-copy-id command.
- The following files were added under the *installation-folder*\agt7\agent*instance-name*\targets*monitoring-target-name*\ folder to the list of folders and files when PFM - RM for Platform is running under Windows:
  - records.stderr_*NNNN*

  - common.stdout_*NNNN*
  - common.stderr_*NNNN*
  - os.stdout_*NNNN*
  - os.stderr_*NNNN*
  - wmi.out_*NNNN*
- An explanation was added about the function for synchronizing the agent information between the PFM - Manager host and the PFM - Web Console host by executing the jpctool service sync command.
- The explanation for the Reason (REASON) field of the System Status (PD) record was changed due to the addition of the function for monitoring a monitored host in a UNIX environment from a PFM - RM host in a Windows environment.
- An explanation was added about cases in which performance data cannot be collected accurately.
- The following messages were added:
  KAVL17023-W, KAVL17024-W, KAVL17025-W, KAVL17026-W
- The explanation for message KAVL17017-W was changed.
- An explanation was added about the action to take when the following problems occur:
  - The Remote Monitor Collector service of PFM - RM does not start.
  - Failure Audit (event ID: 4625 or 4776) is recorded in the Windows security event log.
- An explanation was added about the action to take when the value of the Status field of the PD record is ERROR and the Reason field shows one of the following values:
  - Invalid environment(SSH_Client)
  - Invalid environment(Perl_Module)
  - Invalid environment(Private_Key_File)
- An explanation was added about the action to take when the alarms related to process monitoring are not reported as intended.
- Windows firewall information that needs to be collected is now included in the OS log information.
- An explanation was added about information that needs to be collected by PuTTY and ActivePerl.
- The estimate on the amount of memory required was added.
- The following properties were added to the Remote Monitor Configuration - Remote Monitor directory of the Remote Monitor Collector service:
  - SSH_Client
  - Perl_Module
- The TargetType property was added to the Remote Monitor Configuration - Target directory of the remote agent and group agent of PFM - RM for Platform.
- The following files under the *installation-folder*\agt7\dat\ folder were added to the list of folders and files when PFM - RM for Platform is running under Windows:
  - common.dat
  - cmd2rec
  - cmd2rec_common
  - cmd2rec_OS

    - OS.dat
- A list of redistribution files for Microsoft(R) Visual C++(R) 2005 SP1 that need to be installed in the Windows Server 2003 environment was added.
- An explanation was added about the sources of record field values or formulas (data sources).
- A function was added for monitoring process operation status.
- The following records were added due to the addition of the function for monitoring process operation status:
    - Application Process Count (PD_APPC)
    - Application Process Detail (PD_APPD)
    - Application Process Overview (PD_APS)
    - Application Service Overview (PD_ASVC)
    - Application Summary (PD_APP2)
- The following alarms were added due to the addition of the function for monitoring process operation status:
    - Application Status
    - Process Existence
    - Service Stop
    - Service Stop(dsp nm)
- The following reports were added due to the addition of the function for monitoring process operation status:
    - Application Process Count
    - Application Process Status
    - Application Status
- Windows Server 2008 is now supported.
- The setup command was changed so that it can be executed in non-interactive mode.
- Ps_Category was added to the instance environment settings of PFM - RM for Platform due to the addition of the function for monitoring process operation status.
- The ps command was added to the package (commands) required by a monitored host due to the addition of the function for monitoring process operation status.
- The version of the monitoring template alarm table was changed from 09.00 to 09.10.
- The following alarm tables were added due to the addition of the function for monitoring process operation status:
    - PFM RM Platform Template Alarms [PS] 09.10
    - PFM RM Platform Template Alarms [SVC] 09.10
    - PFM RM Platform Template Alarms [APP] 09.10
- Notes were added about collecting historical data.
- Estimates were added on the amount of memory and disk space required.
- The following logs are now included in the information that needs to be collected in the Windows environment:
    - WMI log
    - Message log during installation (for Windows Server 2008)
- The following directories were added to the remote agent and group agent properties due to the addition of the function for monitoring process operation status:

  - Application monitoring setting
  - ADDITION OR DELETION A SETTING
- The data model version was changed from 4.0 to 5.0.

N. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

N.1 Related publications

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

Manuals associated with JP1/Performance Management:

- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management Planning and Configuration Guide* (3021-3-347(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management User's Guide* (3021-3-348(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management Reference* (3021-3-349(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* (3021-3-354(E)), for Windows systems
- *Job Management Partner 1 Version 10 Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* (3021-3-355(E)), for UNIX systems

Manuals associated with JP1:

- *Job Management Partner 1 Version 6 Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide* (3000-3-841(E))
- *Job Management Partner 1 Version 8 Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide* (3020-3-L42(E)), for UNIX systems
- *Job Management Partner 1 Version 9 Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems
- *Job Management Partner 1 Version 9 Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems

N.2 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
AIX		AIX V6.1
		AIX V7.1
HP-UX	HP-UX (IPF) or HP-UX 11i (IPF)	HP-UX 11i V3 (IPF)
Internet Explorer		Windows(R) Internet Explorer(R)
JP1/Base		Job Management Partner 1/Base
JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View	Job Management Partner 1/Integrated Management - View

Abbreviation			Full name or meaning
JP1/ITSLM	JP1/ITSLM - Manager		Job Management Partner 1/IT Service Level Management - Manager
	JP1/ITSLM - UR		Job Management Partner 1/IT Service Level Management - User Response
JP1/Software Distribution			Job Management Partner 1/Software Distribution Client
			Job Management Partner 1/Software Distribution Manager
			Job Management Partner 1/Software Distribution SubManager
Linux	Linux (IPF)	Linux 5 (IPF)	Red Hat Enterprise Linux(R) 5 (IPF)
		Linux 5 Advanced Platform (IPF)	Red Hat Enterprise Linux(R) 5 Advanced Platform (IPF)
	Linux (x64)	CentOS 6 (x64)	CentOS 6 version 6.1 or later
		Linux 5 (x64)	Red Hat Enterprise Linux(R) 5 (AMD/Intel 64)
		Linux 5 Advanced Platform (x64)	Red Hat Enterprise Linux(R) 5 Advanced Platform (AMD/Intel 64)
		Linux 6 (x64)	Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)
		Oracle Linux 6 (x64)	Oracle Linux 6 (Red Hat Compatible Kernel) version 6.1 or later
		SUSE Linux Enterprise Server 11 (x64)	SUSE Linux Enterprise Server 11
	Linux (x86)	CentOS 6 (x86)	CentOS 6 version 6.1 or later
		Linux 5 (x86)	Red Hat Enterprise Linux(R) 5 (x86)
		Linux 5 Advanced Platform (x86)	Red Hat Enterprise Linux(R) 5 Advanced Platform (x86)
		Linux 6 (x86)	Red Hat Enterprise Linux(R) Server 6 (32-bit x86)
		Oracle Linux 6 (x86)	Oracle Linux 6 (Red Hat Compatible Kernel) version 6.1 or later
		SUSE Linux Enterprise Server 11 (x86)	SUSE Linux Enterprise Server 11
NNM	HP NNM		HP Network Node Manager Software version 6 or earlier
			HP Network Node Manager Starter Edition Software version 7.5 or earlier
Performance Management			Job Management Partner 1/Performance Management
PFM - Agent	PFM - Agent for Enterprise Applications		JP1/Performance Management - Agent Option for Enterprise Applications
	PFM - Agent for Microsoft SQL Server		JP1/Performance Management - Agent Option for Microsoft(R) SQL Server
	PFM - Agent for Oracle		JP1/Performance Management - Agent Option for Oracle
	PFM - Agent for Platform	PFM - Agent for Platform(UNIX)	JP1/Performance Management - Agent Option for Platform(for UNIX systems)

Abbreviation			Full name or meaning
PFM - Agent	PFM - Agent for Platform	PFM - Agent for Platform(Windows)	JP1/Performance Management - Agent Option for Platform(for Windows systems)
	PFM - Agent for Service Response		JP1/Performance Management - Agent Option for Service Response
PFM - Base			Job Management Partner 1/Performance Management - Base
PFM - Manager			Job Management Partner 1/Performance Management - Manager
PFM - RM	PFM - RM for Microsoft SQL Server		JP1/Performance Management - Remote Monitor for Microsoft(R) SQL Server
	PFM - RM for Oracle		JP1/Performance Management - Remote Monitor for Oracle
	PFM - RM for Platform		JP1/Performance Management - Remote Monitor for Platform
	PFM - RM for Virtual Machine		JP1/Performance Management - Remote Monitor for Virtual Machine
PFM - Web Console			JOB MANAGEMENT PARTNER 1/Performance Management - Web Console
Solaris	Solaris 10		Solaris 10 (SPARC)
			Solaris 10 (x64)
			Solaris 10 (x86)
	Solaris 11		Solaris 11 (SPARC)
Visual C++			Microsoft(R) Visual C++(R)

- *PFM - RM*, *PFM - Manager*, *PFM - Agent*, *PFM - Base*, and *PFM - Web Console* are sometimes collectively referred to as *Performance Management*.
- *HP-UX*, *Solaris*, *AIX*, and *Linux* are sometimes collectively referred to as *UNIX*.

N.3 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
CPU	Central Processing Unit
CSV	Comma Separated Value
DCOM	Distributed Component Object Model
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
IP	Internet Protocol
IPF	Itanium(R) Processor Family

Acronym	Full name or meaning
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LAN	Local Area Network
NAPT	Network Address Port Translation
NAT	Network Address Translation
NIC	Network Interface Card
ODBC	Open Database Connectivity
OS	Operating System
PDF	Portable Document Format
RAM	Random Access Memory
RAS	Remote Access Service
SCM	Service Control Manager
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UAC	User Access Control
Web	World Wide Web
WMI	Windows Management Instrumentation
WPAR	Workload Partition

N.4 Notation for product names, service IDs, and service keys in this manual

In Performance Management, version 09-00 and later, enabling the product name display functionality allows you to display service IDs and service keys with product names.

Identifier	Product name display functionality	
	Disabled	Enabled
Service ID	`TS1`*host-name*	*host-name*`<RM Platform>(Store)`
	`TA1`*host-name*	*host-name*`<RM Platform>`
Service key	`agt7`	`RMPlatform`

In this manual, service IDs and service keys are shown in the formats that are in effect when the product name display functionality is enabled.

You can enable the product name display functionality only when both of the following conditions are satisfied:

- The version of the prerequisite program (PFM - Manager or PFM - Base) on the same device as PFM - RM for Platform is 09-00 or later.
- The versions of PFM - Web Console and PFM - Manager on the connection target are 09-00 or later.

N.5 Meaning of "folder" and "directory"

In general, if a Windows folder name is the same as its counterpart UNIX directory name, it is referred to in this manual by its UNIX directory name.

N.6 Notation for folder path names in this manual

In Windows Server 2008, Windows Server 2012, the system-drive\Program Files part might differ depending on the environment because it is determined by the OS environment variable at installation.

The default installation folders for the Windows edition of Performance Management are as follows:

Default installation folder for PFM - Base

- For Windows Server 2003 (x64), the 64-bit edition of Windows Server 2008, or Windows Server 2012
  system-drive`\Program Files (x86)\Hitachi\jp1pc`
- All other cases
  system-drive`\Program Files\Hitachi\jp1pc`

In this manual, the installation folder of PFM - Base is shown as *installation-folder*.

Default installation folder for PFM - Manager

- For Windows Server 2003 (x64), the 64-bit edition of Windows Server 2008, or Windows Server 2012
  system-drive`\Program Files (x86)\Hitachi\jp1pc`
- All other cases
  system-drive`\Program Files\Hitachi\jp1pc`

Default installation folder for PFM - Web Console

- For Windows Server 2003 (x64), the 64-bit edition of Windows Server 2008, or Windows Server 2012
  system-drive`\Program Files (x86)\Hitachi\jp1pcWebCon`
- All other cases
  system-drive`\Program Files\Hitachi\jp1pcWebCon`

N.7 NNM products supported by Performance Management

Performance Management supports linkage to the following products:

- HP Network Node Manager Software version 6 or earlier
- HP Network Node Manager Starter Edition Software version 7.5 or earlier

In this manual, these products are referred to as *NNM*, and the functionality that provides linkage with these products is referred to as *NNM linkage.*

Note that Performance Management does not support linkage with the following product:

- HP Network Node Manager i Software v8.10

N.8 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

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

O. Glossary

action

An operation that is executed automatically by Performance Management when data being monitored reaches a threshold. The following are the types of actions:

- Sending an email
- Executing a command
- Issuing an SNMP trap
- Issuing a JP1 event

Action Handler

One of the PFM - Manager or PFM - RM services. This service executes actions.

administration tool

Various commands and GUI functions that are used to check the service status and to manipulate performance data. It provides the following functions:

- Displaying the configuration and status of services
- Backing up and restoring performance data
- Exporting performance data to a text file
- Erasing performance data

agent

The PFM - RM service that collects performance data.

alarm

Information that defines an action to be executed and the event message to be sent when the data being monitored reaches a threshold.

alarm table

A table consisting of at least one alarm that defines the following information:

- Object to be monitored (such as Process, TCP, or WebService)
- Information to be monitored (such as the CPU usage rate or the number of bytes received per second)
- Condition to be monitored (such as a threshold value)

bind

Process of associating an alarm with an agent. When an alarm is bound to an agent, the user can be notified when the performance data collected by the agent reaches the threshold defined for the alarm.

cluster system

A system of multiple server systems that are linked to each other. The two types of cluster systems are a High Availability (HA) cluster system and a load-balancing cluster system.

An HA cluster system achieves high availability. Its purpose is to provide continuous operation even in the event of a failure. If a server fails during application processing, a standby server inherits the processing. This prevents the application from being interrupted in the event of a failure, thereby improving availability.

A load-balancing cluster system distributes the workload among multiple nodes in order to improve throughput. If a node stops due to a failure, this method can also improve availability by switching nodes so that processing can continue.

In this manual, *cluster system* refers to an HA cluster system.

common account information

Each PFM - RM host can centrally manage the account information that is common in multiple instance environments or on monitored targets. Common account information consists of `pfmhost` for instance environments, and `wmi` (for Windows) and `ssh` (for UNIX) for monitored targets.

Correlator

One of the PFM - Manager services. This service controls event transmission between services. When the Correlator checks an alarm status and determines that the threshold value has been exceeded, it sends an alarm event and an agent event to the Trap Generator service and to PFM - Web Console.

database ID

ID of a database that is added to each of PFM - RM's records. The database ID indicates the type of the records that are stored in the corresponding database. The following are the database IDs:

- PI
  Indicates a database for records of the PI record type
- PD
  Indicates a database for records of the PD record type

data model

A collective name for the records and fields of a PFM - RM. A data model is managed by its version.

drilldown report

A report that is associated with another report or with a field in a report. Use a drilldown report to display detailed or related information about a report.

executing node

The node executing jobs at one of the server systems that constitute a cluster system (node whose logical host is active).

failover

Inheritance in a cluster system of a server's job processing from the executing node to the standby node in the event of a failure.

field

A unit of performance data; multiple fields constitute a record.

function ID

A 1-byte identifier that indicates the function type of a Performance Management program service. This is part of the service ID.

historical report

A report indicating the status of a monitoring target from a point in time in the past to the current time.

instance

In this manual, the term *instance* is used as follows:

- When referring to the record format

  Each row in a record is called an *instance*. A record consisting of a single row is called a *single-instance record*, while a record consisting of multiple rows is called a *multi-instance record*.

- When referring to the PFM - Agent and PFM - RM startup method

  A single agent that monitors the target on the same host is called a *single-instance agent*. On the other hand, when the monitoring target supports multiple instances, an agent that monitors all instances of the monitoring target is called a *multi-instance agent*. Each agent constituting the multi-instance agent is called an *instance*.

instance number

An identifier indicating a 1-byte management number that is used for internal processing. An instance number is part of the service ID.

JP1/ITSLM

A product that helps maintain service levels by monitoring the performance of a business system as experienced by service users. Linking to JP1/ITSLM can enhance the operation status monitoring performed by PFM - RM for Platform.

lifetime

The period over which consistency of the performance data collected in a record is guaranteed.

Master Manager

One of the PFM - Manager services. This is PFM - Manager's main service.

Master Store

One of the PFM - Manager services. This service manages the alarm events issued from each PFM - Agent or PFM - RM. The Master Store service uses a database to retain event data.

monitored host

A host that is monitored by PFM - RM for Platform.

monitoring template

Predefined alarms and reports provided by PFM - RM. The monitoring template simplifies preparations for monitoring the operation status of PFM - RM because the user does not have to create complex definitions.

multi-instance record

A record consisting of multiple rows. Multi-instance records have unique ODBC key fields.

See *instance*.

multiple monitoring

An operation where a duplicate monitoring manager is employed. This eliminates the downtime in monitoring and increases the availability of the system.

Name Server

One of the PFM - Manager services. This service manages service configuration information in the system.

non-interactive (commands)

A mode of executing commands in which user entries required for the execution of commands are provided by means of specification of options or by reading from a definition file rather than by prompting the user to enter responses.

Executing commands non-interactively reduces the burden on the user by helping to automate the installation of the operation monitoring system.

ODBC key field

A field that is needed in order to use SQL with PFM - Manager or PFM - Base to access data in the records stored in a Store database. Some ODBC key fields are common to all records and some are specific to individual records.

PD record type

See *Product Detail record type*.

performance data

Data collected from a monitored system about the operation status of its resources.

Performance Management

A collective name for a group of software programs that are provided for monitoring and analyzing issues related to system performance. Performance Management consists of the following five program products:

- PFM - Manager
- PFM - Web Console
- PFM - Base
- PFM - Agent
- PFM - RM

PFM - Agent

One of the program products constituting Performance Management. PFM - Agent is equivalent to the system monitoring facility. There are various PFM - Agents according to the application being monitored, database, and OS. PFM - Agent provides the following functions:

- Monitoring the performance of the monitoring target
- Collecting and recording data on the monitoring target

PFM - Base

One of the program products constituting Performance Management. It provides Performance Management with the basic operation-monitoring functions. PFM - Base is required in order to run PFM - Agent and PFM - RM. PFM - Base provides the following functions:

- Administrative tools, including various commands
- Common functions needed for linkage between Performance Management and other systems

PFM - Manager

One of the program products constituting Performance Management. PFM - Manager is equivalent to the manager facility and provides the following functions:

- Management of the Performance Management program products
- Management of events

PFM - Manager name

A field name that is specified in SQL statements to access field data in a Store database when SQL is used with PFM - Manager.

A name used to identify a field in a Store database. This name is used to specify fields in commands.

PFM - RM

One of the program products constituting Performance Management. PFM - RM is equivalent to the system monitoring facility. One PFM - RM can monitor multiple targets. There are various PFM - RMs according to the application being monitored, database, and OS. PFM - RM provides the following functions:

- Monitoring the performance of remote monitoring targets
- Collecting and recording data on the monitoring targets

PFM - RM host

A host on which PFM - RM for Platform is installed.

PFM - View name

An alias of the PFM - Manager name. PFM - View names are more intuitive than the PFM - Manager names. For example, a field has the PFM - Manager name `INPUT_RECORD_TYPE`, while its PFM - View name is Record Type. The PFM - View name is used to specify a field using GUI on PFM - Web Console.

PFM - Web Console

One of the program products constituting Performance Management. PFM - Web Console is a browser and provides a Web application server function for achieving central monitoring of the Performance Management system. PFM - Web Console provides the following functions:

- Display of GUI windows
- Integrated monitoring and management
- Definition of reports and alarms

physical host

The environment that is unique to each server constituting a cluster system. A physical host environment is not inherited to any other server even in the event of failover.

PI record type

See *Product Interval record type*.

PL record type

See *Product Log record type*.

primary manager

A manager in a multiple-monitoring configuration, which is prioritized to communicate with monitoring agents (PFM - Agent and PFM - RM).

Product Detail record type

A type of record that stores performance data about the system status at a specific point in time, such as information about the hosts that are being monitored currently. Use the PD record type to obtain the system status at a specific point in time, such as the following:

- System's operation status
- Capacity of the current file system in use

product ID

A 1-byte identifier indicating the Performance Management program product to which a Performance Management program service belongs. This is part of the service ID.

Product Interval record type

A type of record that stores performance data obtained over a specific period of time (interval), such as the CPU usage rate every 5 minutes. Use the PI record type to analyze changes to or trends in the system status over time, such as the following:

- Changes in the number of system calls that are issued over a specific period of time
- Changes in the capacity of the file system being used

Product Log record type

A type of record that stores log information about a database or application being executed on a UNIX system.

real-time report

A report indicating the current status of a monitoring target.

record

A format in which collected performance data is stored. The record type depends on the Store database.

Remote Monitor Collector

One of the PFM - RM services. This service collects performance data and evaluates performance data based on threshold values set for alarms.

remote monitoring

A function for monitoring the operation status of a remote server from a separate host without having to install an agent at the monitored server.

Remote Monitor Store

One of the PFM - RM services. This service stores performance data. The Remote Monitor Store service uses a database to record performance data. There is a Remote Monitor Store service for each PFM - RM.

report

A set of definitions for displaying performance data collected by PFM - RM in a graphical manner. It mainly contains definitions of the following information:

- Records to be displayed in the report
- Performance data items to be displayed
- Performance data display format (such as table or graph)

secondary manager

A manager in a multiple-monitoring configuration, which is not prioritized to communicate with monitoring agents (PFM - Agent and PFM - RM).

service ID

A unique ID that is added to each Performance Management program service. When a command is used to check the configuration of the Performance Management system or to back up individual agents' performance data, the service ID for the Performance Management program is specified in the command.

The format of the service ID depends on the settings for the product name display function. For details about the format of the service ID, see the chapter that describes the functions of Performance Management in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

single-instance record

A record consisting of a single row. Single-instance records do not have a unique ODBC key field.

See *instance*.

stand-alone mode

A status in which PFM - RM is running independently. Even if PFM - Manager's Master Manager and Name Server services cannot be started for a reason such as a failure, PFM - RM can be started independently to collect performance data.

standby node

The node at one of the server systems that constitute a cluster system that is in wait (standby) status so that it can inherit job processing in the event of a failure at the executing node.

See *instance*.

status management function

A function for managing the status of all services that are running on PFM - Manager and PFM - RM. The status management function enables appropriate error recovery actions to be taken promptly because the system administrator can obtain accurate start and stop status information for the services at each host.

Store database

A database in which performance data collected by the Remote Monitor Collector service is stored.

Trap Generator

One of the PFM - Manager services. This service issues SNMP traps.

workgroup

A unit for monitoring processes executed by PFM - RM for Platform. A workgroup can be specified in the following units:

- Windows users
- Windows groups
- Programs executed by a process

Index

A

abbreviations for products 517
acronyms 519
action 25, 523
Action Handler 523
action log
  output format of 477
  outputting 476
  settings for outputting 482
  storage format of 476
  types of events that are output to 476
administration tool 523
agent 523
Agents tree
  deleting monitoring target settings in 176
  setting up collection of process operation status information in 169
  setting up monitoring targets in 169
  using application definition template in 176
alarm 25, 523
  easy setting of 27
alarm table 25, 247, 523

B

backing up 164
  PFM - RM for Platform 164
baseline 33
bind 523
binding 25

C

canceling setup, procedure for
  for UNIX edition 148
  for Windows edition 144
cluster system 523
  applicable to 27
  changing PFM - RM for Platform operation method in 240
  configuration of PFM - RM for Platform in 195
  importing and exporting logical host environment definition file in 242
  operation in 194
  updating instance environment in 240
  updating monitoring target in 241
  WMI connection setting method (when both PFM - RM host and monitored host are running Windows) in 212
cluster system (for UNIX)
  installation and setup flow in 216
  installation and setup in 213
  installation procedure in 218
  issues to consider before installing in 213
  setup procedure in 218
  SSH connection setting method in 225
  uninstallation and unsetup flow in 232
  uninstallation and unsetup in 232
  uninstallation procedure in 238
  unsetup procedure in 233
cluster system (for Windows)
  installation and setup flow in 204
  installation and setup in 200
  installation procedure in 205
  issues to consider before installing in 200
  setup procedure in 205
  SSH connection setting method in (when PFM - RM host is running Windows and monitored host is running UNIX) 212
  uninstallation and unsetup flow in 226
  uninstallation and unsetup in 226
  uninstallation procedure in 231
  unsetup procedure in 227
collection of process operation status information
  example of procedure to follow when alarm is issued during 192
  setting up 169
  setting up (in Services) 180
  setting up (using Agents tree) 169
  setting up (using non-interactive commands) 186
commands
  setting up collection of process operation status information using non-interactive 186
  using, to delete settings for monitoring target 188
  using, to set up monitoring targets 186
common account information 23, 524
common message log 92
conventions
  abbreviations for products 517
  acronyms 519
  diagrams 9
  fonts and symbols 9

KB, MB, GB, and TB 522
mathematical expressions 10
version numbers 10
Correlator 524

D

data
collected for troubleshooting 414
collected from UNIX environment for troubleshooting 418
collected from Windows environment for troubleshooting 414
for troubleshooting, how to collect 421
in UNIX environment for troubleshooting, how to collect 423
in Windows environment for troubleshooting, how to collect 421
database ID 524
data model 24, 322, 524
data sources of records 485
when monitored host is running UNIX 497
when monitored host is running Windows 485
data types, list of 330
diagram conventions 9
directories
list of 463
to check for troubleshooting 408
disk space requirements 429
drilldown report 524

E

error handling procedure 392, 393
example of monitoring
disk 41
memory 38
network 43
processor 33
executing node 524

F

failover 524
processing for (cluster system) 197
when error occurs at PFM - RM host (cluster system) 197
field 24, 524
files, list of 463
firewall passage directions 433
font conventions 9
function ID 525

G

GB meaning 522
glossary 523
group agents 26
list of properties of 453

H

historical report 25, 525

I

identifiers, list of 430
installation 49
installation and setup
in cluster system (for UNIX) 213
in cluster system (for Windows) 200
of UNIX edition 109
of UNIX edition, notes about 141
of Windows edition 50
of Windows edition, notes about 106
installation and setup flow
for UNIX edition 115
for Windows edition 68
in cluster system (for UNIX) 216
in cluster system (for Windows) 204
installation procedure
for UNIX edition 117
for Windows edition 70
in cluster system (for UNIX) 218
in cluster system (for Windows) 205
installing, issues to consider before
in cluster system (for UNIX) 213
in cluster system (for Windows) 200
UNIX edition 109
Windows edition 50
instance 525
instance environment
updating 155
updating, in cluster system 240
instance number 525
IPv4 and IPv6 environments
communication in 511

J

JP1/ITSLM 525
  linkage to 510

K

KB meaning 522

L

lifetime 525
log files to check for troubleshooting 408
logical host environment definition file in cluster system, importing and exporting 242
log information
  collected for troubleshooting 407
  collected for troubleshooting, types of 407

M

manuals
  how to view 167
  settings for using Web browser to reference 166
  setup for referencing 166
Master Manager 525
Master Store 525
mathematical expression conventions 10
MB meaning 522
memory requirements 429
message explanation, format of 374
messages 372, 380
  format of 373
  output destinations of 376
  output format of 373
  output to syslog 379
  output to Windows event log 379
migration
  notes on 474
  procedure for 474
monitored host 22, 525
monitoring
  performance 33
  to see if system is running normally 21
monitoring host 50
monitoring target
  updating 159
  updating, in cluster system 241
monitoring template 27, 244, 525
multi-instance record 525
multiple monitoring 526

N

Name Server 526
non-interactive (commands) 526

O

ODBC key field 526
ODBC key fields, list of 326
operation (in cluster system) 194

P

page faults 39
paging 39
PD record type 24, 526
performance data 526
  changing storage locations of 154
  collecting, by attribute 24
  collecting and managing 30
  collection flow 30
  integrating monitoring and analysis of, for multiple monitored hosts 26
  storing 24
  using collected 24
Performance Management 526
  detecting problems within (troubleshooting) 426
  recovering from system error of (troubleshooting) 427
PFM - Agent 526
PFM - Base 527
PFM - Manager 527
  effects of shutdown and action to take (cluster system) 198
PFM - Manager name 527
PFM - RM 527
PFM - RM for Platform
  changing operation method for 154
  changing operation method for, in cluster system 240
  configuration of (in cluster system) 195
  features of 22
  functions of 29
  overview of 19
  properties of 437
  purposes of performance monitoring using 20
PFM - RM host 527
PFM - View name 527
PFM - Web Console 527

physical host 527
PI record type 24, 528
PL record type 528
port numbers
for PFM - RM for Platform 433
list of 433
primary manager 528
process, example of monitoring 45
processes
list of 431
list of (for UNIX) 431
list of (for Windows) 431
Product Detail record type 528
product ID 528
Product Interval record type 528
Product Log record type 528
properties
list of (Remote Monitor Collector service) 441
list of (Remote Monitor Store service) 437
of group agents, list of 453
of remote agents, list of 453

R

real-time report 25, 528
record 24, 321, 528
records, list of 338
remote agents 26
list of properties of 453
Remote Monitor Collector 528
Remote Monitor Collector service, list of properties of 441
remote monitoring 22, 528
multiple hosts 22
Remote Monitor Store 529
Remote Monitor Store service, list of properties of 437
report 25, 529
easy setting of 27
reports, list of 277
restoring 165
PFM - RM for Platform 164

S

secondary manager 529
service, example of monitoring 45
service ID 529
Services
checking or modifying settings for monitoring targets in 185
deleting settings for monitoring targets in 185
setting up collection of process operation status information in 180
setting up monitoring target in 180
setup 49
setup procedure
for UNIX edition 119
for Windows edition 72
in cluster system (for UNIX) 218
in cluster system (for Windows) 205
single-instance record 529
SSH connection setting method
for UNIX 133
for Windows (when PFM - RM host is running Windows and monitored host is running UNIX) 100
in cluster system (for UNIX) 225
in cluster system (for Windows) (when PFM - RM host is running Windows and monitored host is running UNIX) 212
stand-alone mode 529
standby node 529
status management function 529
Store database 24, 529
swapping 39
symbol conventions 9
system configuration
changing 153
for PFM - RM for Platform, changing 239
system overload, finding cause of 20
system requirements, estimating 429
system resources, identifying effects on 20

T

TB meaning 522
Trap Generator 530
troubleshooting 394
other problems 406
problems with alarm definitions 399
problems with collection and management of performance data 400
problems with command execution 398
problems with report definitions 399
problems with service setup or startup 394

U

uninstallation and unsetup
- in cluster system (for UNIX) 232
- in cluster system (for Windows) 226
- of UNIX edition 148
- of Windows edition 143

uninstallation and unsetup flow
- in cluster system (for UNIX) 232
- in cluster system (for Windows) 226

uninstallation procedure
- for UNIX edition 151
- for Windows edition 146
- in cluster system (for UNIX) 238
- in cluster system (for Windows) 231

uninstalling and canceling setup, issues to consider before
- for UNIX edition 148
- for Windows edition 143

UNIX edition
- installation and setup flow for 115
- installation and setup of 109
- installation procedure for 117
- issues to consider before installing 109
- issues to consider before uninstalling and canceling setup for 148
- notes about installation and setup of 141
- procedure for canceling setup for 148
- setup procedure for 119
- uninstallation and unsetup of 148
- uninstallation procedure for 151

unsetup procedure
- in cluster system (for UNIX) 233
- in cluster system (for Windows) 227

V

version compatibility 475

version number conventions 10

W

Windows edition
- installation and setup flow for 68
- installation and setup of 50
- installation procedure for 70
- issues to consider before installing 50
- issues to consider before uninstalling and canceling setup for 143
- notes about installation and setup of 106
- procedure for canceling setup for 144
- setup procedure for 72
- uninstallation and unsetup of 143
- uninstallation procedure for 146

WMI connection setting method 94
- in cluster system (when both PFM - RM host and monitored host are running Windows) 212

workgroup 530