HITACHI
Inspire the Next

Job Management Partner 1/Performance Management

User's Guide

3020-3-R32(E)

■ Relevant program products

P-242C-AA97 Job Management Partner 1/Performance Management - Manager version 09-00 (for Windows Server 2003)

P-2A2C-AA97 Job Management Partner 1/Performance Management - Manager version 09-00 (for Windows Server 2008)

P-9D2C-AA92 Job Management Partner 1/Performance Management - Manager version 09-00 (for Solaris 9 (SPARC), Solaris 10 (SPARC))

P-1M2C-AA92 Job Management Partner 1/Performance Management - Manager version 09-00 (for AIX 5L V5.3, AIX V6.1)

P-9S2C-BA92 Job Management Partner 1/Performance Management - Manager version 09-00 (for Linux 5 (x86), Linux 5 Advanced Platform (x86), Linux 5 (AMD/Intel 64), Linux 5 Advanced Platform (AMD/Intel 64))

P-242C-AJ97 Job Management Partner 1/Performance Management - Base version 09-00 (for Windows Server 2003)

P-2A2C-AJ97 Job Management Partner 1/Performance Management - Base version 09-00 (for Windows Server 2008)

P-1J2C-AJ92 Job Management Partner 1/Performance Management - Base version 09-00 (for HP-UX 11i V2 (IPF), HP-UX 11i V3 (IPF))

P-9D2C-AJ92 Job Management Partner 1/Performance Management - Base version 09-00 (for Solaris 9 (SPARC), Solaris 10 (SPARC))

P-9E2C-AJ92 Job Management Partner 1/Performance Management - Base version 09-00 (for Solaris 10 (x86), Solaris 10 (x64))

P-1M2C-AJ92 Job Management Partner 1/Performance Management - Base version 09-00 (for AIX 5L V5.3, AIX V6.1)

P-9S2C-BJ92 Job Management Partner 1/Performance Management - Base version 09-00 (for Linux AS 4 (x86), Linux ES 4 (x86), Linux AS 4 (AMD64 & Intel EM64T), Linux ES 4 (AMD64 & Intel EM64T), Linux 5 (x86), Linux 5 Advanced Platform (x86), Linux 5 (AMD/Intel 64), Linux 5 Advanced Platform (AMD/Intel 64))

P-9V2C-AJ92 Job Management Partner 1/Performance Management - Base version 09-00 (for Linux AS 4 (IPF), Linux 5 (IPF), Linux 5 Advanced Platform (IPF))

P-242C-AR97 Job Management Partner 1/Performance Management - Web Console version 09-00 (for Windows Server 2003)

P-2A2C-AR97 Job Management Partner 1/Performance Management - Web Console version 09-00 (for Windows Server 2008)

P-9S2C-AR92 Job Management Partner 1/Performance Management - Web Console version 09-00 (for Linux 5 (x86), Linux 5 Advanced Platform (x86), Linux 5 (AMD/Intel 64), Linux 5 Advanced Platform (AMD/Intel 64))

In addition to the above products, this product is targeted at the PFM - Agent and PFM - RM products of Job Management Partner 1/Performance Management, which require Job Management Partner 1/Performance Management - Base. Also, these products include parts that were developed under licenses received from third parties.

■ Trademarks

■ Restrictions

■ Microsoft product screen shots

■ Edition history

Edition 1 (3020-3-R32(E)): November 2009

■ Copyright

Preface

This manual describes methods of operating JP1/Performance Management, how to manage a system when linking with other systems, and troubleshooting. In this manual, *Job Management Partner 1* is abbreviated to *JP1*.

Intended readers

This manual is intended for readers with an interest in operating a system that uses JP1/Performance Management. It also assumes that the reader is familiar with the system being monitored.

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

Organization of this manual

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

PART 1: Operation

PART 1 describes how to operate JP1/Performance Management.

PART 2: System Linkage

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

PART 3: Troubleshooting

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

Related publications

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

For Job Management Partner 1/Performance Management:

- *Job Management Partner 1/Performance Management Planning and Configuration Guide* (3020-3-R31(E))
- *Job Management Partner 1/Performance Management Reference*

(3020-3-R33(E))

- *Job Management Partner 1/Performance Management - Remote Monitor for Platform Description, User's Guide and Reference* (3020-3-R39(E))
- *Job Management Partner 1/Performance Management - Remote Monitor for Oracle Description, User's Guide and Reference* (3020-3-R40(E))
- *Job Management Partner 1/Performance Management - Remote Monitor for Microsoft(R) SQL Server Description, User's Guide and Reference* (3020-3-R41(E))
- *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* (3020-3-R48(E)), for Windows systems
- *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* (3020-3-R49(E)), for UNIX systems
- *Job Management Partner 1/Performance Management - Agent Option for Virtual Machine Description, User's Guide and Reference* (3020-3-R50(E))
- *Job Management Partner 1/Performance Management - Agent Option for Oracle Description, User's Guide and Reference* (3020-3-K67(E))
- *Job Management Partner 1/Performance Management - Agent Option for SQL Server Description, User's Guide and Reference* (3020-3-K69(E))
- *Job Management Partner 1/Performance Management - Agent Option for Job Management Description, User's Guide and Reference* (3020-3-K75(E))
- *Job Management Partner 1/Performance Management - Agent Option for Enterprise Applications Description, User's Guide and Reference* (3020-3-K66(E))

For Job Management Partner 1:

- *Job Management Partner 1/Base User's Guide* (3020-3-R71(E))
- *Job Management Partner 1/Integrated Management - Manager Quick Reference* (3020-3-R75(E))
- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* (3020-3-R76(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3020-3-R77(E))
- *Job Management Partner 1/Integrated Management - Manager Administration Guide* (3020-3-R78(E))
- *Job Management Partner 1/Integrated Management - Manager GUI Reference*

(3020-3-R79(E))

- *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference* (3020-3-R80(E))
- *Job Management Partner 1/Integrated Management - Manager Messages* (3020-3-R81(E))
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems
- *Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide* (3020-3-L42(E)), for UNIX systems
- *Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide* (3000-3-841(E))

Differences between versions

For JP1 Version 9 JP1/Performance Management, the manual contents of the old edition JP1 Version 8 *Job Management Partner 1/Performance Management System Configuration and User's Guide* (3020-3-K61-40(E)) have now been divided into the following two manuals.

- *Job Management Partner 1/Performance Management Planning and Configuration Guide* (3020-3-R31(E))
- *Job Management Partner 1/Performance Management User's Guide* (3020-3-R32(E))

The following table describes the correspondence between the Version 8 JP1 manual (*Job Management Partner 1/Performance Management System Configuration and User's Guide* (3020-3-K61-40(E))) and this manual (*Job Management Partner 1/ Performance Management User's Guide* (3020-3-R32(E))):

JP1 Version 8 ***Job Management Partner 1/ Performance Management System Configuration and User's Guide*** **(3020-3-K61-40(E))**	**JP1 Version 9** ***Job Management Partner 1/ Performance Management User's Guide*** **(3020-3-R32(E))**
PART 1: Overview	Moved to the *Job Management Partner 1/ Performance Management Planning and Configuration Guide* (3020-3-R31(E)).
1. Overview of Performance Management	
2. Using Performance Management	
PART 2: Design	
3. Design of Operation Monitoring Systems that Use Performance Management	
4. Performance Management Functions	
PART 3: Configuration	
5. Installation and Setup (in Windows)	
6. Installation and Setup (in UNIX)	
PART 4: Operation	PART 1: Operation
7. Starting and Stopping Performance Management	1. Starting and Stopping Performance Management
8. Managing User Accounts	2. Managing User Accounts
9. Monitoring Agents	3. Monitoring Agents
10. Managing Operation Monitoring Data	4. Managing Operation Monitoring Data
11. Creation of Reports for Operation Analysis	5. Creation of Reports for Operation Analysis
12 Operation Monitoring with Alarms	6. Operation Monitoring with Alarms
13. Displaying Events	7. Displaying Events
14. Backing Up and Restoring Data	8. Backing Up and Restoring Data
PART 5: System Linkage	PART 2: System Linkage
15. Construction and Operation with a Cluster System	9. Construction and Operation with a Cluster System
16. Operation Monitoring Linked with the Integrated Management Product JP1/IM	10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring
17. Linking with Network Node Manager (NNM) for Operation Monitoring	11. Linking with Network Node Manager (NNM) for Operation Monitoring
18. Linking with ODBC-Complaint Application Programs for Operation Analysis	12. Linking with ODBC-Compliant Application Programs for Operation Analysis

JP1 Version 8 ***Job Management Partner 1/ Performance Management System Configuration and User's Guide*** **(3020-3-K61-40(E))**	**JP1 Version 9** ***Job Management Partner 1/ Performance Management User's Guide*** **(3020-3-R32(E))**
PART 6: Troubleshooting	PART 3: Troubleshooting
19. Detecting Problems within Performance Management	13. Detecting Problems within Performance Management
20. Error Handling Procedures	14. Error Handling Procedures
Appendix A. Limits	Moved to the *Job Management Partner 1/ Performance Management Planning and Configuration Guide* (3020-3-R31(E)).
Appendix B. Naming Rules	
Appendix C. System Estimates	
Appendix D. Kernel Parameter List	
Appendix E. Migration Steps and Notes on Migration	
Appendix F. Version Compatibility	
Appendix G. Outputting Action Log Data	
Appendix H. Health Check Agent	
Appendix I. Version Changes	Appendix A. Version Changes
Appendix J. Glossary	Appendix B. Glossary

Conventions: Abbreviations

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
AIX	AIX 5L V5.3
	AIX V6.1
HP-UX	HP-UX 11i V2 (IPF)
	HP-UX 11i V3 (IPF)
Internet Explorer	Microsoft(R) Internet Explorer(R)
	Windows(R) Internet Explorer(R)
IPF	Itanium(R) Processor Family

Abbreviation			Full name or meaning
JP1/IM	JP1/IM - Manager		Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View		Job Management Partner 1/Integrated Management - View
JP1/NETM/DM			Job Management Partner 1/NETM/DM Client
			Job Management Partner 1/NETM/DM Manager
			Job Management Partner 1/NETM/DM SubManager
Linux	Linux (IPF)	Linux 5 Advanced Platform (IPF)	Red Hat Enterprise Linux(R) 5 Advanced Platform (IPF)
		Linux 5 (IPF)	Red Hat Enterprise Linux(R) 5 (IPF)
		Linux AS 4 (IPF)	Red Hat Enterprise Linux(R) AS 4 (IPF)
	Linux (x64)	Linux 5 Advanced Platform (AMD/Intel 64)	Red Hat Enterprise Linux(R) 5 Advanced Platform (AMD/Intel 64)
		Linux 5 (AMD/Intel 64)	Red Hat Enterprise Linux(R) 5 (AMD/Intel 64)
		Linux AS 4 (AMD64 & Intel EM64T)	Red Hat Enterprise Linux(R) AS 4 (AMD64 & Intel EM64T)
		Linux ES 4 (AMD64 & Intel EM64T)	Red Hat Enterprise Linux(R) ES 4 (AMD64 & Intel EM64T)
	Linux (x86)	Linux 5 Advanced Platform (x86)	Red Hat Enterprise Linux(R) 5 Advanced Platform (x86)

Abbreviation			Full name or meaning
		Linux 5 (x86)	Red Hat Enterprise Linux(R) 5 (x86)
		Linux AS 4 (x86)	Red Hat Enterprise Linux(R) AS 4 (x86)
		Linux ES 4 (x86)	Red Hat Enterprise Linux(R) ES 4 (x86)
MSCS			Microsoft(R) Cluster Service
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		Job Management Partner 1/Performance Management - Agent Option for Enterprise Applications
	PFM - Agent for Job Management		Job Management Partner 1/Performance Management - Agent Option for Job Management
	PFM - Agent for Microsoft SQL Server		Job Management Partner 1/Performance Management - Agent Option for Microsoft(R) SQL Server
	PFM - Agent for Oracle		Job Management Partner 1/Performance Management - Agent Option for Oracle

Abbreviation			Full name or meaning
	PFM - Agent for Platform	PFM - Agent for Platform (UNIX)	Job Management Partner 1/Performance Management - Agent Option for Platform (for UNIX systems)
		PFM - Agent for Platform (Windows)	Job Management Partner 1/Performance Management - Agent Option for Platform (for Windows systems)
	PFM - Agent for Service Response		Job Management Partner 1/Performance Management - Agent Option for Service Response
	PFM - Agent for Virtual Machine		Job Management Partner 1/Performance Management - Agent Option for Virtual Machine
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		Job Management Partner 1/Performance Management - Remote Monitor for Microsoft(R) SQL Server
	PFM - RM for Oracle		Job Management Partner 1/Performance Management - Remote Monitor for Oracle
	PFM - RM for Platform		Job Management Partner 1/Performance Management - Remote Monitor for Platform

Abbreviation		Full name or meaning
PFM - Web Console		Job Management Partner 1/Performance Management - Web Console
Solaris	Solaris 9	Solaris 9 (SPARC)
	Solaris 10	Solaris 10 (SPARC)
		Solaris 10 (x64)
		Solaris 10 (x86)
Windows Server 2003	Windows Server 2003 (x64) or 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) or 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
Windows Server 2008	Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 Enterprise

Abbreviation		Full name or meaning
		Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM)
	Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 Standard
		Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM)
WSFC		Windows Server(R) Failover Cluster

- PFM - Manager, PFM - Agent, PFM - Base, PFM - Web Console, and PFM - RM are sometimes referred to as *Performance Management*.
- Windows Server 2003 and Windows Server 2008 are sometimes referred to as *Windows*.
- HP-UX, Solaris, AIX, and Linux are sometimes referred to as *UNIX*.

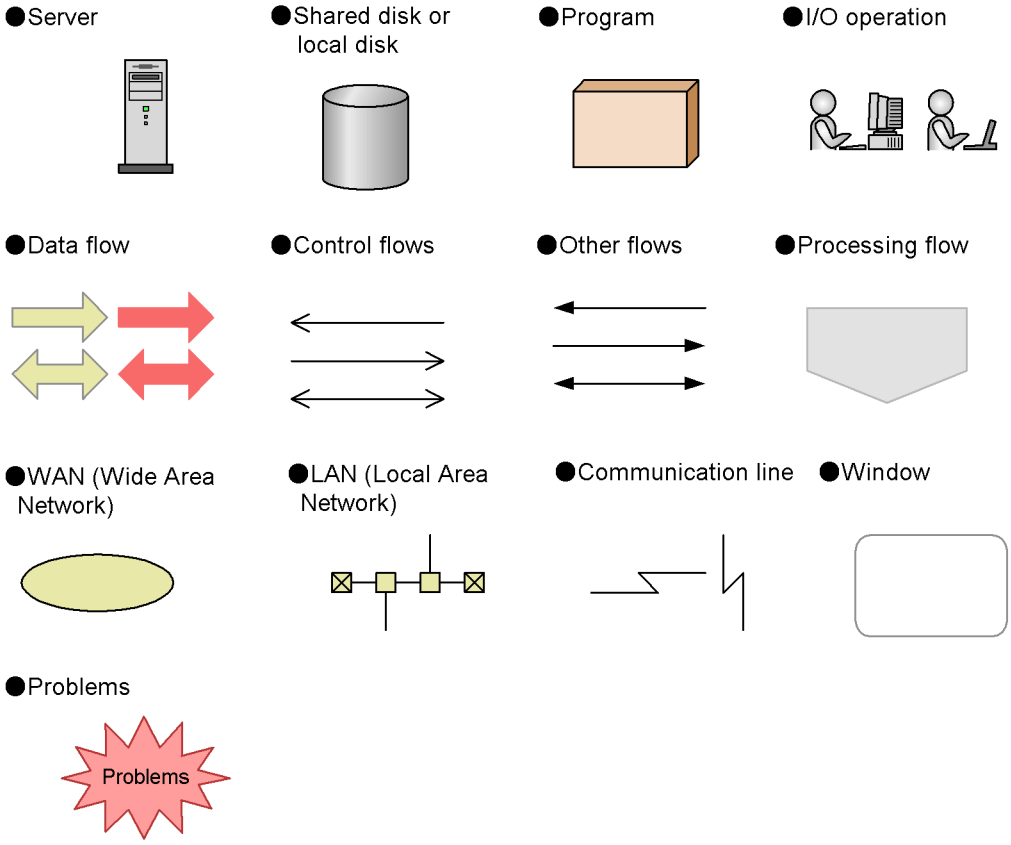
This manual also uses the following abbreviations:

Abbreviation	Full name
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	DataBase
DDE	Dynamic Data Exchange
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network

Abbreviation	Full name
MIB	Management Information Base
NAT	Network Address Translation
NFS	Network File System
ODBC	Open DataBase Connectivity
OS	Operating System
PQL	Program Query Language
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UAC	User Account Control
URL	Uniform Resource Locator
XML	eXtensible Markup Language

Conventions: Diagrams

This manual uses the following conventions in diagrams:



Conventions: Fonts and symbols

Font and symbol conventions are classified as:

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

These conventions are described below.

General font conventions

The following table lists the general font conventions:

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

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

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

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

Conventions in syntax explanations

Syntax definitions appear as follows:

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

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
`StoreDatabase`	Code-font characters must be entered exactly as shown.
database-name	This font style marks a placeholder that indicates where appropriate characters are to be entered in an actual command.
SD	Bold code-font characters indicate the abbreviation for a command.
perm	Underlined characters indicate the default value.
[ ]	Square brackets enclose an item or set of items whose specification is optional.

Example font or symbol	Convention
| (vertical bar)	A vertical bar separates items in a list, and means "OR". For example, `A|B|C` means one of `A` or `B` or `C`.
. . .	An ellipsis (...) indicates that the item or items enclosed in ( ) or [ ] immediately preceding the ellipsis may be specified as many times as necessary.
`()`	Parentheses indicate the range of items to which the vertical bar (|) or ellipsis (...) is applicable.
`{}`	Curly brackets enclose a list of items, and indicate that one (and only one) of the items in the list must be used. A vertical bar (|) separates the items in the list. For example, `{A|B|C}` means that one of `A` or `B` or `C` must be used.

Conventions for mathematical expressions

This manual uses the following symbols in mathematical expressions:

Symbol	Meaning
x	Multiplication sign
/	Division sign

Conventions: Format of product names, service IDs, and service keys in this manual

In Performance Management of version 09-00 or later, enabling the product name display functionality allows the service IDs and service keys to be displayed as the product name. The following table lists the displayed examples of service IDs and service keys for PFM - Agent for Platform (Windows) when the product name display functionality is enabled.

Identifier	Product name display functionality	
	Disabled	Enabled
Service ID	TS1 *host-name*	*host-name*<Windows>(Store)
	TA1 *host-name*	*host-name*<Windows>
Service key	agtt	Windows

This manual generally uses the format when the product name display functionality is assumed to be enabled.

Note that the product name display functionality can be enabled when the following conditions are satisfied:

- The version of PFM - Agent or the prerequisite program (PFM - Manager or PFM - Base) within the same device of PFM -RM is 09-00 or later.
- The version of PFM - Web Console or the connected PFM - Manager is 09-00 or later.

Conventions: KB, MB, GB and TB

This manual uses the following conventions:

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

Conventions: Meaning of "bookmark"

In this manual, *bookmark* is generally used when there is no need to distinguish *bookmark* and *combination bookmark*. *Combination bookmark* is used only for describing original functionalities of combination bookmarks.

Conventions: Meaning of "directory" and "folder"

This manual uses the term *directory* wherever possible to refer to what Windows calls a *folder* and what UNIX calls a *directory*.

Conventions: Meaning of Performance Management "installation directory"

This manual uses the expression *installation folder* for Windows Performance Management, and *installation directory* for UNIX Performance Management.

The default installation folder for Windows Performance Management is as follows:

Performance Management installation folder except for PFM - Web Console:

- For programs other than Windows Server 2003 (x64) and Windows Server 2008 (64 bit)

    system-drive`:\Program Files\Hitachi\jp1pc\`

- For Windows Server 2003 (x64) and Windows Server 2008 (64 bit)

    system-drive`:\Program Files (x86)\Hitachi\jp1pc\`

PFM - Web Console installation folder:

- For programs other than Windows Server 2003 (x64) and Windows Server 2008 (64 bit)

    system-drive`:\Program Files\Hitachi\jp1pcWebCon\`

- For Windows Server 2003 (x64) and Windows Server 2008 (64 bit)

system-drive:\Program Files (x86)\Hitachi\jp1pcWebCon\

The default installation directory for UNIX Performance Management is as follows:

Performance Management installation directory except for PFM - Web Console:

/opt/jp1pc/

PFM - Web Console installation directory:

/opt/jp1pcwebcon/

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.

Proper use of JP1/Performance Management manuals

Manuals for JP1/Performance Management are divided into following manuals. Check the description below and refer to the appropriate manual depending on your purpose.

Manual name	Description
Job Management Partner 1/Performance Management Planning and Configuration Guide	Functionalities, and set up or configuration method
Job Management Partner 1/Performance Management User's Guide	Operation method
Job Management Partner 1/Performance Management Reference	Windows, commands, and messages

NNM products supported by Performance Management

Performance Management supports the linkage with the following products:

- HP Network Node Manager Software version 6 or earlier
- HP Network Node Manager Starter Edition Software version 7.5 or earlier

This manual generally uses *NNM* to indicate the above products, and *NNM linkage* for functionalities for linking with these products.

Note that Performance Management does not support the linkage with the following product:

- HP Network Node Manager i Software v8.10

Contents

Preface i

Intended readers i
Organization of this manual i
Related publications i
Differences between versions.... iii
Conventions: Abbreviations v
Conventions: Diagrams xi
Conventions: Fonts and symbols....xii
Conventions: Format of product names, service IDs, and service keys in this manual xiv
Conventions: KB, MB, GB and TB xv
Conventions: Meaning of "bookmark"....xv
Conventions: Meaning of "directory" and "folder"....xv
Conventions: Meaning of Performance Management "installation directory" xv
Conventions: Version numbers....xvi
Proper use of JP1/Performance Management manuals xvi
NNM products supported by Performance Management....xvi

PART 1: Operation

1. Starting and Stopping Performance Management 1

1.1 Start and stop sequence for the entire Performance Management system 2
1.1.1 Start sequence for the entire Performance Management system....2
1.1.2 Stop sequence for the entire Performance Management system....5
1.2 Starting services....7
1.2.1 Starting services on the monitoring manager or the monitoring agent 7
1.2.2 Starting services on the monitoring console server....11
1.3 Stopping services....15
1.3.1 Stopping monitoring manager and monitoring agent services....15
1.3.2 Stopping monitoring console server services....19
1.4 Synchronizing the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console 22
1.4.1 Configuration for synchronizing service starting and stopping 22
1.4.2 Procedure for synchronizing service starting and stopping 23
1.5 Logging on to and off from PFM - Web Console....24
1.5.1 Logging on to PFM - Web Console....24
1.5.2 Logging off from PFM - Web Console 26

1.6 Checking the status of service operations 28
1.6.1 Checking the operating status of services by using a command 28
1.6.2 Checking the operating status of services on the browser 31
1.7 Specifying automatic refresh intervals for the browser 32
1.8 Notes 33
1.8.1 When starting PFM - Agent or PFM - RM in a large-scale system 33
1.8.2 Starting a PFM - Agent or PFM - RM service during command execution 40
1.8.3 Starting on a Windows machine 40
1.8.4 Starting the Status Server service 41
1.8.5 Monitoring alarm events 43
1.8.6 Executing actions 43

2. Managing User Accounts 45

2.1 User account authentication and permissions 46
2.2 Setting the user account authentication mode 58
2.3 Creating a Performance Management user account 60
2.3.1 Creating a new Performance Management user account 60
2.3.2 Copying and customizing an existing user account 62
2.4 Editing a Performance Management user account 64
2.4.1 Changing the password 64
2.4.2 Changing the permissions of a Performance Management user account 66
2.4.3 Deleting a Performance Management user account 67

3. Monitoring Agents 69

3.1 Monitoring by using the Agents tree 70
3.1.1 Agent types 72
3.2 Creating an Agents tree 73
3.2.1 Creating a new agent management folder 73
3.2.2 Placing agents in a management folder 74
3.2.3 Editing an Agents tree used for monitoring 76
3.3 Monitoring the status of agent operations 81
3.3.1 Checking the status of agents 81
3.3.2 Checking the status of alarms 84
3.3.3 Displaying reports 86
3.3.4 Displaying event history 86
3.3.5 Using summary display to check the operating status 87
3.3.6 Displaying agent properties 98
3.3.7 Editing agent properties 100
3.3.8 Distributing agent properties as a batch 100

4. Managing Operation Monitoring Data 115

4.1 Managing performance data 116
4.1.1 Modifying the recording options for performance data 116
4.1.2 Modifying the retention conditions for performance data (in Store 2.0) 130

4.1.3 Modifying the retention conditions for performance data (in Store 1.0) 140
4.1.4 Exporting performance data 152
4.1.5 Checking the disk space used for performance data 153
4.1.6 Erasing performance data 155
4.1.7 Initializing the settings for the Store database 155
4.1.8 Importing backup data (with Store 2.0) 158
4.1.9 Converting the data model of backup data (with Store 2.0) 159
4.1.10 Displaying information about the Agent Store and Remote Monitor Store services or backup directory (in Store 2.0) 160
4.2 Managing event data 162
4.2.1 Changing the maximum number of records for event data 162
4.2.2 Exporting event data 163
4.2.3 Checking the disk space used for event data 164
4.2.4 Erasing event data 165
4.3 Notes 167
4.3.1 Size limit of the Store database 167
4.3.2 When the Agent Store or Remote Monitor Store service stopped abnormally 168
4.3.3 When the disk capacity is insufficient 168
4.3.4 Checking the size of, and reorganizing, the Store database 173
4.3.5 When files or folders are not deleted after their retention period expires 174
4.3.6 The default retention period of records in Store 2.0 175
4.3.7 Performance data stored after a data model upgrade 176

5. Creation of Reports for Operation Analysis 179

5.1 Overview of reports 180
5.1.1 About reports 180
5.1.2 Report types 180
5.1.3 Display formats of reports 181
5.2 Process flow for creating a report 184
5.3 Creating reports by using a browser 187
5.3.1 Creating a report folder 187
5.3.2 Displaying the New Report window 188
5.3.3 Setting the name and type of a report 188
5.3.4 Setting fields displayed in a report 190
5.3.5 Setting display conditions for fields displayed in a report (filter condition) 193
5.3.6 Setting the display information for a report (refresh interval and display period) 195
5.3.7 Setting the display format (table, list, or graph) of a report 198
5.3.8 Associating a report with another report (drilldown report) 201
5.3.9 Copying a report 205
5.3.10 Editing a report 205
5.3.11 Renaming a folder or report 207

5.3.12 Deleting a folder or report ... 209
5.3.13 Exporting reports ... 210
5.3.14 Importing a report ... 210
5.4 Creating reports by using the Quick Guide ... 212
5.4.1 Procedure for creating reports by using the Quick Guide ... 212
5.4.2 Searching fields ... 214
5.4.3 Default values used for reports created with the Quick Guide ... 215
5.5 Creating reports by using commands ... 217
5.5.1 Outputting and customizing report definitions ... 217
5.5.2 Deleting an unnecessary report ... 218
5.6 Creating and editing bookmarks by using a browser ... 220
5.6.1 Creating bookmarks ... 220
5.6.2 Adding a bookmark folder ... 224
5.6.3 Renaming folders and bookmarks ... 225
5.6.4 Deleting folders, bookmarks, and reports ... 227
5.6.5 Checking the properties of a bookmark ... 228
5.6.6 Tiling display of reports registered in bookmarks ... 229
5.7 Displaying reports ... 235
5.7.1 Displaying reports ... 235
5.7.2 Checking the report properties (definition) ... 240
5.7.3 Setting the display conditions for a report ... 240
5.7.4 Displaying a drilldown report ... 243
5.8 Displaying combination reports ... 247
5.8.1 Preparing to display combination reports ... 250
5.8.2 Displaying combination reports ... 253
5.8.3 Checking the properties (definitions) of combination bookmarks ... 254
5.8.4 Examples of using combination reports in real-world situations ... 254
5.9 Outputting reports ... 262
5.9.1 Exporting reports in CSV or HTML format by using a browser ... 262
5.9.2 Exporting reports in CSV or HTML format by using a command ... 263
5.9.3 CSV format ... 264
5.9.4 HTML format ... 265
5.10 Notes on reports ... 269
5.10.1 Notes on creating reports ... 269
5.10.2 Notes on displaying reports ... 269
5.10.3 Notes on combination reports ... 271

6. Monitoring Operations with Alarms 277

6.1 Overview of alarms ... 278
6.2 Process of setting up and operating alarms ... 279
6.3 Procedures before setting alarms ... 282
6.4 Setting alarms by using the browser ... 287
6.4.1 Creating an alarm table ... 287
6.4.2 Creating an alarm (setting the basic information) ... 288

6.4.3 Setting a value whose existence is to be monitored 291
6.4.4 Setting the alarm conditions 292
6.4.5 Setting the actions 294
6.4.6 Associating a report with an alarm 301
6.4.7 Copying an alarm table or alarm 302
6.4.8 Editing an alarm 304
6.4.9 Deleting an alarm table or alarm 305
6.4.10 Exporting alarm tables 306
6.4.11 Importing alarm tables 307
6.5 Setting alarms by using the Quick Guide 309
6.5.1 Procedure for creating alarms by using the Quick Guide 309
6.5.2 The default values of an alarm created by using the Quick Guide 312
6.6 Operating alarms by using the browser 314
6.6.1 Changing the association between an alarm table and a monitoring agent 314
6.6.2 Displaying the monitoring agents bound to an alarm table 318
6.6.3 Stopping monitoring with an alarm 319
6.6.4 Starting monitoring with an alarm 319
6.6.5 Displaying alarm properties (definitions) 320
6.7 Setting alarms by using commands 324
6.7.1 Creating an alarm definition file 324
6.7.2 Checking the alarm definition file 337
6.7.3 Modifying an alarm definition 338
6.7.4 Copying an alarm table 340
6.7.5 Deleting an alarm table 342
6.7.6 Deleting an alarm 343
6.8 Operating alarms by using commands 346
6.8.1 Associating an alarm table with a monitoring agent 346
6.8.2 Unbinding an alarm table bound to a monitoring agent 350
6.8.3 Checking the connection between an alarm table and a monitoring agent 354
6.8.4 Starting monitoring with an alarm 355
6.8.5 Stopping monitoring with an alarm 357
6.8.6 Checking the properties of an alarm table 359
6.9 Notes on alarms 362
6.9.1 Notes on creating alarms 362
6.9.2 Relationship between the alarm damping and alarm event issues 363
6.9.3 Notes on evaluating alarms 378

7. Displaying Events 385

7.1 Displaying the latest events 386
7.1.1 Displaying the latest events information 386
7.1.2 Displaying a report associated with an alarm 393
7.1.3 Displaying alarm properties 393
7.1.4 Setting the display conditions for the Event Monitor window 395
7.2 Displaying the event history 397

7.2.1 Displaying the event history 397
7.3 Outputting the event history 404
7.3.1 Outputting the event history in CSV format 404
7.3.2 Outputting the event history in HTML format 404

8. Backing Up and Restoring Data 407

8.1 Overview of backing up and restoring data 408
8.1.1 Data backup methods 408
8.1.2 Information that needs to be backed up 408
8.2 Overview of partial backups 409
8.3 Backing up and restoring definition information 413
8.3.1 Backing up and restoring report definition information 414
8.3.2 Backing up and restoring alarm definition information 415
8.3.3 Backing up and restoring service definition information 415
8.3.4 Backing up and restoring bookmark definition information 438
8.4 Backing up and restoring operation-monitoring data 446
8.4.1 Backing up and restoring the event data 448
8.4.2 Backing up and restoring the performance data 451
8.4.3 Partially backing up performance data (Store 2.0) 454

PART 2: System Linkage

9. Cluster System Configuration and Operation 459

9.1 Overview and design of cluster systems 460
9.1.1 Overview of cluster systems 460
9.1.2 Designing a cluster configuration 463
9.1.3 Designing the network configuration 470
9.1.4 Designing the data configuration 472
9.1.5 Operation design in cluster systems 473
9.1.6 Designing the failover policy 473
9.2 Configuration of a cluster system (in Windows) 474
9.2.1 Before installation and setup 474
9.2.2 Installing and setting up PFM - Manager 476
9.2.3 Installing and setting up PFM - Web Console 490
9.2.4 Installing an upgrade for PFM - Agent or PFM - RM 499
9.2.5 Unsetup and uninstallation of PFM - Manager 499
9.2.6 Unsetup and uninstallation of PFM - Web Console 507
9.3 Changing the cluster system configuration (in Windows) 510
9.3.1 Adding PFM - Agent or PFM - RM 510
9.3.2 Deleting PFM - Agent or PFM - RM 515
9.3.3 Changing logical host names after starting operation 517
9.4 Configuration of a cluster system (in UNIX) 531
9.4.1 Before installation and setup 531

9.4.2 Installing and setting up PFM - Manager 533
9.4.3 Installing and setting up PFM - Web Console 547
9.4.4 Installing an upgrade for PFM - Agent or PFM - RM 556
9.4.5 Unsetup and uninstallation of PFM - Manager 556
9.4.6 Unsetup and uninstallation of PFM - Web Console 564
9.5 Changing the cluster system configuration (in UNIX) 567
9.5.1 Adding PFM - Agent or PFM - RM 567
9.5.2 Deleting PFM - Agent or PFM - RM 573
9.5.3 Changing logical host names after starting operation 574
9.6 Cluster system operations 589
9.6.1 Starting and stopping Performance Management in a cluster system 589
9.6.2 Managing user accounts in a cluster system 593
9.6.3 Managing agents in an integrated manner in a cluster system 594
9.6.4 Collecting and managing the operation management data in a cluster system 595
9.6.5 Creating operation management reports in a cluster system 595
9.6.6 Performing realtime operation monitoring by alarms in a cluster system 596
9.6.7 Performing backup and restore in a cluster system 596
9.6.8 Performing the required operation when a failover occurs in a cluster system 597
9.7 Failure recovery in a cluster system 603
9.8 Notes on cluster systems 605

10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring 607

10.1 Overview of linking with the integrated management product JP1/IM for operation monitoring 608
10.1.1 Monitoring by using integrated console 610
10.1.2 Monitoring by using integrated scope 610
10.1.3 Linkage of Performance Management and JP1/IM 611
10.2 Considerations for linking with JP1/IM 612
10.2.1 JP1 event types 612
10.2.2 Prerequisite conditions for issuing JP1 events 613
10.3 Setting up the linkage with JP1/IM 614
10.3.1 Installation 614
10.3.2 Setup 615
10.3.3 Unsetup 630
10.4 Operating the linkage with JP1/IM 631
10.4.1 Procedure for alarm event monitoring via the JP1/IM integrated console 631
10.4.2 Procedure for monitoring via the integrated scope of JP1/IM 631
10.4.3 Displaying a report from the integrated console of JP1/IM 631
10.4.4 Procedure for starting PFM - Web Console from the JP1/IM integrated management menu 631
10.5 List of JP1 event attributes 633

11. Linking with Network Node Manager (NNM) for Operation Monitoring 643

11.1 Overview of linking with Network Node Manager (NNM) for operation monitoring ... 644
11.2 Constructing the linkage with NNM ... 647
11.2.1 Supported OSs for linking with NNM ... 647
11.2.2 Installation ... 648
11.2.3 Setup ... 649
11.2.4 Unsetup ... 656
11.2.5 Changing configuration ... 659
11.3 Operations for linkage with NNM ... 660
11.3.1 Starting and terminating the service of the OpenView linkage facility ... 660
11.3.2 Monitoring alarm events from NNM ... 660
11.4 Configuration of MIB objects ... 665

12. Linking with ODBC-Compliant Application Programs for Operation Analysis 669

12.1 Overview of linking with an ODBC-compliant operation analysis application program ... 670
12.2 Installation and setup ... 672
12.2.1 Supported OSs for linking with an ODBC-compliant application program ... 672
12.2.2 Installation ... 672
12.2.3 Setup ... 673
12.3 Example of using Microsoft Excel to extract performance data ... 677
12.4 Notes ... 680
12.4.1 Supported SQL functions ... 680
12.4.2 Supported expressions ... 681
12.4.3 Specification rules for the names of columns and tables ... 682
12.4.4 Specifying common key fields ... 684
12.4.5 Adjusting the time ... 685
12.4.6 Executing a query among multiple agents ... 685
12.4.7 Notes on using ODBC from Microsoft Excel ... 686

PART 3: Troubleshooting

13. Detecting Problems within Performance Management 687

13.1 Overview of detecting problems within Performance Management ... 688
13.2 Using the health check function to check the operating status of monitoring agents and their hosts ... 691
13.2.1 Configuring the health check function ... 691
13.2.2 Checking operating statuses ... 697
13.2.3 Examples of using the health check function ... 705
13.3 Using the status management function to check service status ... 711

13.3.1 Configuring the status management function....711
13.3.2 How to check the service status....714
13.3.3 Status management during cluster system operation....716
13.3.4 When a problem occurs within the status management function....718
13.4 Using the PFM service automatic restart functionality to restart PFM services....720
13.4.1 Prerequisite conditions....720
13.4.2 Service startup unit for the PFM service automatic restart functionality....721
13.4.3 Configuring the PFM service automatic restart functionality....722
13.4.4 Using the PFM service automatic restart functionality....726
13.5 Detecting problems by linking with the integrated system monitoring product....729
13.5.1 Configuring the log output method....729
13.5.2 Example of creating a definition file for the JP1/Base log file trapping function....731
13.5.3 Starting the JP1/Base log file trapping function....731

14. Error Handling Procedures 733

14.1 Error handling procedures....734
14.2 Troubleshooting....735
14.2.1 Setting up and starting a service....736
14.2.2 Connecting to agents....741
14.2.3 Logging on to PFM - Web Console....742
14.2.4 Executing commands....743
14.2.5 Agent management....744
14.2.6 Report definition....746
14.2.7 Alarm definition....749
14.2.8 Collecting and managing performance data....750
14.2.9 Linking with other programs....751
14.2.10 Other problems....753
14.3 Log information....754
14.3.1 Type of log information....754
14.3.2 Log information files....755
14.4 Data to be collected in the event of trouble....765
14.4.1 Data to be collected in the event of an error (in Windows)....765
14.4.2 Data to be collected in the event of an error (in UNIX)....772
14.5 Data collection procedure....778
14.5.1 Data collection procedure (in Windows)....778
14.5.2 Data collection procedure (in UNIX)....782
14.5.3 Data collection procedure (in PFM - Web Console)....785
14.6 Restoring the Performance Management system....786
14.6.1 Restore procedure for an error related to changes in the configuration....787
14.6.2 Restore procedure for a serious error related to a disk failure....791

Appendixes 795

A. Version Changes....796

A.1 Changes in 09-00 796
A.2 Changes in 08-11 797
A.3 Changes in 08-00 798
A.4 Changes in 07-10 799
A.5 Changes in 07-00 799
B. Glossary 800

Index 811

Chapter

1. Starting and Stopping Performance Management

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

1.1 Start and stop sequence for the entire Performance Management system
1.2 Starting services
1.3 Stopping services
1.4 Synchronizing the starting and stopping of PFM - Manager or PFM - Base and PFM - Web Console
1.5 Logging on to and off from PFM - Web Console
1.6 Checking the status of service operations
1.7 Specifying automatic refresh intervals for the browser
1.8 Notes

1.1 Start and stop sequence for the entire Performance Management system

This section describes the start and stop sequence for the entire Performance Management system.

Note:

The sequence for starting and stopping of Performance Management in a cluster system is different from the ordinary sequence. For details, see sections that describe the setup of each Performance Management program in *9. Cluster System Configuration and Operation*.

1.1.1 Start sequence for the entire Performance Management system

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

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

To start the entire Performance Management system:

1. Start PFM - Manager on the monitoring manager.

   Execute the `jpcspm start` command on the monitoring manager to start the following PFM - Manager services:

   - Status Server
   - Name Server
   - Master Manager
   - Master Store
   - Correlator
   - Trap Generator
   - View Server
   - Agent Store (health check agent)#
   - Agent Collector (health check agent)#
   - Action Handler

Start these services only when using the health check function.

2. Start PFM - Base and either PFM - Agent or PFM - RM in all monitoring agents.

   Execute the `jpcspm start` command on all monitoring agents to start the following services of PFM - Base and either PFM - Agent or PFM - RM:

   - Status Server[#1]
   - Action Handler[#1]
   - Agent Collector and Agent Store[#2]
   - Remote Monitor Collector and Remote Monitor Store[#3]

   #1: PFM - Base services

   #2: PFM - Agent services

   #3: PFM - RM services

   You do not need to be concerned about distinguishing between the PFM - Base and PFM - Agent services or between PFM - Base and PFM - RM services when executing the `jpcspm start` command.

3. Start PFM - Web Console on the monitoring console server.

   Execute the `jpcwstart` command on the monitoring console server to start the following PFM - Web Console services:

   - Web Console
   - Web Service

The services for each Performance Management program are started in sequence by the `jpcspm start` command or the `jpcwstart` command. Service dependencies have been pre-set in Windows. Therefore, you do not need to be concerned with the starting sequence when starting services.

Reference note:

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

Notes:

- When you install version 08-00 or later of a Performance Management program, the setting for the status management function is as follows:
  - After a new installation of version 08-00 or later of PFM - Manager or PFM - Base on a host that does not already have a Performance Management program installed:

Status management function setting: Enabled

- Other cases[#]:

  Status management function setting: Remains the same

The following fall under the other cases category:

- Upgrading version 06-70 to 07-10 of PFM - Manager to version 08-00 or later
- Performing a new installation of version 08-00 or later of PFM - Manager or PFM - Base in an environment where version 06-70 to 07-00 of PFM - Agent is installed

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

For the procedure to change the settings of the status management function, see *13.3.1 Configuring the status management function*.

- If the Agent Collector or Remote Monitor Collector service fails to start, stop the PFM - Agent or PFM - RM services, and check the common message log to identify the cause of the start failure. Restart the PFM - Agent or PFM - RM services after solving the cause of the Agent Collector or Remote Monitor Collector start failure.
- You can use the health check function with PFM - Manager 08-11 or later. Depending on the PFM - Manager version and your installation environment, the settings of the health check function are as follows:
  - After a new installation of version 09-00 or later of PFM - Manager in an environment that does not already have a Performance Management program installed:

    Health check function setting: Enabled
  - After a new installation of version 09-00 or later of PFM - Manager in an environment that already has a Performance Management program installed:

    Health check function setting: Disabled
  - After a new installation of version 08-11 to 08-50 of PFM - Manager:

    Health check function setting: Disabled
  - After upgrading version 06-70 to 08-10 of PFM - Manager to version 08-11 or later:

    Health check function setting: Disabled
  - After upgrading version 08-11 or later of PFM - Manager:

Health check function setting: Setting prior to upgrading is used.

Because 06-70 to 08-10 versions of PFM - Manager do not have the health check function, the setting status in this case becomes *invalid*. For details on configuring the health check function, see *13.2.1 Configuring the health check function*.

1.1.2 Stop sequence for the entire Performance Management system

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

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

To stop the entire Performance Management system:

1. Stop PFM - Web Console on the monitoring console server.

   Execute the `jpcwstop` command on the monitoring console server to stop the following PFM - Web Console services:

   - Web Console
   - Web Service

2. Stop PFM - Base and either PFM - Agent or PFM - RM in all monitoring agents.

   Execute the `jpcspm stop` command on all monitoring agents to stop the following services of PFM - Base and either PFM - Agent or PFM - RM:

   - Status Server[#1]
   - Action Handler[#1]
   - Agent Collector and Agent Store[#2]
   - Remote Monitor Collector and Remote Monitor Store[#3]

   #1: PFM - Base service

   #2: PFM - Agent service

   #3: PFM - RM services

3. Stop PFM - Manager on the monitoring manager.

   Execute the `jpcspm stop` command on the monitoring manager to stop the following PFM - Manager services:

- Action Handler
- Agent Collector (health check agent)#
- Agent Store (health check agent)#
- View Server
- Trap Generator
- Correlator
- Master Store
- Master Manager
- Name Server
- Status Server

Start these services only when using the health check function.

The services for each Performance Management program are stopped in sequence by the `jpcspm stop` command or the `jpcwstop` command. Service dependencies have been pre-set in Windows. Therefore, you do not need to be concerned with the stopping sequence when stopping services.

Reference note:

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

Point:

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

1.2 Starting services

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

Notes:

The following OS user permissions are necessary to start services:

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

1.2.1 Starting services on the monitoring manager or the monitoring agent

This subsection describes how to start the monitoring manager and monitoring agent services.

(1) Starting services manually

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

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

To manually start services:

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

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

2. Execute the `jpcspm start` command.

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

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

   For details on the service keys used to start specific PFM - Agent or PFM - RM services on the host, see the appendix describing service naming rules in the manual *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

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

```
jpcspm start -key jp1pc
```

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

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

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

(2) Starting services automatically

The following describes procedures for starting services automatically at system startup for each OS.

(a) In Windows

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

Notes:

- If services are set to start automatically, the Agent Store service or Remote Monitor Store service might take a longer time to start, and the Agent Collector service or the Remote Monitor Collector service might not start successfully.
- The service control manager might output the following message if it takes time to start services of the Performance Management programs when restarting the OS:

  Event ID: `7022`

  Type: `Error`

  Description: <*service-name*> `service hung on starting.`

  In this case, check if a service start message has been output in the common message log. The service has started normally if a service start message has been output.
- Performance Management services are usually operated by using the system account. Changing the settings might cause service operation errors. Do not modify the account settings of a service, unless this manual recommends that you change the settings of that service.

  The PFM - Base, PFM - Manager, and PFM - Web Console services are

operated by using the all system account.

For details on PFM - Agent, see each of the PFM - Agent manuals.

- During OS startup, a factor such as a heavy load might cause the automatic startup of the OS to time out, and Performance Management might fail to start. Therefore, use the `jpcspm start` command to start the Performance Management system, instead of setting the OS to automatically start services.

(b) In UNIX

To automatically start services at system startup, use the service automatic start script file for the Performance Management system. If you are using AIX, also use the automatic start script file for AIX.

Supplemental information:

- By using this script file, you can start services on the physical host only. You cannot start services on the logical host.
- If you want only specific services to start automatically, edit the following line in the script file:

Before:

```
nohup /opt/jp1pc/tools/jpcstart all -nochk 2> /dev/null
1> /dev/null &
```

After:

```
nohup /opt/jp1pc/tools/jpcstart act -nochk 2> /dev/null
1> /dev/null
```

```
nohup /opt/jp1pc/tools/jpcstart <service-key> -nochk 2> /
dev/null 1> /dev/null &
```

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

- To automatically start the PFM - Manager service, edit the following line in the script file:

Before:

```
nohup /opt/jp1pc/tools/jpcstart all -nochk 2> /dev/null
1> /dev/null &
```

After:

```
nohup /opt/jp1pc/tools/jpcstart mgr -nochk 2> /dev/null
1> /dev/null
```

```
nohup /opt/jp1pc/tools/jpcstart act -nochk 2> /dev/null
1> /dev/null
nohup /opt/jp1pc/tools/jpcstart <service-key> -nochk 2> /
dev/null 1> /dev/null &
```

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

To set automatic start of services:

1. Log on to the host that you want to set for the automatic start of services.

   Log on to the monitoring manager if you are going to operate the PFM - Manager services. Log on to the monitoring agent if you are going to operate the services of PFM-Base and either PFM - Agent or PFM - RM.

2. Execute the following command to move to the `/opt/jp1pc` directory:

   ```
   cd /opt/jp1pc
   ```

3. Set the service automatic start script file for the Performance Management system.

   The names of the `.model` file of the service automatic start script and the service automatic start script file are as follows:

   - Name of the `.model` file of the service automatic start script: `jpc_start.model`
   - Name of the service automatic start script file: `jpc_start`

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

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

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

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

   Names of the automatic start script file and settings file are as follows:

   - Name of the automatic start script file: `/etc/rc.jp1_pc`
   - Name of the settings file: `/etc/inittab`

To perform the registration:

1. Use the `mkitab` command to register the `/etc/rc.jp1_pc` file to the `/etc/inittab` settings file.

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

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

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

Registering the file by the `mkitab` command places the file to the bottommost line of the `/etc/inittab` settings file. If the program that is linked by execution of an action has already been registered to the `/etc/initta` settings file, it is recommended that you edit the `/etc/inittab` settings file to place the program after the bottommost line.

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

To cancel the registration at uninstallation:

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

```
rmitab jp1pc
```

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

```
lsitab jp1pc
```

1.2.2 Starting services on the monitoring console server

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

Note:

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

(1) Starting services manually

The following two methods can be used to start the PFM - Web Console services on

the monitoring console server. Note that the instructions for starting services from the Control Panel apply only to Windows systems.

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

The following describes each procedure.

(a) Starting by using a command

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

To start services by using a command:

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

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

   - In Windows:

     PFM-Web-Console-installation-folder`\tools`
   - In UNIX:

     `/opt/jp1pcwebcon/tools`

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

(b) Starting from the Control Panel

To start services from the Control Panel:

1. Log on to the monitoring console server (the host that has PFM - Web Console installed).
2. From the **Start** menu of Windows, choose **Settings**, **Control Panel**, **Administrative Tool**, and then **Services**.

   The Services dialog box appears.
3. Right-click the **PFM - Web Console** service, and from the pulldown menu choose **Start**.
4. Right-click the **PFM - Web Service** service, and from the pulldown menu choose **Start**.

(2) Starting services automatically

(a) In Windows

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

Reference note: How to cancel or reset the automatic start:

To cancel or reset the automatic start:

1. Log on to the monitoring console server (the host that has PFM - Web Console installed).
2. From the **Start** menu of Windows, choose **Settings**, **Control Panel**, **Administrative Tool**, and then **Services**.

   The Services dialog box appears.
3. Choose the **PFM - Web Console** service, and from the pulldown menu choose **Properties**.

   The Properties dialog box of the PFM - Web Console service appears.
4. Set the **startup type**.

   To cancel the automatic start, select **Manual**.

   To reset the automatic start, select **Automatic**.
5. Click the **OK** button.

   The Properties dialog box of the PFM - Web Console service is closed.
6. Choose the **PFM - Web Service** service, and from the pulldown menu choose **Properties**.

   The Properties dialog box of the PFM - Web Service appears.
7. Set the **startup type**.

   To cancel the automatic start, select **Manual**.

   To reset the automatic start, select **Automatic**.
8. Click the **OK** button.

Notes:

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

(b) In UNIX

To automatically start services at system startup, use the service automatic start script file for the PFM - Web Console service.

To set up automatic starting of services:

1. Log on to the host where you want to start services automatically.
2. Execute the following command to move to the `/opt/jp1pcwebcon` directory:

   ```
   cd /opt/jp1pcwebcon
   ```

3. Set the service automatic start script file for PFM - Web Console.

   The names of the `.model` file of the service automatic start script and the service automatic start script file are as follows:

   - Name of the `.model` file of the service automatic start script: `jpcw_start.model`
   - Name of the service automatic start script file: `jpcw_start`

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

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

1.3 Stopping services

This section describes how to stop Performance Management program services.

Note:

The following OS user permissions are necessary to start services:

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

1.3.1 Stopping monitoring manager and monitoring agent services

This subsection describes how to stop each service on the monitoring manager or the monitoring agent.

(1) Stopping services manually

You can use the following two methods to stop services manually:

- Stopping services by using the `jpcspm stop` command
- Stopping services from the browser

(a) Stopping services by using a command

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

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

To stop services:

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

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

2. Execute the `jpctool service list` command.

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

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

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

For details on the information which you can display by executing the `jpctool service list` command, see *1.6.1 Checking the operating status of services by using a command*.

3. Execute the `jpcspm stop` command.

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

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

   For details on the service keys to stop a specific PFM - Agent or PFM - RM service on the host, see the sections that describe the naming rules for services in an appendix of the manual *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

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

   ```
   jpcspm stop -key jp1pc
   ```

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

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

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

Reference note:

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

- PFM - Manager service

- PFM - Agent or PFM - RM service

(b) Stopping services from the browser

This subsection describes how to stop the Performance Management program services from the monitoring console browser.

Note:

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

To stop services:

1. From the monitoring console browser, log on to PFM - Web Console.

   Log on to a user account that has administrator user permissions.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

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

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

   Machines folder

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

   PFM-Manager folder

   This folder manages the PFM - Manager services.

   The selected service is marked with a checkmark.

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

   A message box appears to confirm the service stop.

5. Click the **OK** button in the message box.

   The selected service stops.

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

Note:

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

(2) Stopping services automatically

The following describes procedures for stopping services automatically at system startup for each OS.

(a) In Windows

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

Note:

The OS automatic stop might cause OS shutdown while PFM services are stopping. Therefore, we recommend that you stop services by using the `jpcspm stop` command.

(b) In UNIX

To automatically stop services at the system stop, use the service automatic stop script file for the Performance Management system. If you are using AIX, also use the automatic start script file for AIX.

To set the automatic stopping of services:

1. Log on to the host to be set for the automatic starting of the services.

   Log on to the monitoring manager if you are going to operate PFM - Manager services. Log on to the monitoring agent if you are going to operate the services of PFM-Base and either PFM - Agent or PFM - RM.

2. Execute the following command to move to the `/opt/jp1pc` directory:

   ```
   cd /opt/jp1pc
   ```

3. Set the service automatic stop script file for the Performance Management system.

   Names of the `.model` file of the service automatic stop script, and the service automatic stop script file are as follows:

   - Name of the `.model` file of the service automatic stop script: `jpc_stop.model`
   - Name of the service automatic stop script file: `jpc_stop`

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

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

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

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

   The name of the automatic stop script file is as follows:

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

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

```
if [ -x /opt/jp1pc/jpc_stop ]; then
        /opt/jp1pc/jpc_stop
fi
```

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

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

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

1.3.2 Stopping monitoring console server services

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

(1) Stopping services manually

You can use the following two methods to stop PFM - Web Console services on the monitoring console server. Note that the instructions for stopping services from the Control Panel apply only to Windows systems.

- Stop by using the `jpcwstop` command
- Stopping from the Control Panel (Windows only)

The following describes each procedure.

(a) Stopping by using a command

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

To stop services by using a command:

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

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

   - In Windows:

     PFM-Web-Console-installation-folder`\tools`
   - In UNIX:

     `/opt/jp1pcwebcon/tools`

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

(b) Stopping from the Control Panel

To stop services from the Control Panel:

1. From the **Start** menu of Windows, choose **Settings**, **Control Panel**, **Administrative Tool**, and then **Services**.

   The Services dialog box appears.
2. Right-click the **PFM - Web Service** service, and from the pulldown menu choose **Stop**.
3. Right-click the **PFM - Web Console** service, and from the pulldown menu choose **Stop**.

(2) Stopping services automatically

(a) In Windows

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

(b) In UNIX

To automatically stop services at system shutdown, use the service automatic stop script file for the PFM - Web Console service.

To set up automatic stopping of services:

1. Log on to the host where you want to stop services automatically.
2. Execute the following command to move to the `/opt/jp1pcwebcon` directory:

```
cd /opt/jp1pcwebcon
```

3. Set the service automatic stop script file for PFM - Web Console.

   The names of the `.model` file of the service automatic stop script and the service automatic stop script file are as follows:

   - Name of the `.model` file of the service automatic stop script: `jpcw_stop.model`
   - Name of the service automatic stop script file: `jpcw_stop`

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

   ```
   cp -p jpcw_stop.model jpcw_stop
   ```

   ```
   chmod 555 jpcw_stop
   ```

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

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

1.4.1 Configuration for synchronizing service starting and stopping

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

To modify the `pfmwebcon_host.conf` file:

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

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

   - In Windows:

     PFM-Web-Console-installation-folder`\conf\`

   - In UNIX:

     `/opt/jp1pcwebcon/conf/`

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

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

   # Operate Host
   HOST_NAME=HOSTNAME

   The following table describes valid values of *HOSTNAME*.

   Table 1-1: Valid values of HOSTNAME

Value	Description
--	Specifies that starting and stopping are not to be synchronized.
`localhost`	Specifies that starting and stopping are to be synchronized in a non-cluster system environment. Use lower-case characters only.

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

Legend

--: No value

1.4.2 Procedure for synchronizing service starting and stopping

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

- `all`: All services on the host, including PFM - Web Console.
- `WebConsole` or `wc`: The PFM - Web Console service on the host.

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

```
jpcspm start -key all
```

For details on starting or stopping services, see *1.2 Starting services* and *1.3 Stopping services*.

1.5 Logging on to and off from PFM - Web Console

This section describes how to log on to PFM - Web Console from the monitoring console browser, and how to log off from PFM - Web Console.

1.5.1 Logging on to PFM - Web Console

To log on to PFM - Web Console from the monitoring console browser:

1. In the browser, enter the following URL:

   `http://`*PFM-Web-Console-server-name*`:20358/PFMWebConsole/login.do`

   Reference note:

   For details on how to change the port number to access to PFM - Web Console from the browser, see an appendix of the manual *Job Management Partner 1/Performance Management Reference*.

   Note

   If you log on more than once from the same browser on the same monitoring console, the previously logged-in session might be invalidated. For details on controlling multiple logins, see the chapter describing the initialization file (`config.xml`) in the manual *Job Management Partner 1/Performance Management Reference*.

   The **Login** window appears.

Figure 1-1: **Login** window

2. Enter a **User name** and **Password**.

   Enter a user name and password.

   Reference note:

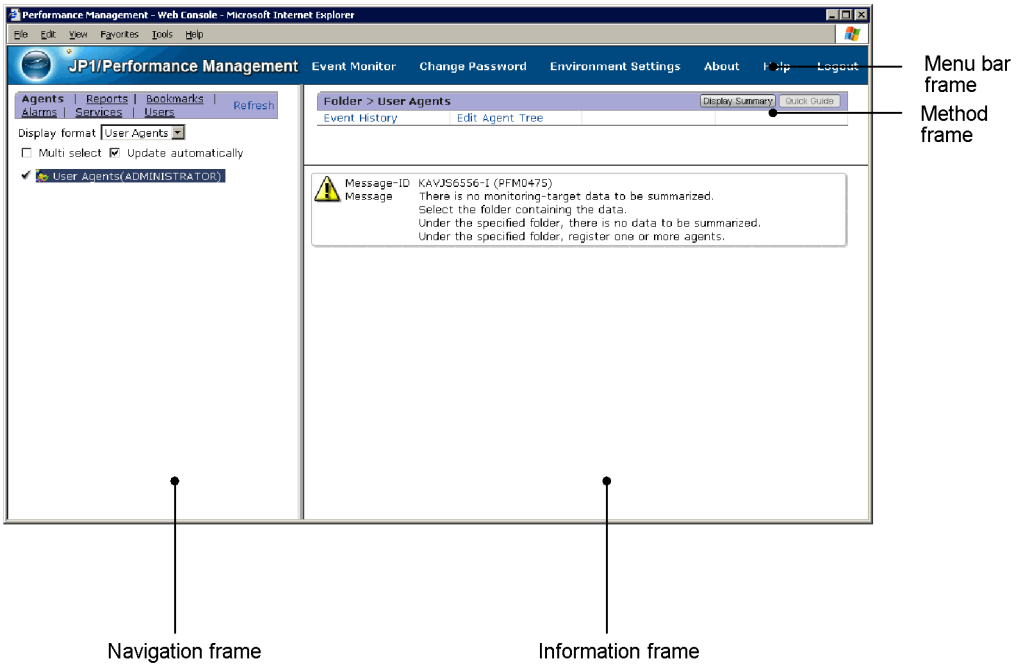
   > Use the following user account when logging on for the first time:
   >
   > **User name**: `ADMINISTRATOR`
   >
   > **Password**: None
   >
   > For security reasons, configure a password for the ADMINISTRATOR account before starting to use Performance Management. For details on user account management, see *2. Managing User Accounts*.

3. Click the **Login** button.

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

   In the navigation frame immediately after login, **User Agents** (*logged-on-user-name*) appears in the root of the Agents tree. In the information frame, the summary that **User Agents** (*logged-on-user-name*) is being selected appears. For details on how to display the summary, see *3.3.5 Using summary display to check the operating status*.

Figure 1-2: **Main** window



For details on the main window, see the chapters that describe windows in the manual *Job Management Partner 1/Performance Management Reference*.

1.5.2 Logging off from PFM - Web Console

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

Note:

The Reports window, when displayed, might not close in conjunction with the closing of the main window.

In the following cases, close each Reports window by using the **Close** button:

- When numerous Reports windows are displayed

  Try to have 10 or less windows displayed for history reports or for realtime reports that do not refresh automatically.

  When you display multiple realtime reports that refresh automatically and their refresh processing occurs at the same time, the refresh processing cannot keep up even if 10 windows or less are open. This causes the

processing time to exceed the automatic refresh request interval leading to the possible stoppage of automatic refresh.

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

1.6 Checking the status of service operations

You can use the following two methods to check the status of service operations:

- Checking the status of service operations by using the `jpctool service list` command
- Checking the status of service operations by using the browser

Note:

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

In other situations, you cannot check information of the PFM - Web Console services by using the `jpctool service list` command. To check information of the PFM - Web Console services by using the Services dialog box, from the **Start** menu of Windows, choose **Settings**, **Control Panel**, **Administrative Tools**, and then **Services**.

1.6.1 Checking the operating status of services by using a command

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

You can also use this command to check the operating status of the PFM - Web Console service that is installed on the host where the `jpctool service list` command is executed. To do so, edit the `pfmwebcon_host.conf` file in the same way as for synchronized starting and stopping of the PFM - Manager or PFM - Base and PFM - Web Console services. For details on how to edit the `pfmwebcon_host.conf` file, see *1.4.1 Configuration for synchronizing service starting and stopping*.

To check the status of service operations:

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

   For example, to check the status of all service operations on the host WebAP, specify as follows:

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

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

Output information	Description
Host Name	Name of the host on which services are operating
ServiceID	Service ID
Service Name	Service name
PID	The process ID of the service. • When the status management function is enabled: The process ID appears only when the Status is Active, Busy, S Active, S Busy, Starting, or Stopping. • When the status management function is disabled or your product version does not support the status management function: The process ID appears only when the Status is Active.
Port	The communication port number used by the service. • When the status management function is enabled: The port number appears only when the Status is Active, Busy, S Active, or S Busy. • When the status management function is disabled or your product version does not support the status management function: The port number appears only when the Status is Active.

Output information	Description
Status	The status of the service. When the status management function is enabled: • Status display in versions that support the status management function: Active: The service is waiting for a request. Inactive: The service is stopped. Starting: The service is starting. Busy: The service is processing a request. S Active: The service is waiting for a request (stand-alone mode). S Busy: The service is processing a request (stand-alone mode). Stopping: The service is stopping. • Status display in versions that do not support the status management function: Active*: The service is running. Incomp*: The service is starting or stopping. Inactive*: Either the system cannot establish a connection to the service or the service is stopped. Comm Err*: The system is able to establish a connection to the service but there is no response. Timeout*: The connection to the service has timed out. Error*: An error other than a connection timeout has occurred. Refer to the common message log for details of the error. For details on PFM - Web Console service errors, see the trace log. In the following situations, the above status display applies for services that support the status management function. - The Status Server service is stopped. - The Status Server has started but the status management function cannot recognize the status of the service#. # You will need to restart the service for the status management function to recognize the service status correctly. When the status management function is disabled or your product version does not support the status management function: Active: The service is running. Incomp: The service is starting or stopping. Inactive: Either the system cannot communicate with the service or the service is stopped. Comm Err: The system is able to establish a connection to the service but there is no response. Timeout: The connection to the service has timed out. Error: An error other than a connection timeout has occurred. Refer to the common message log for details of the error. For details on PFM - Web Console service errors, see the trace log.

1.6.2 Checking the operating status of services on the browser

This subsection describes how to log on to PFM - Web Console from the monitoring console browser, and how to check the status of service operations in the Services window.

Note:

Administrator user permissions are necessary to check the status of service operations by using a browser.

To check the status of service operations in the monitoring console browser:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, choose the service of which you want to check an operation status.

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

   Machines folder

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

   PFM-Manager folder

   This folder manages the PFM - Manager services.

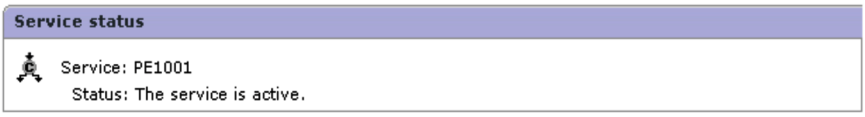
   The selected service is marked with a checkmark.

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

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

   The following figure shows an example of the service operation status display:

   Figure 1-3: Example of the service operation status display



1.7 Specifying automatic refresh intervals for the browser

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

The specified automatic refresh interval applies to the following windows:

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

To specify the automatic refresh interval:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.
2. In the menu bar frame, click the **Environment Settings** menu.

   The Environment Settings window appears.
3. Specify a refresh interval.

   Refresh Interval

   Specify an interval within 10 to 3600. The unit is seconds.

   The default setting is 60 seconds.
4. Click the **OK** button.

1.8 Notes

This section gives cautionary notes on starting or stopping the Performance Management.

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

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

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

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

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

- Only PFM - Agent, PFM - RM, or PFM - Base is running.

  This is called *stand-alone mode*.

- Initially PFM - Manager is running together with PFM - Agent, PFM -RM, or PFM - Base. Then PFM - Manager is stopped, so that only PFM - Base, PFM - Agent, or PFM - RM is running.

  This is called *non stand-alone mode*.

- PFM - Manager, PFM - Base, and either PFM - Agent or PFM - RM have started in this sequence and are all running.

  This is called *normal mode*.

Note:

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

(1) Overview of stand-alone mode

If the Master Manager services and Name Server services of PFM - Manager have not been started, PFM - Agent, PFM - RM, or PFM - Base start in stand-alone mode to collect the performance data.

The system checks the connection to PFM - Manager once every 5 minutes in stand-alone mode. If PFM - Manager starts after PFM - Agent, PFM - RM, or PFM -

Base have already started in stand-alone mode, and PFM-Manager performs a successful connection check with one of those programs, that program switches from stand-alone mode to normal mode connected to PFM - Manager. At this time, you can consult history reports to check the performance data stored in PFM - Agent or PFM - RM during stand-alone mode.

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

(2) Functions available in stand-alone mode

The following table describes the availability of functions in stand-alone mode operation.

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

Function	Availability	Service name
Starting and stopping services, and checking operation status	Y	• In PFM-Agent host Agent Store, Agent Collector, and Action Handler • In PFM-RM host Remote Monitor Store, Remote Monitor Collector, and Action Handler
Collecting history data	Y	• In PFM-Agent host Agent Store and Agent Collector • In PFM-RM host Remote Monitor Store and Remote Monitor Collector
Displaying reports and connecting from ODBC-compliant application programs	N	Agent Store and Remote Monitor Store
Issuing alarms that indicate agent start	Y	Agent Collector and Remote Monitor Collector
Monitoring the performance data by alarms	N	Agent Collector and Remote Monitor Collector
Executing actions in response to alarm events	N	Action Handler
Service status management	Y	Status Server

Legend:

Y: Available

N: Not available

(3) Commands available in stand-alone mode

The following table describes the availability of commands in stand-alone mode operation.

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

Command	Function	Availability
`jpcconf db define`	Changing the directory settings of the Agent Store service and the Remote Monitor Store service	Y
`jpcconf db display`	Displaying information about the Agent Store service, the Remote Monitor Store service, or backup data	Y
`jpcconf db vrset`	Changing the version of the Store database	Y
`jpcconf hc`	Enabling or disabling the health check function	Y
`jpcconf stat`	Enabling or disabling the status management function	Y
`jpcras`	Collecting troubleshooting data of PFM - Manager, PFM - Agent, or PFM - RM	Y
`jpcspm start`	Starting services	Y
`jpcspm stop`	Stopping services	Y
`jpctool db backup`	Creating backup files of the data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y#
`jpctool db clear`	Deleting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	N
`jpctool db dmconvert`	Converting the data model of backup data	Y
`jpctool db dump`	Exporting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y#
`jpctool db import`	Importing backup data	Y
`jpctool service delete`	Deleting service information of the agents registered in Performance Management	N

Command	Function	Availability
`jpctool service list` (when other host is specified by the `-host` option)	Displaying the structure and status of the Performance Management program services	N
`jpctool service list` (when the `-host` option is not used)	Checking the status of service operations on the local host	Y
`jpctool service register`	Re-registering service information of the Performance Management program	N

Legend:

Y: Available

N: Not available

#

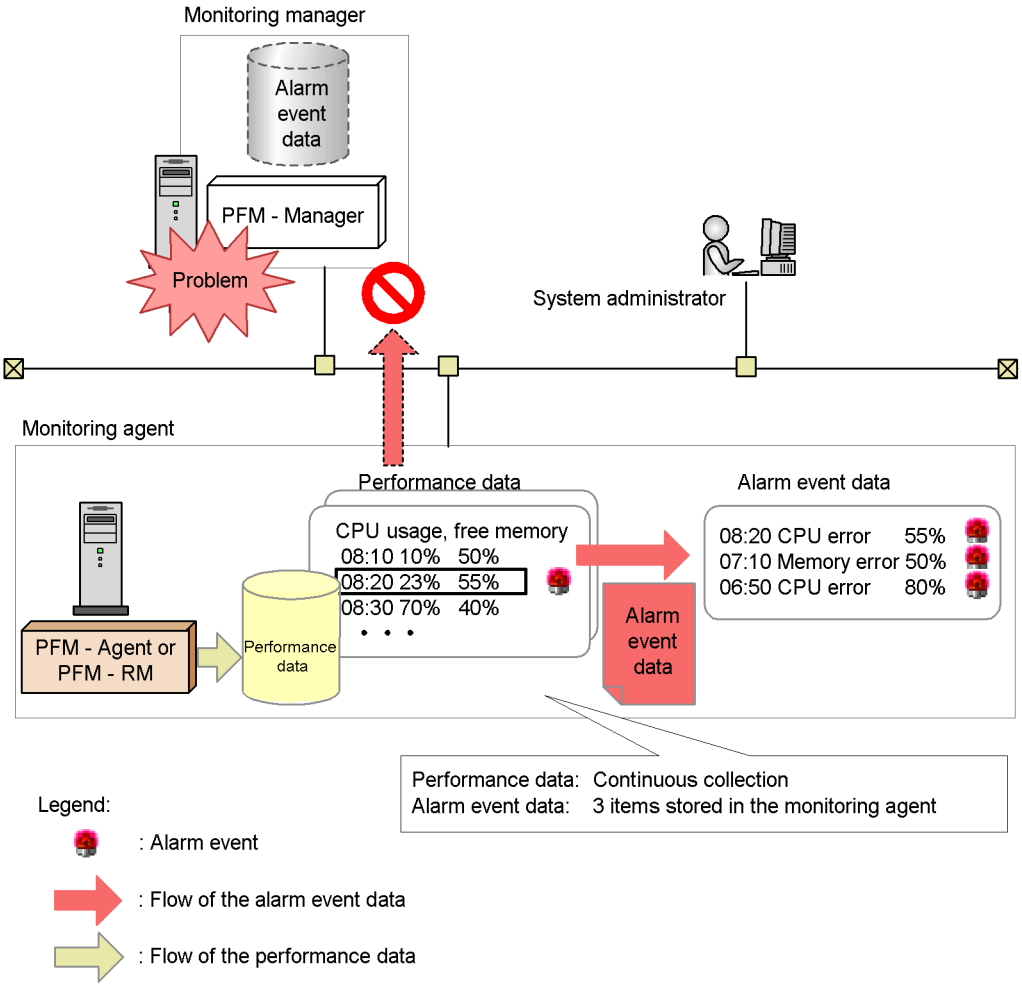
You can execute commands only when specifying the `-alone` option.

(4) Overview of non stand-alone mode

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

Unlike stand-alone mode, the system does not check the connection to PFM - Manager once every 5 minutes in non stand-alone mode. When PFM - Manager starts and communicates with PFM - Agent or PFM - RM (for example, to display a report), the system reconnects and switches to normal mode. At this time, you can consult history reports to check the performance data stored in PFM - Agent or PFM - RM during non stand-alone mode.

Figure 1-4: Overview of non stand-alone mode



Notes:

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

PFM - Manager again.

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

(5) Functions available in non stand-alone mode

The following table describes the availability of functions in non stand-alone mode operation.

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

Function	Availability	Service name
Starting and stopping services, and checking operation status	Y	• In PFM-Agent host Agent Store, Agent Collector, and Action Handler • In PFM-RM host Remote Monitor Store, Remote Monitor Collector, and Action Handler
Collecting history data	Y	• In PFM-Agent host Agent Store and Agent Collector • In PFM-RM host Remote Monitor Store and Remote Monitor Collector
Displaying reports and connecting from ODBC-compliant application programs	N	Agent Store and Remote Monitor Store
Monitoring the performance data by alarms	Y	Agent Collector and Remote Monitor Collector
Executing actions in response to alarm events	N#	Action Handler
Service status management	Y	Status Server

Legend:

Y: Available

N: Not available

#

The system operates differently according to the following conditions:

- If you specify LOCAL for the Action Handler services and no action has been executed.

  No action is executed while PFM - Manager is stopped.

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

- If you specify LOCAL for the Action Handler services, at least one action has been executed, but the Action Handler service executing the action has not restarted.

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

- If you specify something other than LOCAL for the Action Handler services.

  No actions are executed while PFM - Manager is stopped.

  After PFM - Manager starts, any actions that were generated while PFM - Manager was stopped are executed. Actions cannot be executed correctly if the Action Handler service of the PFM - Manager host is specified.

(6) Commands available in non stand-alone mode

The following table describes the availability of commands in non stand-alone mode operation.

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

Command	Function	Availability
`jpcconf db define`	Changing the directory settings of the Agent Store service or the Remote Monitor Store service	Y
`jpcconf db display`	Displaying information about the Agent Store service, the Remote Monitor Store service, or backup data	Y
`jpcconf db vrset`	Changing the version of the Store database	Y
`jpcconf hc`	Enabling or disabling the health check function	Y
`jpcconf stat`	Enabling or disabling the status management function	Y
`jpcras`	Collecting troubleshooting data of PFM - Manager, PFM - Agent, or PFM - RM	Y
`jpcspm start`	Starting services	Y
`jpcspm stop`	Stopping services	Y
`jpctool db backup`	Creating backup files of the data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	Y#
`jpctool db clear`	Deleting data stored in the database of the Master Store service, the Agent Store service, or the Remote Monitor Store service	N
`jpctool db dmconvert`	Converting the data model of backup data	Y

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

Legend:

Y: Available

N: Not available

#

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

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

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

1.8.3 Starting on a Windows machine

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

In this case, re-execute the `jpcspm start` command.

If the system frequently outputs this message even though you re-execute the `jpcspm start` command, change the retry intervals and counts of the automatic service start

by using the jpcspm start command. Changing the retry intervals and counts avoids service start errors caused by the service control manager.

Directly edit the settings of the jpccomm.ini file when changing the retry intervals and counts. The following table describes the section name, label name, and range of setting values that you can edit in the jpccomm.ini file.

Section	Label	Value range	Default value	Description
Tools Section	StartService Retry Interval	30 - 600[#1]	45	Retry intervals for service starts (unit: seconds)
	StartService Retry Count	0 - 120[#2]	3	Retry counts for service start (unit: times)

#1

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

#2

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

The installation folder stores the jpccomm.ini file.

To change the retry intervals and counts:

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

   Change values of the following labels:

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

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

1.8.4 Starting the Status Server service

To recreate the jpccomm.ini file, you make a copy of the jpccomm.ini.model file and rename the copy to jpccomm.ini. Note, however, that this will disable the status management function and prevent the Status Server service from starting. To remedy this, choose the appropriate procedure from following list.

(1) In Windows:

(a) If Performance Management is not configured to use logical hosts

1. Stop all PFM services on the host where you want to edit the `jpccomm.ini` file.
2. Delete the `jpccomm.ini` file from the *installation-folder*`\jp1pc` directory.
3. Make a copy of the `jpccomm.ini.model` file found in the *installation-folder*`\jp1pc` directory and rename the copy to `jpccomm.ini`.
4. Execute the `jpcconf stat enable` command to enable the status management function.
5. Set any parameters that were set in the previous `jpccomm.ini` file.
6. Start the PFM services on the host.

(b) If Performance Management is configured to use logical hosts

1. Stop all PFM services (including those for logical hosts) on the host where you want to edit the `jpccomm.ini` file.
2. Delete the `jpccomm.ini` file from the *installation-folder*`\jp1pc` directory.
3. Delete the `jpccomm.ini` file from *environment-directory*`\jp1pc` directory.
4. Make a copy of the `jpccomm.ini.model` file found in the *installation-folder*`\jp1pc` directory and rename the copy to `jpccomm.ini`.
5. Make a copy of the `jpccomm.ini.model` file found in the *environment-directory*`\jp1pc` directory and rename the copy to `jpccomm.ini`.
6. Execute the `jpcconf stat enable` command to enable the status management function.
7. Set any parameters for the logical and physical hosts that were changed in the previous `jpccomm.ini` file.
8. Start all the PFM services (including those for logical hosts).

(2) In UNIX:

(a) If Performance Management is not configured to use logical hosts

1. Stop all PFM services on the host where you want to edit the `jpccomm.ini` file.
2. Delete the `jpccomm.ini` file from the `/opt/jp1pc` directory.
3. Make a copy of the `jpccomm.ini.model` file found in the `/opt/jp1pc` directory and rename the copy to `jpccomm.ini`.
4. Execute the following command to set the permissions for the file:
   `chmod 666 jpccomm.ini`

5. Execute the `jpcconf stat enable` command to enable the status management function.
6. Set any parameters that were set in the previous `jpccomm.ini` file.
7. Start the PFM services on the host.

(b) If Performance Management is configured to use logical hosts

1. Stop all PFM services (including those for logical hosts) on the host where you want to edit the `jpccomm.ini` file.
2. Delete the `jpccomm.ini` file from the `/opt/jp1pc` directory.
3. Delete the `jpccomm.ini` file from the *environment-directory*`/jp1pc` directory.
4. Make a copy of the `jpccomm.ini.model` file found in the `/opt/jp1pc` directory and rename the copy to `jpccomm.ini`.
5. Execute the following command to set the permissions for the file:
   `chmod 666 jpccomm.ini`
6. Make a copy of the `jpccomm.ini.model` file found in the *environment-directory*`/jp1pc` directory and rename the copy to `jpccomm.ini`.
7. Execute the following command to set the permissions for the file:
   `chmod 666 jpccomm.ini`
8. Execute the `jpcconf stat enable` command to enable the status management function.
9. Set any parameters for the logical and physical hosts that were changed in the previous `jpccomm.ini` file
10. Start the PFM services (including those for logical hosts).

1.8.5 Monitoring alarm events

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

While PFM - Manager is stopped, PFM - Agent or PFM - RM retains a maximum of three alarm events per alarm definition. If more than three alarm events occur for a specific alarm definition, the alarm events are overwritten in order from the oldest. The retained alarm events are issued after PFM - Manager restarts.

1.8.6 Executing actions

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

Chapter

2. Managing User Accounts

This chapter explains the authentication management method and user permissions that Performance Management provides, and describes how to manage user accounts.

2.1 User account authentication and permissions
2.2 Setting the user account authentication mode
2.3 Creating a Performance Management user account
2.4 Editing a Performance Management user account

2.1 User account authentication and permissions

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

The details of each authentication mode are as follows:

PFM authentication mode

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

JP1 authentication mode

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

Note:

- To use PFM - Manager in a logical host environment to set the JP1 authentication mode, JP1/Base must be running on the same logical host as PFM - Manager.
- To use the JP1 authentication mode, you must set up an authentication server to be used by JP1/Base. However, the JP1/Base authentication server does not need to be running on the same host as PFM - Manager. For details on how to set up an authentication server used by JP1/Base, see the JP1/Base manual.
- To use the JP1 authentication mode in an environment using PFM - Manager on a cluster system, JP1/Base must also be used on the cluster system. The version of JP1/Base must be 08-00 or later.

For user account, you can select either the *administrator user permissions* (for management users) or the *general user permissions* (for ordinary users), depending on the purpose of usage.

The following table describes the Performance Management functions that are available for user account permissions in each authentication mode.

Table 2-1: User permissions and available functions in Performance Management

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Management of the Performance Management program services	Displaying the Services window	Services tree	Y	N	Y	N
	Stopping the Performance Management program services	Services tree	Y	N	Y	N
	Checking the status of the Performance Management program services	Services tree	Y	N	Y	N
Management of the Performance Management user accounts	Displaying the Users window	Users tree	Y	N	N	N
	Creating, copying, and deleting user accounts	Users tree	Y	N	N	N
	Changing the logon password for currently logged-on user accounts	Change Password window	Y	Y	N	N

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Changing the logon password or permission of other user accounts	Users tree	Y	N	N	N
Management of agents	Displaying the Agents window	Agents tree	Y	Y	Y	Y
	Creating, copying, and deleting folders	Agents tree	Y	Y	Y	Y
	Changing folder names	Agents tree	Y	Y	Y	Y
	Adding, copying, and deleting agents	Agents tree	Y	Y	Y	Y
	Displaying agent properties	Agents tree	Y	Y	Y	Y
	Displaying the summary	Agents tree	Y	Y	Y	Y
	Changing agent properties	Services tree	Y	N	Y	N
	Distributing agent properties	Services tree	Y	N	Y	N

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Displaying bound agents	Alarms tree	Y	N	Y	N
Definition and operation of reports	Displaying a report hierarchy	Reports tree	Y	C	Y	C
	Defining reports by using the report wizard	Reports tree	Y	C	Y	C
	Editing reports from the Reports window	Reports tree	Y	Y	Y	Y
	Saving report definitions from the Reports window	Reports tree	Y	C	Y	C
	Importing and exporting report definitions	Reports tree	Y	C	Y	C
	Displaying reports about agents	Agents tree/ Bookmarks tree/ Reports window	Y	Y	Y	Y

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Displaying reports about alarms	Agents tree	Y	Y	Y	Y
	Editing, copying, and deleting reports	Reports tree	Y	C	Y	C
	Changing report names	Reports tree	Y	C	Y	C
	Displaying report properties	Reports tree	Y	C	Y	C
	Changing report display conditions	Reports tree	Y	Y	Y	Y
	Printing reports	Reports tree	Y	Y	Y	Y
	Outputting report files	Agents tree/ Bookmarks tree	Y	Y	Y	Y
Definition and operation of alarms	Displaying the Alarms window	Alarms tree	Y	N	Y	N
	Defining an alarm by using the alarm wizard	Alarms tree	Y	N	Y	N

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Defining an alarm by using the Quick Guide	Alarms tree	Y	N	Y	N
	Binding or unbinding alarm tables in the Agents window	Agents tree	Y	N	Y	N
	Importing and exporting alarm definitions	Alarms tree	Y	N	Y	N
	Displaying the status of agent-related alarms in the Alarms window	Agents tree	Y	Y	Y	Y
	Operating and stopping alarms	Alarms tree	Y	N	Y	N
	Copying and deleting alarm tables	Alarms tree	Y	N	Y	N
	Copying and deleting alarms	Alarms tree	Y	N	Y	N
	Editing alarms	Alarms tree	Y	N	Y	N

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Displaying alarm properties in the Agents window	Agents tree	Y	Y	Y	Y
	Displaying alarm properties in the Event Monitor window	Event Monitor window	Y	Y	Y	Y
	Displaying alarm properties in the Alarms window	Alarms tree	Y	N	Y	N
Event display	Displaying the Event Monitor window	Event Monitor window	Y	Y	Y	Y
	Changing the event to be displayed	Event Monitor window	Y	Y	Y	Y
	Displaying reports about alarm events	Event Monitor window	Y	Y	Y	Y
	Displaying the Event History window	Agents tree	Y	Y	Y	Y

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
Management of the Store database	Collecting user-specific performance data	Services tree	Y	Y	Y	Y
	Changing the recording method of performance data	Services tree	Y	N	Y	N
	Adjusting the retention period of the Store database	Services tree	Y	N	Y	N
	Checking the capacity of the Store database	Services tree	Y	N	Y	N
Management of bookmarks	Displaying the Bookmarks tree	Bookmarks tree	Y	Y	Y	Y
	Creating folders	Bookmarks tree/ Agents tree/ Reports window/ Bookmark window of Agents tree	Y	C	Y	C

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Deleting folders	Bookmarks tree	Y	C	Y	C
	Changing folder names	Bookmarks tree	Y	C	Y	C
	Deleting bookmarks	Bookmarks tree	Y	C	Y	C
	Displaying bookmark properties	Bookmarks tree	Y	Y	Y	Y
	Changing bookmark names	Bookmarks tree	Y	C	Y	C
	Deleting registered reports	Bookmarks tree	Y	C	Y	C
	Displaying registered reports	Bookmarks tree	Y	Y	Y	Y
	Editing combination reports	Bookmarks tree	Y	C	Y	C
	Tiling display	Bookmarks tree	Y	Y	Y	Y

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Registering bookmarks or combination bookmarks	Reports window of Agents tree/ Bookmark window of Agents tree	Y	C	Y	C
	Registering a baseline	Reports window of Agents tree	Y	C	Y	C
	Updating a baseline	Reports window of Agents tree	Y	C	Y	C
Display of health check status	Displaying the health check status of each agent from the Agents tree	Agents tree	Y	Y	Y	Y
	Displaying the status of lower-level agents as the icon of a higher-level folder in the Agents tree	Agents tree	Y	Y	Y	Y

Function	Function detail	Tree or window	Performance Management user		JP1 user	
			Management user	Ordinary user	Management user	Ordinary user
	Changing the priority for displaying the status of lower-level agents as the icon of a higher-level folder	Agents tree	Y	Y	Y	Y
	Displaying the health check status of an agent from the Alarm Status window	Agents tree	Y	Y	Y	Y
	Displaying health check events in the Event Monitor window or the Event History window	Event Monitor window/ Event History window	Y	Y	Y	Y

Legend:

Y: Available

N: Not available

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

Reference note:

To set user permissions in the JP1 authentication mode, specify the following settings on the instance of JP1/Base that acts as an authentication server:

- Administrator user permissions

  JP1 resource group name: `JP1_PFM`, **permission level**: `JP1_PFM_Admin`

- General user permissions

  JP1 resource group name: `JP1_PFM`, **permission level**: `JP1_PFM_Operator`

2.2 Setting the user account authentication mode

Use the `jpcvsvr.ini` file to set the authentication mode of a user account (management method).

To set the authentication mode (management method) of a user account:

1. Stop the PFM - Manager and PFM - Web Console services.

   Stop the services in the order of PFM - Web Console and PFM - Manager.

2. Use a text editor or a similar tool to open the `jpcvsvr.ini` file.

   The `jpcvsvr.ini` file is stored in the following locations:

   On physical hosts:

   In Windows:

   installation-folder`\mgr\viewsvr\jpcvsvr.ini`

   In UNIX:

   `/opt/mgr/viewsvr/jpcvsvr.ini`

   On logical hosts:

   In Windows:

   environment-directory`\jp1pc\mgr\viewsvr\jpcvsvr.ini`

   In UNIX:

   environment-directory`/jp1pc/mgr/viewsvr/jpcvsvr.ini`

3. Change the value of `UserServer.authenticationMode` in the `jpcvsvr.ini` file.

   The following table describes the authentication mode settings for `UserServer.authenticationMode` in the `jpcvsvr.ini` file.

   Table 2-2: Authentication mode settings

Authentication mode	Settings
PFM authentication mode	`UserServer.authenticationMode=PFM`
JP1 authentication mode	`UserServer.authenticationMode=JP1`

Reference note:

The PFM authentication mode is set if you specify an invalid value.

4. Save and then close the `jpcvsvr.ini` file.
5. Start the services of PFM - Manager and PFM - Web Console.

   Start PFM - Manager, and then start PFM - Web Console.

   The changed `jpcvsvr.ini` file is loaded, and then the authentication mode is set.

Note:

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

Reference note:

Overwrite the `jpcvsvr.ini` file with the `jpcvsvr.ini.model` file (in the same folder) to restore the default settings for the `jpcvsvr.ini` file.

2.3 Creating a Performance Management user account

Log on to PFM - Web Console from the monitoring browser to create a user account when you set the PFM authentication mode.

You can use the following two methods to create a Performance Management user account:

- Create a new user account
- Customize an existing user account to create a new user account

JP1/Base manages user accounts when you set the JP1 authentication mode. For details on how to manage JP1 users, see the manual *Job Management Partner 1/Base User's Guide*.

2.3.1 Creating a new Performance Management user account

This subsection describes how to create a new Performance Management user account.

Reference note: The user account set immediately after installation

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

The default user account settings are as follows:

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

To create a new Performance Management user account:

1. From the monitoring console browser, log on to PFM - Web Console.

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

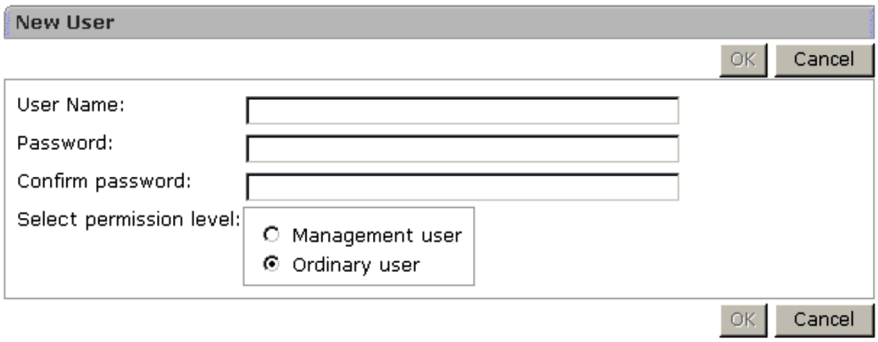
2. In the navigation frame of the Main window, choose the **Users** tab.

   The Users window appears.

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

   The New User window appears.

Figure 2-1: Example of the New User window



4. Specify information of the Performance Management user account.

   Items to be specified are as follows:

   User Name

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

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

   Password and **Confirm password**

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

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

   Note:

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

   Select permission level

   Select the administrator user permissions or the general user permissions for the permission level of the new user account.

5. Click the **OK** button.

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

2.3.2 Copying and customizing an existing user account

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

Point:

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

To create a new user account by customizing an existing user account:

1. From the monitoring console browser, log on to PFM - Web Console.

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

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

   The Users window appears.

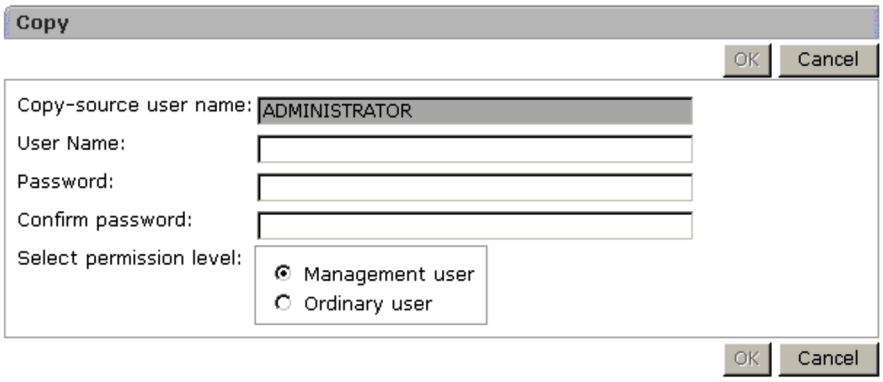
3. In the navigation frame of the Users window, select a source user account.

   The selected user is marked with a checkmark.

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

   The Copy window appears.

   Figure 2-2: Example of the Copy window



5. Specify the information for the Performance Management user account to be newly created.

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

User Name

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

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

Password and **Confirm password**

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

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

Note:

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

Select permission level

Select the administrator user permissions or the general user permissions for the permission level of the new user account.

6. Click the **OK** button.

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

2.4 Editing a Performance Management user account

This section describes how to edit information of an existing Performance Management user account.

You can perform the following operations when you edit user account information:

- Changing the password
- Changing the permissions of a user account
- Deleting a user account

Each operation is described below.

2.4.1 Changing the password

This subsection describes how to change the password for a user account. The procedures differ depending on the user account to be changed.

- When changing the password for a currently logged-on user account
- When changing the password for the user account of another user

The procedures in each case are described below.

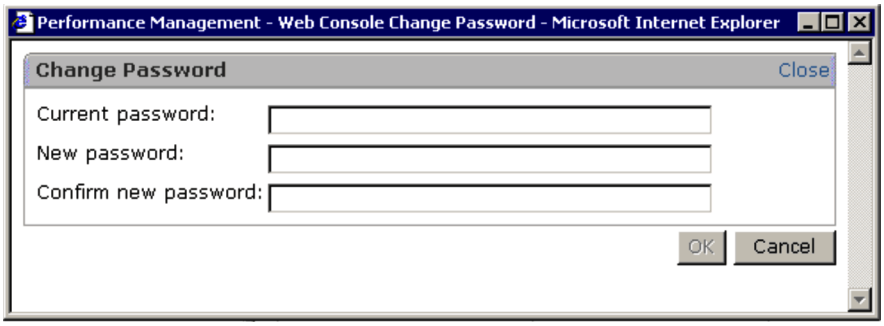
(1) When changing the password for a currently logged-on user account

To change the password for a currently logged-on user account:

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

   The Change Password window appears.

   Figure 2-3: Example of the Change Password window



2. Enter password information.

   Enter information for the following items:

Current password

Enter the current password.

New password and **Confirm new password**

Enter the new password you wish to specify.

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

Note:

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

3. Click the **OK** button.

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

(2) When changing the password for the user account of another user

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

1. From the monitoring console browser, log on to PFM - Web Console.

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

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

   The Users window appears.

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

   The selected user is marked with a checkmark.

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

   The Edit window appears.

5. Change the password for the user account that you specified in step 3.

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

distinguishes between upper- and lower-case characters.

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

Note:

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

6. Click the **OK** button.

   The changed password for the selected user account takes effect.

2.4.2 Changing the permissions of a Performance Management user account

To change the permissions of an existing Performance Management user account:

1. From the monitoring console browser, log on to PFM - Web Console.

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

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

   The Users window appears.

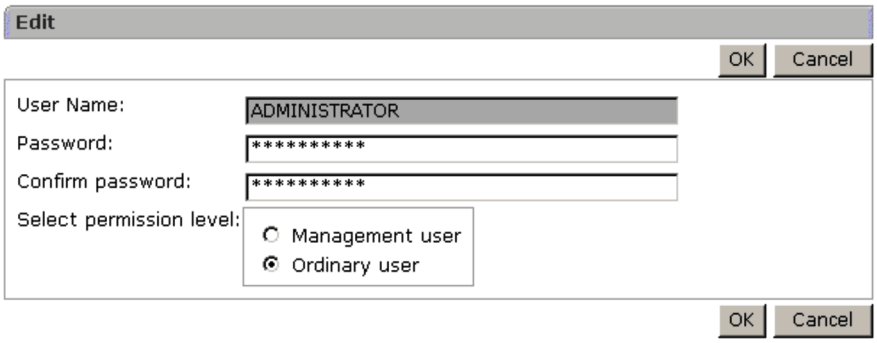
3. In the navigation frame of the Users window, select the user account whose permissions you want to change.

   The selected user is marked with a checkmark.

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

   The Edit window appears.

Figure 2-4: Example of the Edit window



5. Change the permissions of the user account that you selected in step 3.
6. Click the **OK** button.

   The changed permissions of the selected user account takes effect.

2.4.3 Deleting a Performance Management user account

This subsection describes how to delete an existing Performance Management user account.

Note:

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

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

To delete a Performance Management user account:

1. From the monitoring console browser, log on to PFM - Web Console.

   Log on with a user account that has the administrator user permissions (for example, the default user account ADMINISTRATOR).
2. In the navigation frame of the Main window, choose the **Users** tab.

   The Users window appears.
3. In the navigation frame of the Users window, select a user account to be deleted.

   The selected user is marked with a checkmark.
4. Choose the **Delete** method in the method frame.

   A message box appears to confirm the execution of deletion.
5. Click the **OK** button in the message box.

The selected user account is deleted from the navigation frame.

Chapter 3. Monitoring Agents

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

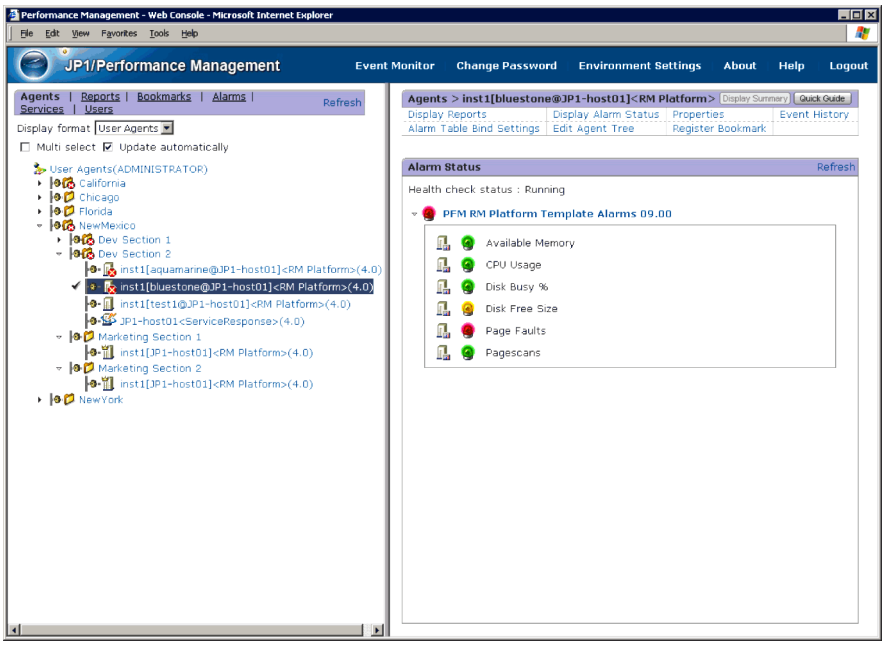
3.1 Monitoring by using the Agents tree
3.2 Creating an Agents tree
3.3 Monitoring the status of agent operations

3.1 Monitoring by using the Agents tree

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

The following figure shows an example of the Agents window of PFM - Web Console.

Figure 3-1: Example of the Agents window



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

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

- Monitoring by agent tree grouped for each product

  Use this format to monitor by using the Agents tree with items grouped in PFM - Agent product folders.

- Monitoring by using the Agents tree with items grouped for each logged-on user

  Use this format to monitor by using an Agents tree that is optionally created by

each logged-on user. Users can create and freely compose folders in units such as system structures or organizations.

The following table describes components of the Agents tree.

Table 3-1: Components of the Agents tree

Component	Description
Root ()	This indicates a root node of the Agents tree. • For monitoring by using a tree of each product The root appears with the name **Products**. • For monitoring by using a user-created tree The root appears with the name **User Agents** (*logged-on-user-name*). You cannot change the root name. You can choose formats by using **Display format** in the navigation frame of the Agents window.
Folder ()	This component is used to categorize agents. You can optionally make a maximum of 8 trees under a root (not including the root or agent) when creating an Agents tree.
Agent ()	This indicates PFM - Agent connected to PFM - Manager. Names of agents appear as service IDs. For details on service IDs, see the description of the service naming rules in the appendixes of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
Remote Monitor Collector service ()	This is a PFM - RM service that collects performance data. Each Remote Monitor Collector service appears with the name *instance-name* [*name-of-host-running-PFM-RM*] .
Remote agent ()	This is an agent used by PFM - RM to monitor a program. An agent is created for each monitored program. Each remote agent appears with the name *instance-name* [*monitored-object-name*@*name-of-host-running-PFM-RM*] .
Group agent ()	This is an agent used by PFM - RM to monitor multiple programs simultaneously. Each group agent appears with the *name instance-name* [*group-name*@*name-of-host-running-PFM-RM*] .

Supplemental information:

- You can create a maximum of 64 folders and 128 agents in one Agents tree

when using a user-created Agents tree.

- In the case of a tree organized by each product (when the selected display format is **Products**), the **Unknown** folder stores the PFM - RMs or PFM - Agents that are not registered in the Performance Management system. For details on how to register PFM - Agents or PFM - RMs, see the chapter that describes installation and setup in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

3.1.1 Agent types

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

- Agent for PFM - Agent

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

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

- PFM - RM remote agent

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

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

- PFM - RM group agent

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

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

3.2 Creating an Agents tree

This section describes how to create an Agents tree (for monitoring by using a user-created Agents tree).

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

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

Point:

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

3.2.1 Creating a new agent management folder

To create a new agent management folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

   In the navigation frame, the Agents tree with the root **User Agents** (*logged-on-user-name*) appears.

   - When logging on for the first time:

     Only the root **User Agents** (*logged-on-user-name*) appears.

   - If the logged-on user has already created components in the Agents tree:

     All folders under the root appear.

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

   The Edit Agent Tree window appears.

   - When logging on for the first time:

     Only the root **User Agents** (*logged-on-user-name*) appears in the information frame.

   - If the logged-on user has already created components in the Agents tree:

     All folders under the root appear.

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

- When logging on for the first time:

  Select **User Agents** (*logged-on-user-name*).

- When the logged-on user has already created components in the Agents tree, select **User Agents** (*logged-on-user-name*) or a higher folder of the folder to be created.

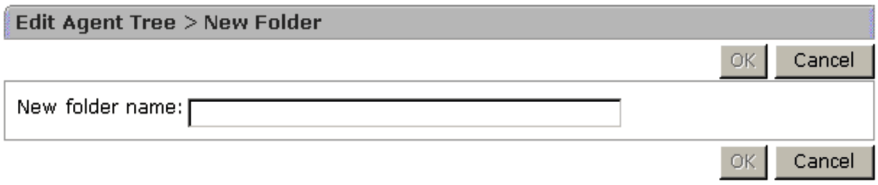
  The selected component is marked with a checkmark.

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

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

   The Edit Agent Tree > New Folder window appears.

   Figure 3-2: Example of the Edit Agent Tree > New Folder window



6. In **New folder name**, enter a folder name (1-64 characters).
7. Click the **OK** button.

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

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

3.2.2 Placing agents in a management folder

To place agents in a created folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

   The navigation frame displays the Agents tree that has **User Agents** (*logged-on-user-name*) as the root.

   - When logging on for the first time:

     Only the Agent tree root **User Agents** (*logged-on-user-name*) appears.

   - If the logged-on user has already created components in the Agents tree:

All folders under the root appear.

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

   The Edit Agent Tree window appears.

   - When logging on for the first time

     Only the root **User Agents** (*logged-on-user-name*) appears in the information frame.

   - When the logged-on user has already created components of the Agents tree

     All folders under the root appear.

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

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

   The selected component is marked with a checkmark.

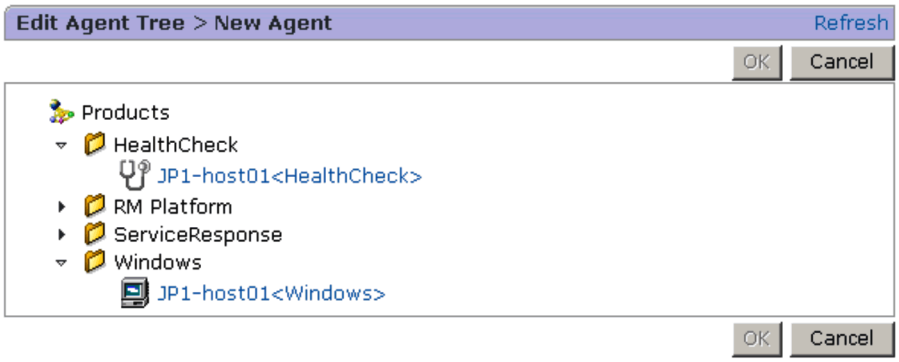
   Select a folder or **User Agents** (*logged-on-user-name*) to activate the **New Agent** button.

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

   The Edit Agent Tree > New Agent window appears.

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

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



Reference note:

Agents are listed by their service IDs. The format of the service ID depends on whether the product name display function is enabled. For example, if the host name for a PRM - RM Platform remote agent is `remmon`, its instance

name is `inst01`, its monitored host name is `rma1`, and the product name display function is enabled, the service ID is displayed as `inst01[rma1@remmon]<`*RMPlatform*`>`. If the product name display function is disabled, the same service ID is displayed as `7A1inst01[rma1@remmon]`.

For details on service IDs, see the description of the service naming rules in the appendixes of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. For details on the product name display function, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*

6. In the Agents tree displayed in the information frame, select an agent to be placed in the folder selected in step 4.

   The selected agent is marked with a checkmark.

7. Click the **OK** button.

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

3.2.3 Editing an Agents tree used for monitoring

This subsection describes the procedures to change the structure of an Agents tree:

- Copying a folder
- Deleting a folder
- Renaming a folder
- Copying an existing agent to a different folder
- Deleting an agent

(1) Copying a folder

To copy a folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

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

   The Edit Agent Tree window appears.

   In the information frame, the Agents tree that the logged-on user created appears.

4. In the Agents tree displayed in the information frame, select a resource folder of

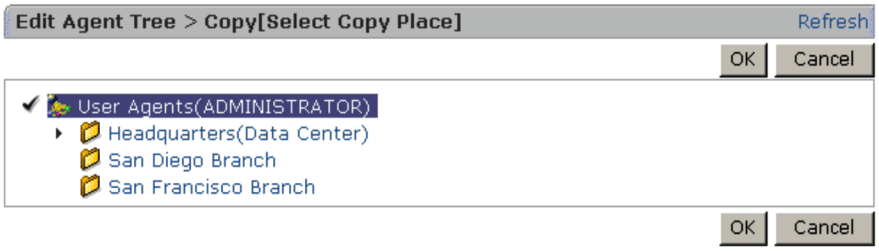
copying.

The selected folder is marked with a checkmark.

5. Click the **Copy** button.

   The Edit Agent Tree > Copy [Select Copy Place] window appears.

   Figure 3-4: Example of the Edit Agent Tree > Copy [Select Copy Place] window



6. Select the folder that is the copy destination.

   The selected folder is marked with a checkmark.

7. Click the **OK** button.

   The folder selected in step 4 is copied to under the folder selected in step 6. This procedure also copies folders and agents that are under the copied folder.

(2) Deleting a folder

To delete a folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

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

   The Edit Agent Tree window appears.

   In the information frame, the Agents tree that the logged-on user created appears.

4. In the information frame, select a folder to be deleted from the Agents tree.

   The selected folder is marked with a checkmark.

5. Click the **Delete** button.

   A message box appears to confirm the deletion.

6. Click the **OK** button in the message box.

   The folder selected in step 4 is deleted.

   This procedure also deletes folders and agents that are under the deleted folder.

(3) Renaming a folder

To rename a folder:

1. From the monitoring console browser, log on to PFM - Web Console.

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

   The Agents window appears.
3. In the method frame, choose the **Edit Agent Tree** method.

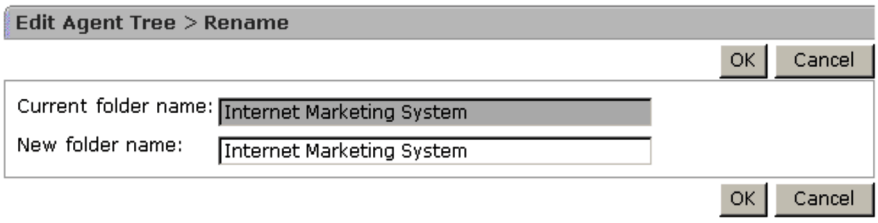
   The Edit Agent Tree window appears.

   In the information frame, the Agents tree that the logged-on user created appears.
4. In the Agents tree in the information frame, select a folder to be renamed.

   The selected folder is marked with a checkmark.
5. Click the **Rename** button.

   The Edit Agent Tree > Rename window appears.

   Figure 3-5: Example of the Edit Agent Tree > Rename window



6. In **New folder name**, enter a new folder name (1-64 characters).
7. Click the **OK** button.

   The changed name of the folder selected in step 4 takes effect.

(4) Copying an existing agent to a different folder

To copy an existing agent to a different folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

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

   The Edit Agent Tree window appears.

   In the information frame, an Agents tree of **User Agents** (*logged-on-user-name*) appears.

4. In the information frame, select an agent to be copied in the Agents tree.

   The selected agent is marked with a checkmark.

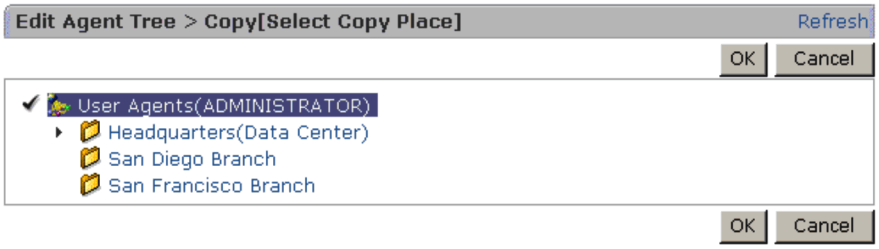
   Note:

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

5. Click the **Copy** button.

   The Edit Agent Tree > Copy [Select Copy Place] window appears.

   Figure 3-6: Example of the Edit Agent Tree > Copy [Select Copy Place] window



6. Select the folder that is the copy destination.

   The selected folder is marked with a checkmark.

7. Click the **OK** button.

   The agent selected in step 4 is copied to the folder selected in step 6.

(5) Deleting an agent

To delete an agent from a monitoring Agents tree:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

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

   The Edit Agent Tree window appears.

   In the information frame, an Agents tree of **User Agents** (*logged-on-user-name*) appears.

4. In the information frame, select an agent to be deleted from the Agents tree.

   The selected agent is marked with a checkmark.

5. Click the **Delete** button.

   A message box appears to confirm the deletion of the agent.

6. Click the **OK** button in the message box.

   The agent selected in step 4 is deleted.

3.3 Monitoring the status of agent operations

You can check the status of each agent by using the Agents tree icons displayed in the navigation frame of the Agents window.

In addition to monitoring, the following operations are available for any agents selected in the Agents tree:

- Displaying the status of alarms
- Displaying related reports
- Displaying event history
- Displaying the summary of the operational statuses
- Displaying properties

Each procedure is described below.

3.3.1 Checking the status of agents

You can check the status of agents by using the Agents tree icons displayed in the navigation frame of the Agents window.

Reference note:

You cannot check the status of the group agent.

To check the status of agents:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. From the **Display format** pull-down menu in the navigation frame, choose the display format for the Agents tree.

   The Agents tree appears in the selected display format.

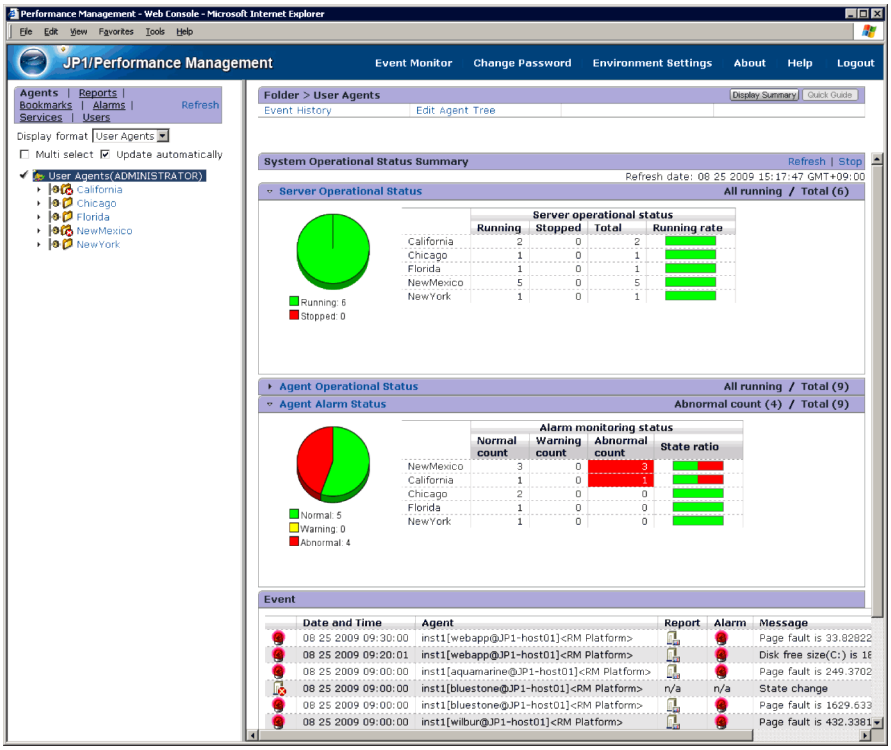
   - When **User Agents** is selected:

     The root appears as **User Agents** (*logged-on-user-name*) in the Agents tree.

   - When **Products** is selected:

     The root appears as **Products** in the Agents tree.

Figure 3-7: Example of an Agents tree



4. Check the icon displayed on the left of the Agents tree.

   The following tables describe the status indicated by the folder or agent icons:

   Table 3-2: Status indicated by folder icons

Icon	Description
	This icon indicates that all of the alarms in the alarm table bound to an agent under the folder are in normal status.
	This icon indicates that no alarm in the alarm table bound to an agent under the folder is in abnormal status and at least one alarm is in warning status.
	This icon indicates that at least one alarm in the alarm table bound to an agent under the folder is in abnormal status.
	This icon indicates the operating status of the agents in the folder.#

   Note:

The folder icon indicates the most severe status level among those of the agents in the folder. The severity levels starting from the most severe are abnormal, warning, and normal.

For a description of the icons that indicate the health check status, see Table 3-4.

Table 3-3: Status indicated by agent icons

Icon	Description
	This icon indicates that all of the alarms in the alarm table bound to an agent are in normal status.
	This icon indicates that no alarm in the alarm table bound to an agent is in abnormal status and at least one alarm is in warning status.
	This icon indicates that at least one alarm in the alarm table bound to an agent is in abnormal status.
	This icon indicates the operating status of the agent.#

For a description of the icons that indicate the health check status, see Table 3-4.

Table 3-4: Health check status indicated by icons

Icon	Description
	Not Supported#1,#2
	Running#1
	Incomplete#1
	Stopped#1
	Unconfirmed#1,#2
	Host Not Available#1

#1

For details on the status indicated by each health check event icon, see *13.2.2 Checking operating statuses*.

#2

For details about how to respond to a Not Supported or Unconfirmed health check status for an agent, see *14.2.5(2) The operating status of a server or agent is Unconfirmed or Not Supported*.

3.3.2 Checking the status of alarms

You can check the status of each alarm defined in the alarm table bound to each agent. You can also display reports that are bound to alarms.

Note:

You cannot display the status of alarms if an alarm table is not bound to agents. For details on how to bind an alarm table to agents, see *6.6.1 Changing the association between an alarm table and a monitoring agent*.

To check the status of alarms:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. From the **Display format** pull-down menu in the navigation frame, choose the display format for the Agents tree.

   The Agents tree appears in the selected display format.

   - When **User Agents** is selected:

     The root appears as **User Agents** (*logged-on-user-name*) in the Agents tree.

   - When **Products** is selected:

     The root appears as **Products** in the Agents tree.

4. In the Agents tree of the navigation frame, select the agent for which you want to check the alarm status.

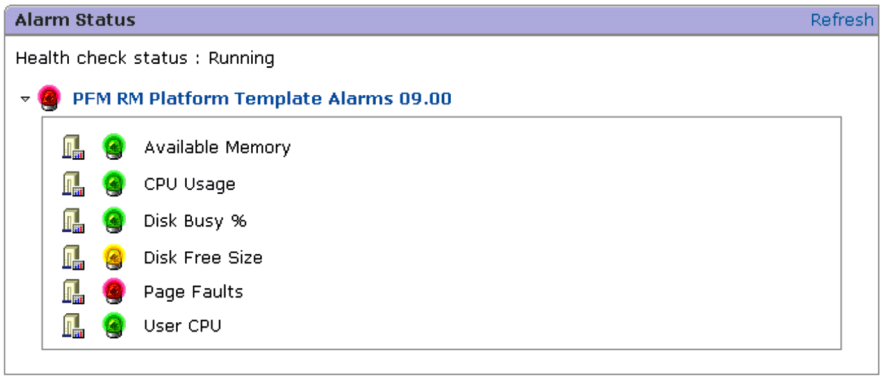
   The selected agent is marked with a checkmark.

5. Select the **Display Alarm Status** method in the method frame.

   The Alarm Status window appears.

   The following figure shows an example of the Alarm Status window.

Figure 3-8: Example of the Alarm Status window



A list of alarms appears displaying alarms defined in the alarm table that is bound to the agent selected in step 4.

You can check the status of alarms by examining the color of the alarm icons.

Alarm table status indicator icons

In the alarm table, the icon to the left of the alarm table name indicates the status of greatest importance.

The icon color represents the status of the alarm table as follows:

- : Indicates that the alarm table is expanded (with the definitions shown).
- : Indicates that the alarm table is collapsed (with the definitions hidden).
- (Green): This icon indicates normal status.
- (Yellow): This icon indicates warning status.
- (Red): This icon indicates abnormal status.

Alarm icons

An alarm icon appears to the left of each alarm name. The icon color represents the alarm status.

The status of alarms indicated by icon colors are as follows:

- (gray): Indicates that the alarm is inactive.

-  (green): Indicates normal status.
-  (yellow): Indicates warning status.
-  (red): Indicates abnormal status.
-  #: Always appears regardless of the alarm status.

  # Only when **Always notify** is selected in the alarm definition

Reference note:

The color of an alarm icon changes based on the thresholds and other conditions that you set in the Alarms window. For details on the settings of thresholds and conditions, see *6.4 Setting alarms by using the browser* or *6.7 Setting alarms by using commands*.

Report icons (for example, ) appear on the left of the alarm when you have bound a report to alarms. Click the report icon to display related reports.

For details on how to bind a report to alarms, see *5.7.1(2) Displaying a report associated with an alarm*.

A message indicating the health check status also appears.

For details on each health check status, see *13.2.2 Checking operating statuses*.

3.3.3 Displaying reports

Items that display performance data collected in each agent in graphical formats such as graphs and tables are called *reports*.

You can display various reports for each agent in the Agents window of PFM - Web Console.

Templates, called *monitoring templates*, are available for reports to be displayed. You can also create your own reports as desired. For details on how to display and create reports, see *5.7 Displaying reports* or *5.8 Displaying combination reports*.

3.3.4 Displaying event history

You can view a history of events that occurred in the Performance Management system. You can check the event history for each agent in the Event History window. You can also output event history data to a text file in CSV or HTML format.

For details, see *7.2 Displaying the event history*.

3.3.5 Using summary display to check the operating status

You can view a summary of results for operating status, stopped status, and Normal and Abnormal status counts to check the operating status of servers and agents, as well as the alarm status of agents. You can also view alarm and agent events with Abnormal status and Warning status. A view showing summarized results together with Abnormal and Warning status events is called a *summary display*.

(1) Prerequisite conditions

The following prerequisites must be met prior to using the summary display.

Requirements for server operating status monitoring

To be able to monitor server operating status, the version of the PFM - Manager for the connection destination must be 08-11 or later, the version of PFM - Web Console must be 09-00 or later, and the health check function must be enabled.

Requirements for agent operating status monitoring

To be able to monitor agent operating status, the version of the PFM - Manager for the connection destination must be 08-11 or later, the version of PFM - Web Console must be 09-00 or later, and the health check function must be enabled. In addition, you must set the following health check agent properties in the Service Properties window of the PFM - Web Console Services tree window:

- **Monitoring Level** in **Health Check Configurations**: Service

For details on the health check function, see *13.2 Using the health check function to check the operating status of monitoring agents and their hosts*.

(2) Agent types for which summary displays are supported

The following table lists the types of agents for which summary displays are supported, according to window type.

Table 3-5: Types of agents for which summary displays are supported

Agent type	Window type		
	Server Operational Status window	Agent Operational Status window	Agent Alarm Status window
PFM - Agent	Yes	Yes	Yes
Remote agent	Yes	Yes	Yes
Group agent	No	No	Yes
Remote Monitor Collector service	Yes	Yes	No

Legend:

Yes: Count supported

No: Count not supported

Summary displays are not supported for the following agents:

- Any agent that has been deleted from the Products tree in the Agents tree window using the `jpctool service delete` command, but remains in the User Agents tree.

  To update the agent trees to reflect the results of the `jpctool service delete` command, restart PFM - Manager and PFM - Web Console after executing the command.

(3) Procedure for displaying a summary

To check the operational statuses by displaying a summary:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

2. In the navigation frame of the main window, select the Agents tree tab.

   The Agents tree window is displayed.

3. From the **Display format** pull-down menu in the navigation frame, choose the display format for the Agents tree.

   The Agents tree appears in the selected display format.

   - When **User Agents** is selected:

     The Agents tree that has **User Agents** (*logged-on-user-name*) as the root appears.

   - When **Products** is selected:

     The Agents tree that has **Products** as the root appears.

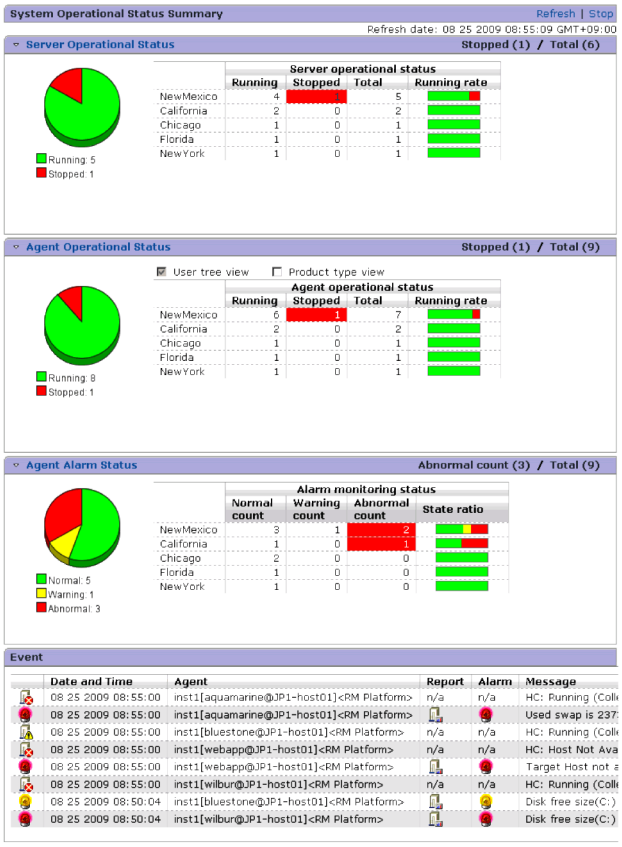
4. In the navigation frame, select the folders to be counted for the summary display.

   Depending on whether you select the root of the Agents tree, or you select a desired folder other than the root, the counting unit and counting range for summary display differ. For details on the counting unit and counting range for summary displays, see *3.3.5(5) Counting unit and counting range for a summary display*.

5. From the method frame, select the **View Summary** button.

   The System Operational Status Summary window appears in the information frame. The following figure shows an example of the System Operational Status Summary window.

Figure 3-9: Example of the System Operational Status Summary window



The items displayed in the Server Operational Status, Agent Operational Status and Agent Alarm Monitoring Status views are described below.

- ▽ : Indicates that an Operational Status or Monitoring Status view is currently displayed.
- ▶ : Indicates that an Operational Status or Monitoring Status view is not currently displayed.

The following table describes the items displayed in the Server Operational Status or Agent Operational Status views.

Table 3-6: Items displayed in the Server Operational Status and Agent Operating Status views

Item	Meaning
Pie chart	A pie chart showing the operating status of the servers or agents in the folder selected in the navigation frame. The meanings of the colors are as follows: • Green: Percentage of operating servers or agents. • Red: Percentage of stopped servers or agents. • Blue: Percentage of servers or agents with Unconfirmed status#1. For details on operational statuses, see *(4) Operating status classifications*.
Table	A table listing the operating status of the servers or agents in each folder selected in the navigation frame. The meanings of the items in a table are as follows: • Number operating: Number of servers or agents that are operating normally. • Number stopped#2: Number of servers or agents that are currently stopped (if the number stopped is one or greater, the cell is colored red). • Total: Total number of servers or agents (including those with Unconfirmed status). • Operating rate: Percentage of operating servers or agents (green indicates the percentage operating, red indicates the percentage stopped, and blue indicates the percentage with Unconfirmed status#1). The table shows the servers or agents with the five largest stopped counts, in descending order. The remaining servers are shown as Others. You can specify in the initialization file (`config.xml`) the number of servers or agents to be displayed. For details on the `config.xml`, see the chapter that describes installation and setup in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.
[User tree view] check box	This check box appears in the Agent Operational Status view when you select User Agents in the Agents tree. Selecting this check box displays the operating status at the folder levelthat the logged-on user created in the Agents tree.
[Product type view] check box	This check box appears in an Agent Operational Status view when you select User Agents in the Agents tree. Selecting this check box displays the operating status at the folder level where the agents are grouped according to the PFM - Agent product or the PFM - RM product.

#1:

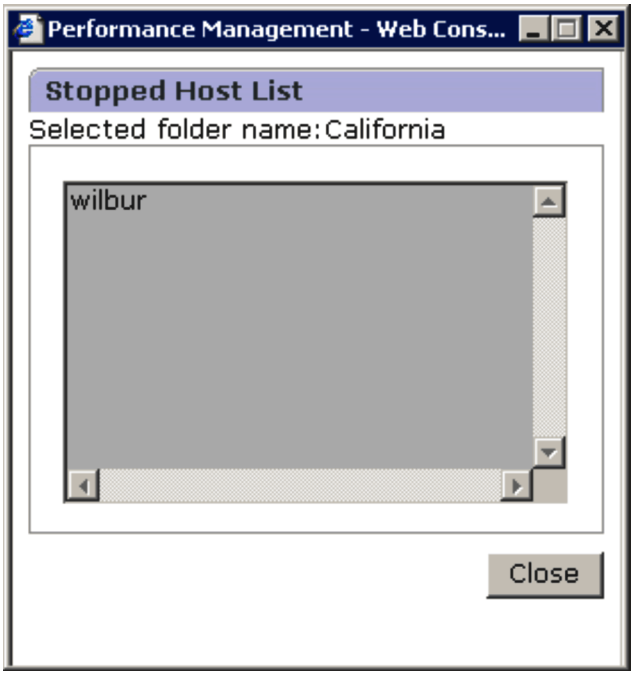
For details on how to take action when operational statuses become unknown, see *14.2.5(2) The operating status of a server or agent is Unconfirmed or Not Supported*.

#2:

In the Server Operational Status window, when the number of **Stopped** is one or more, clicking the number displays the Stopped Host List window. If you do this, you can check the host names of the stopped servers. The following figure shows

an example of the Stopped Host List window.

Figure 3-10: Stopped Host List window



The following table describes the items displayed in the Agent Alarm Monitoring Status view.

Table 3-7: Items displayed in the Agent Alarm Monitoring Status view

Item	Description
Pie chart	A pie chart showing the alarm monitoring status of agents in each folder selected in the navigation frame. Each color in the chart indicates an alarm status#. The meanings of the colors are as follows: • Green: Percentage of agents with Normal alarm status. • Yellow: Percentage of agents with Warning alarm status. • Red: Percentage of agents with Abnormal alarm status. The numbers in the pie chart indicate the number of agents for each alarm status. The numbers do not indicate the number of bound alarms.

Item	Description
Table	A table showing the alarm monitoring status of agents in the folder selected in the navigation frame. The meanings of the items in a table are as follows: • Normal count: Number of agents with Normal alarm status. • Warning count: Number of agents with Warning alarm status. • Abnormal count: Number of agents with Abnormal alarm status (if the number of Abnormal alarm status agents is one or greater, the cell is colored red). • Status ratio: Alarm event status ratio (green indicates the percentage with Normal status, yellow indicates the percentage with Warning status, and red indicates the percentage with Abnormal status). The table shows agents with the five greatest Abnormal status counts in the Alarm Monitoring Status view, in descending order. The remaining agents are shown as Others. You can specify the number of alarms to be displayed by setting the `maxDisplayAlarm` parameter in the initialization file (`config.xml`). For details on the `config.xml`, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#

The alarm status is determined as follows:

- Normal
- All bound alarms show a Normal status or there are no bound alarms.
- Warning

  No bound alarm shows an Abnormal status, but at least one bound alarm shows a Warning status.
- Abnormal

  At least one bound alarm shows an Abnormal status.

When the **Always notify** check box is selected for an alarm, the alarm always shows a Normal (green) status, because the alarm is not evaluated. However, remote and group agents are evaluated. The Remote Monitor Collector service is not evaluated because an alarm cannot be bound to it and it is not counted as a parameter in the pie chart.

If more than one alarm is bound to a single agent, these alarms are evaluated in order of priority. The priority starting from the highest is abnormal, warning, and normal.

Reference note:

The number of agents is counted as follows:

(Example 1) An agent has six alarms bound to it, where two alarms each show Normal, Warning, and Abnormal statuses.

The agent is classified with an Abnormal status of the highest priority. Thus, the agent is counted as an Abnormal agent.

(Example 2) An alarm for which the **Always notify** check box is selected is bound and the alarm status is Abnormal.

An alarm status for which the **Always notify** check box is selected is classified as Normal. Thus, the agent is counted as a Normal agent.

You can check for Abnormal and Warning status alarm events and agent events in the Events view. Unlike the Event Monitor window that displays all alarm and agent events that have been issued, the Events view displays only those alarms and agent events that have been issued with an Abnormal or Warning status and are currently pending. Any alarm event that is returning to Normal status is not shown. For details on displayed contents of each event, see 7. *Displaying Events* or see the description of the Event Monitor window in the manual *Job Management Partner 1/Performance Management Reference*.

The target alarms of the Agent Alarm Status window are those for which the **Always notify** check box is not selected. For details, see *6.9.3 Notes on evaluating alarms*.

(4) Operational status classifications

The meaning of the operating statuses shown in the Server Operational Status and Agent Operational Status views are described below.

(a) Operating statuses in the Server Operational Status view

The operating statuses displayed in the Server Operating Status view are determined based on the health check results from an agent monitoring the server. The health check results for the server are classified into three operating statuses: Operating, Stopped, and Unconfirmed.

In the Server Operational Status view, a single operating status is shown for each server. If more than one agent monitors a single server, the health check results from the agents might differ. In such a case, the health check results determined to have the highest priority in the range based on *(5) Counting unit and counting range for summary display* is shown as the operating status of the server in the Server Operational Status view.

The following table lists the agent health check results, resulting operating statuses, and their priority levels.

Table 3-8: Agent health check results, resulting operated statuses and priority levels

Agent type	Health check result	Judgment of operational status	Judgment priority
• PFM - Agent • Remote Monitor Collector service	Host Not Available	Stop	1
	Not Supported	Running	2
	Running		3
	Incomplete		4
	Stopped		5
	Unconfirmed		6
Remote agent	Host Not Available	Stop	7
	Running	Running	8
	Incomplete		9
	Unconfirmed	Unknown	10
	Not Supported		11

The following is an example of where the health check results from a PFM - Agent differ from those of a remote agent, while both are monitoring the same server.

In this example, the following health check results are assumed:

- The health check result from the PFM - Agent is Host Not Available.

  This health check result is determined to have priority level 1.

- The health check result from the remote agent is Not Supported.

  This health check result is determined to have priority level 11.

The operating status for the server is determined as follows:

- If PFM - Agent and the remote agent are in the same folder

  For both the pie chart and the table, Host Not Available with the higher priority is selected. Therefore, the operating status of the server is Stopped.

- If PFM - Agent and the remote agent are in different folders

  For the pie chart, Host Not Available with the higher priority is selected. Therefore, the operating status of the server is Stopped.

For the table, the result depends on the folder where the agent is located. A Host Not Available status is selected in the folder where PFM - Agent is located. Therefore, the operating status of the server is Stopped. A Not Supported status is selected in the folder where the remote agent is located. Therefore, the operating status of the server is Unconfirmed.

(b) Operating statuses in the Agent Operational Status view

The operating statuses displayed in the Agent Operational Status view are determined based on the health check result from an agent. The health check results are classified into three operating statuses: Operating, Stopped, and Unconfirmed.

The following table lists the agent health check results and the resulting operating statuses.

Table 3-9: Agent health check results and resulting operating statuses

Agent type	Health check result	Judgment of operational status
• PFM - Agent • Remote agent • Remote Monitor Collector service	Running	Running
	Incomplete	Stop
	Stopped	
	Host Not Available	
	Not Supported	Unknown
	Unconfirmed	

(5) Counting unit and counting range for a summary display

The following table lists the counting units and counting range for a summary display.

Table 3-10: Counting units and counting range for a summary display

Selected folder in the Agents tree	Pie graph / table	Counting unit	Counting range
Desired folder	Pie graph	Selected folder	All of the agents under the selected folder

Selected folder in the Agents tree	Pie graph / table	Counting unit	Counting range
	Table	Folders directly under the selected folder (The selected folder will be counted as **Other**.)	All of the agents under the folders directly under the selected folder (The agents directory under the selected folder will be counted as **Other**.)

Figure 3-11 and 3-12 show the summarized units and ranges for summary display.

Figure 3-11: Summarized units and ranges for summary display (when a route is selected)

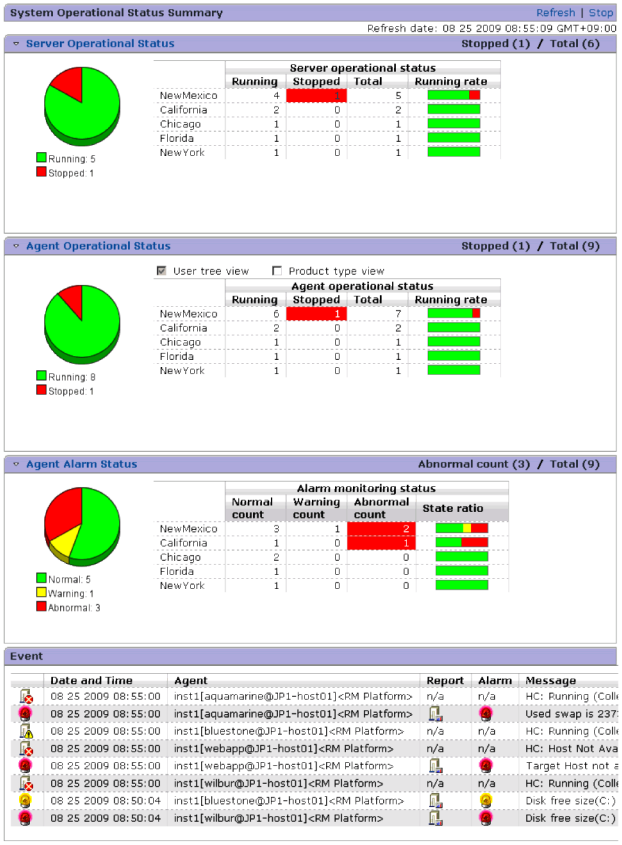
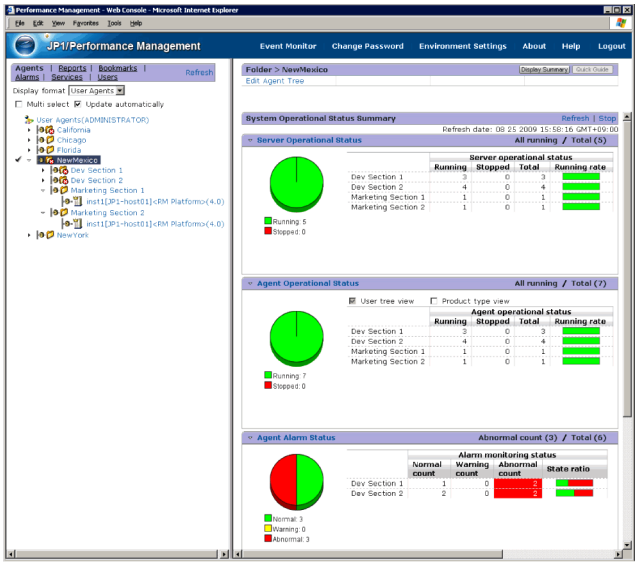


Figure 3-12: Summarized units and ranges for summary display (when a folder is selected)



(6) Printing a summary display

To print a summary display, click the **Stop** button on the System Operation Status Summary Monitoring window and click the **Print** button. An example of the System Operation Status Summary Monitoring print window is shown below.

Figure 3-13: System Operation Status Summary Monitoring print window

3.3.6 Displaying agent properties

You can display the properties of each agent (Collector service) to view settings of data collection intervals and collecting conditions. You cannot change property settings.

To see agent properties:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. From the **Display format** pull-down menu in the navigation frame, choose the

display format for the Agents tree.

The Agents tree appears in the selected display format.

- When **User Agents** is selected:

  The root appears as **User Agents** (*logged-on-user-name*) in the Agents tree.

- When **Products** is selected:

  The root appears as **Products** in the Agents tree.

4. In the Agents tree of the navigation frame, select the agent whose properties you want to display.

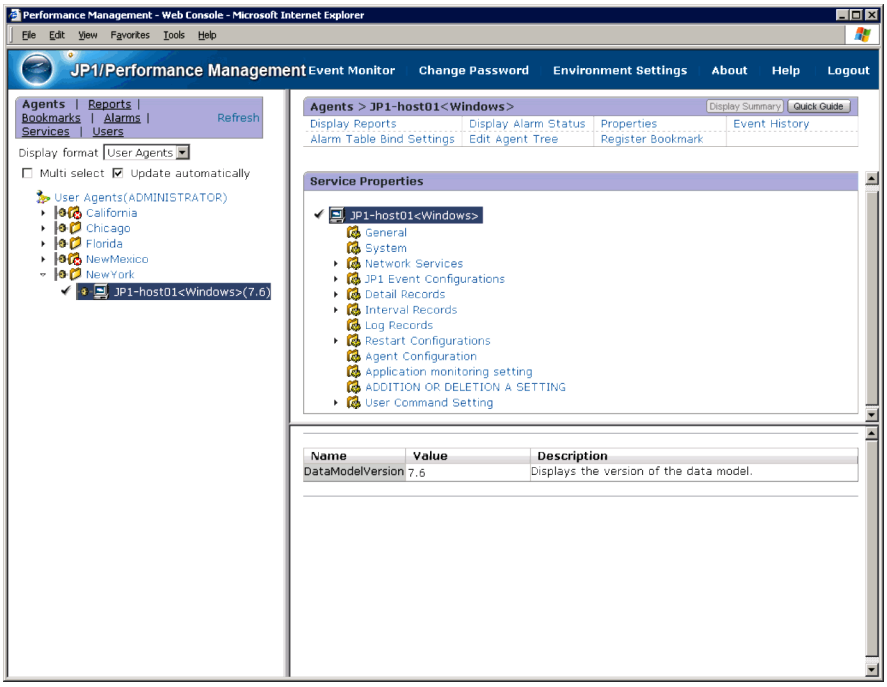
   The selected agent is marked with a checkmark.

5. In the method frame, choose the **Properties** method.

   The Service Properties window appears.

   The following figure shows an example of the Service Properties window.

   Figure 3-14: Example of the Service Properties window



The tree appears at the top of the information frame. The properties of the node selected in the tree appear at the bottom of the information frame, allowing you to view the settings for data collection intervals and conditions.

Displayed property settings differ depending on each agent. For details on property settings, see the appendixes of appropriate agent manual.

3.3.7 Editing agent properties

Users whose accounts have administrator user permissions can modify the properties in the Services window. For details, see *4. Managing Operation Monitoring Data*.

3.3.8 Distributing agent properties as a batch

Agent properties can be distributed as a batch to any services with the same product name and data model version. This feature has the following benefits:

- When managing multiple agents of the same type, you can define the same settings for each agent as a batch
- When you add a new agent, it can be configured with the same settings as existing agents.

The following table lists the nodes whose properties can be distributed as a batch.

Table 3-11: Nodes whose properties can be viewed and selected when performing batch distribution

Service	Node name	Description
Agent Collector and Remote Monitor Collector	JP1 Event Configurations	These nodes contain the properties that define the conditions for issuing JP1 events. For details, see *10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring*.
	Detail Records	These nodes contain the properties that define how performance data is recorded. For details, see *4. Managing Operation Monitoring Data*.
	Interval Records	
	Log Records	
	Restart Configurations	These nodes contain the properties that configure automatic restart of PFM services. For details on automatic restart of PFM services, see *13.4 Using the PFM service automatic restart functionality to restart PFM services*.
	Node count variation property[#1]	These nodes contain the properties for which the number of nodes increases or decreases. The properties subject to batch distribution differ depending on the type of agent. For details, see the appendixes of the appropriate PFM - Agent or PFM - RM manual.

Service	Node name	Description
Agent Store and Remote Monitor Store[#2]	Retention	These nodes contain the properties that define how performance data is stored. For details, see *4. Managing Operation Monitoring Data*.
	RetentionEx	
	Disk Usage	
	Configuration	
Remote agent and group agent	Detail Records[#3]	These nodes contain the properties that define how performance data is recorded. For details, see *4. Managing Operation Monitoring Data*.
	Interval Records[#3]	
	Log Records[#3]	

#1

You must be using version 08-11 or later of PFM - Manager and PFM - Web Console to perform batch distribution of properties for which the number of nodes increases or decreases.

#2

Whether properties can be distributed from one Agent Store or Remote Monitor Store service to another depends on the versions of the Agent Store and Remote Monitor Store services and the Store database serving as the source and destination in the distribution process. For details, see *(2) Property distribution capability by Agent Store and Remote Monitor Store versions*.

#3

Only the Log property can be distributed.

Properties cannot be distributed among the Remote Monitor Collector service and the remote or group agents.

(1) Procedure for distributing agent properties

To distribute agent properties as a batch:

1. From the monitoring console browser, log on to PFM - Web Console.

   Log on to a user account that has administrator user permissions.

   The main window of PFM - Web Console appears. You must have administrator user permissions to use the Services window.

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

The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

   The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by the service ID. For details on the service ID, see the appendix describing service naming rules in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*, and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

   The format of the service ID depends on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4. Select the distribution source agent node.

   You can select any of the following services to be the distribution source node:

   - Agent and Remote Monitor Collector services
   - Agent and Remote Monitor Store services
   - Remote agent
   - Group agent

   The selected node is marked with a checkmark.

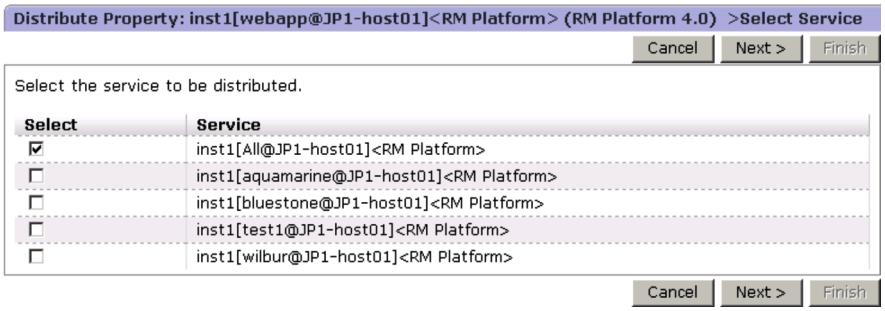
5. In the method frame, select the **Distribute Property** method.

   The Select Service window appears with a list of services available for selection as the distribution destination. The list is populated with services that have the same product name and data model version as the distribution source.

6. Select the distribution destination service.

   The following figure shows an example of selecting the distribution destination service.

Figure 3-15: Example of selecting the distribution destination service



7. Click the **Next** button.

   The Select Property window appears with a list of properties available for distribution to the distribution destination services, along with check boxes for selecting individual properties.

8. Select the properties to distribute.

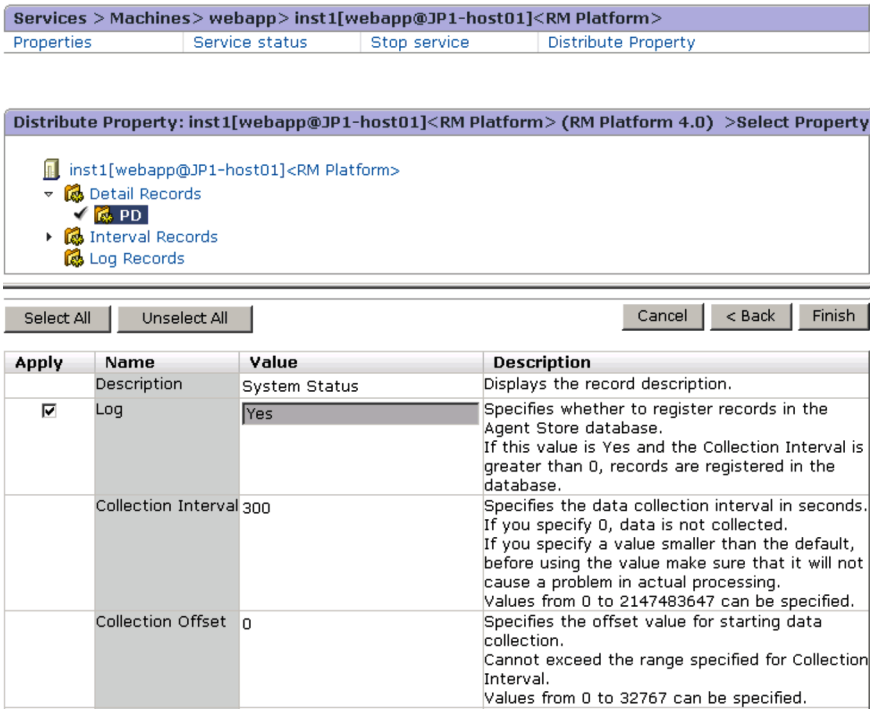
   When you select a node in the tree, a list of the properties you can select appears at the bottom of the information frame.

   Click the **Select All** button to select all of the properties in the list. Click the **Unselect All** button to clear all selections.

   To select a different distribution destination service, click the **Back** button in the Select Property window. This button returns you to the Select Service window where you selected the distribution destination service in step 6.

   The following figure shows an example of setting up property distribution.

Figure 3-16: Example of setting up property distribution



9. Click the **Finish** button.

   The batch distribution process begins, and the Distribute Property > Progress Reports window appears.

   When batch distribution to a service has finished, **OK** appears in the **Property Distribution** column for that service.

   The **OK** button becomes available when batch distribution has finished for all services.

10. Click the **OK** button.

    The contents of the information frame are cleared.

Reference note:

In step 8, you can select additional properties to distribute by repeating the process of selecting another node in the tree and selecting the properties to distribute from that node, before clicking the **Finish** button.

(2) Property distribution capability by Agent Store and Remote Monitor Store versions

Whether properties can be distributed from one Agent Store service to another depends on the versions of the Agent Store and Remote Monitor Store services and the Store database serving as the source and destination in the distribution process. The following table describes whether properties can be distributed between certain versions of the Agent Store and Remote Monitor Store services.

Table 3-12: Property distribution capability by Agent Store and Remote Monitor Store versions

Distribution source Agent Store and Remote Monitor Store	Distribution destination Agent Store and Remote Monitor Store		
	08-00 or earlier	08-11 or later with Store 2.0	08-11 or later with Store 1.0
08-00 or earlier	Y	N	Y
08-11 or later with Store 2.0	N	Y	N
08-11 or later with Store 1.0	Y	N	Y

Legend:

Y: Can be distributed.

N: Cannot be distributed.

(3) Batch distribution of properties for which the number of nodes increases or decreases

Some properties for which the number of nodes increases or decreases can change the structure of the tree by adding or deleting higher-level nodes. For example, nodes below the Application monitoring setting node of PFM - Agent for Platform can change the tree structure by adding or deleting nodes.

This type of property, for which the number of nodes increases or decreases, can be included in batch distribution even when the source and destination of the distribution have different tree structures. You can also choose to match the structure of the distribution destination to that of the distribution source. Note that you must be using version 08-11 or later of PFM - Manager and PFM - Web Console to perform batch distribution of properties for which the number of nodes increases or decreases.

(a) Operations by batch distribution of the properties for which the number of nodes increases or decreases

By using the feature that distributes, in a batch, properties for which the number of nodes increases or decreases, you can operate the Performance Management system in

the following ways:

- Configure all agents identically when building a new system
- Configure all agents identically during operation of the Performance Management system
- Update specific properties on multiple agents during operation of the Performance Management system
- Add a node to multiple agents during operation of the Performance Management system
- Remove a node from multiple agents during operation of the Performance Management system

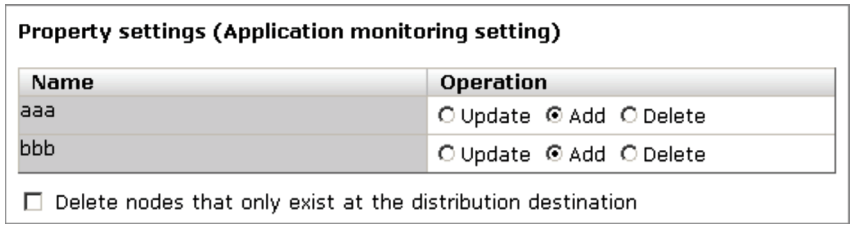
By adding and deleting nodes and setting properties on a single agent, and then distributing the properties of that agent in a batch, you can match the property settings of the distribution destinations including the tree structure to those of the distribution source.

The following provides examples of configuring batch-distribution of agent properties.

For details on how to add or remove nodes from a single agent, see the appropriate PFM - Agent or PFM - RM manual. For details on how to distribute properties in a batch, see *(b) Procedure for batch distribution of properties for which the number of nodes increases or decreases*.

Configuring all agents identically when building a new system:

When configuring batch distribution of agent properties, select the **Add** operation for each node as shown in the figure below.

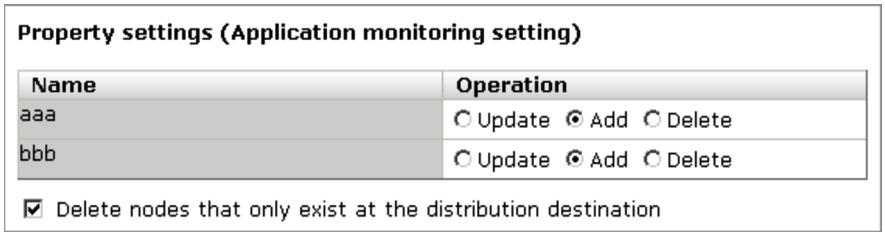


The nodes are added to the distribution destination so that the tree structure mirrors that of the distribution source. The values of the properties all match the values on the distribution source.

Configuring all agents identically during operation of the Performance Management system:

When configuring batch distribution of agent properties, select the **Add** operation for each node as shown in the figure below, and select the **Delete nodes that only**

exist at the distribution destination check box.

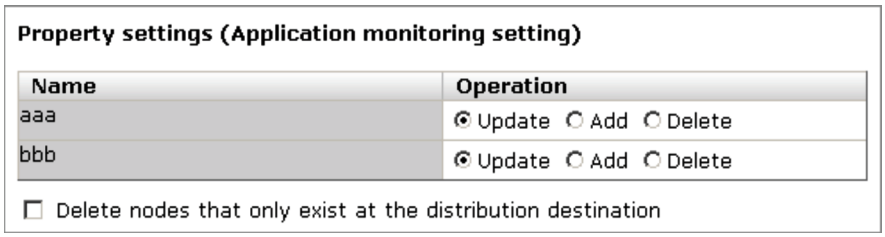


Any nodes that do not exist on the distribution destination agent are added in the distribution process. In this case, the property settings of the added nodes match those of the destination agent. The settings of any node that already exists at the distribution destination agent will match the settings of that node on the source agent. Any nodes that only exist at the distribution destination agent will be removed.

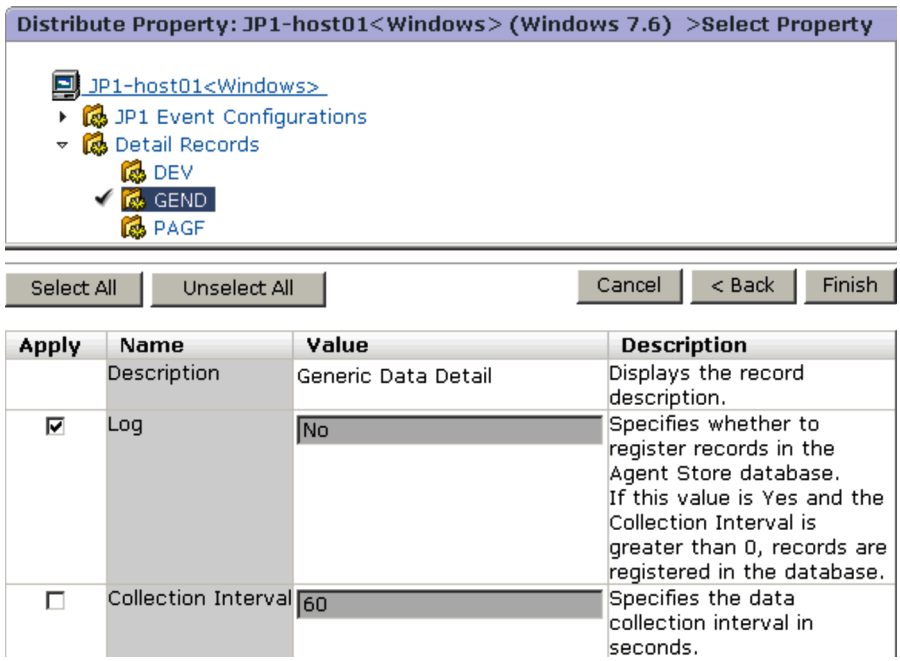
As a result of this process, the tree structure of the distribution destination agent will match that of the distribution source agent.

Updating the value of specific properties on multiple agents during operation of the Performance Management system:

When configuring batch distribution of agent properties, select the **Update** operation for each node as shown in the figure below.



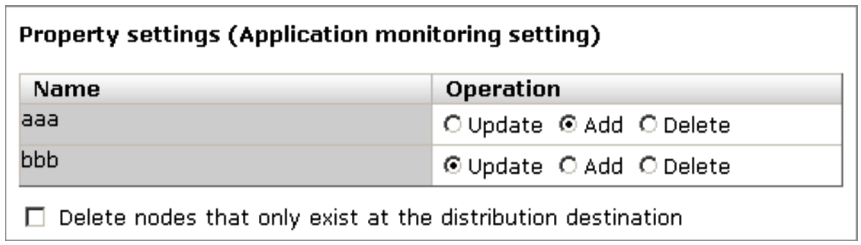
Also, select the **Apply** check box for each property you want to update.



The **Update** operation updates the values of properties with the **Apply** check box selected.

Adding a node to multiple agents during operation of the Performance Management system:

When configuring batch distribution of agent properties, select the **Add** operation for the node you want to add as shown in the figure below.

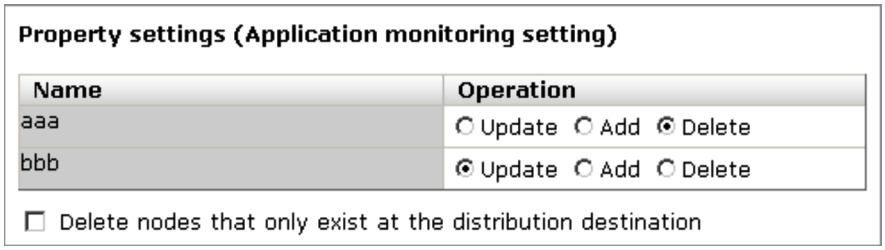


The node is added to the distribution target agent, so that the tree structure mirrors that of the distribution source. The property settings of the added node will match those of the destination agent.

If you perform batch distribution with the **Add** operation selected for a node that exists at the distribution destination, the values of the properties on that node are overwritten regardless of whether the **Apply** check box is selected.

Removing a node from multiple agents during operation of the Performance Management system:

When configuring batch distribution of agent properties, select the **Delete** operation for the node you want to delete as shown in the figure below.



The node for which **Delete** is selected is deleted if it exists at the distribution destination.

Hint:

The **Delete** operation does not delete the corresponding node from the distribution source agent. For this reason, the distribution source and distribution destination agents will have different tree structures after the batch distribution process.

(b) Procedure for batch distribution of properties for which the number of nodes increases or decreases

Use the procedure below to distribute, in a batch, properties for which the number of nodes increases or decreases. This example distributes the tree structure below the Application monitoring setting node available with version 08-11 or later of PFM - Agent for Platform. The following procedure assumes that the properties have been set on the distribution source agent.

1. From the monitoring console browser, log on to PFM - Web Console.

   Log on to a user account that has administrator user permissions.

   The main window of PFM - Web Console appears. You must have administrator user permissions to use the Services window.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

   The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these

folders, the services installed on that host are displayed. The name of each service is represented by a service ID.

4. For PFM - Agent hosts, expand the hierarchy under the folder named for the host running the Agent Store or Agent Collector service whose properties you want to distribute, and select the service to act as the distribution source. For PFM - RM hosts, expand the hierarchy under the folder named for the host running the Remote Monitor Store or Remote Monitor Collector service whose properties you want to distribute, and then select the service to act as the distribution source.

   Because this procedure involves distributing the Application monitoring setting of PFM - Agent for Platform, select an Agent Collector service that begins with `TA`.

   For details on service IDs, see the description of the service naming rules in the appendixes of the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

   The selected Agent Collector service is marked with a checkmark.

5. In the method frame, select the **Distribute Property** method.

   The Select Service window appears with a list of services available for selection as the distribution destination. The list is populated with services that have the same product name and data model version as the distribution source.

6. Select the distribution destination service and click **Next**.

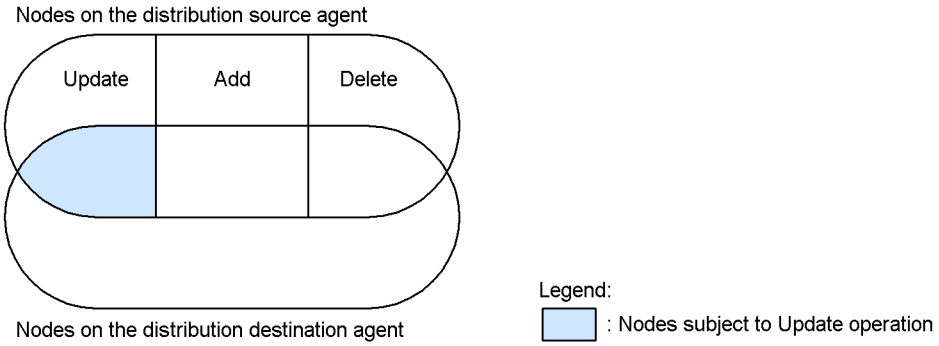
   The Select Property window appears.

7. In the information frame, select **Application monitoring setting** from the tree.

   A list of the nodes under the Application monitoring setting appears at the bottom of the information frame.

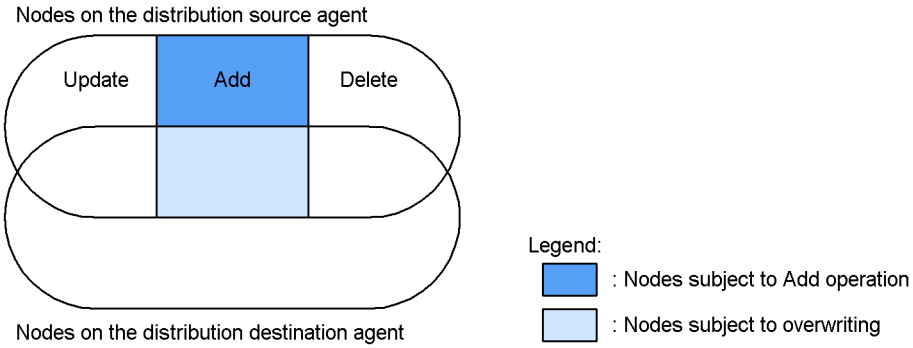
8. Select **Update**, **Add**, or **Delete** for each node.

   The following figure indicates the nodes that are subject to an **Update** operation.



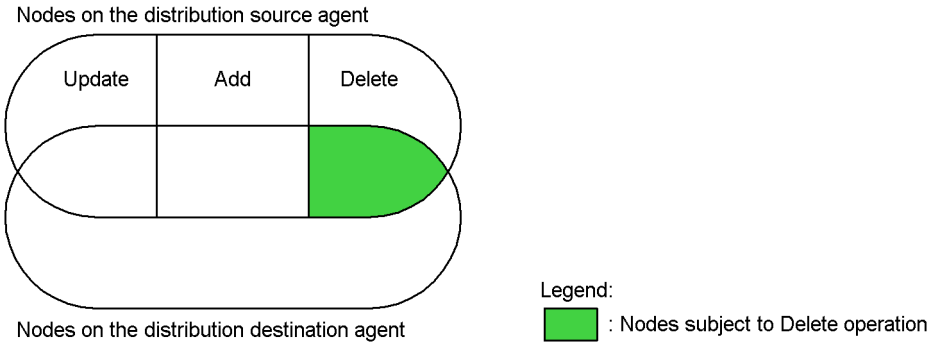
The **Update** operation only updates the values of properties for which the **Apply** check box is selected in step 10.

The following figure indicates the nodes that are subject to an **Add** operation.



If you perform batch distribution with the **Add** operation selected for a node that exists at the distribution destination, the values of the properties on that node are overwritten regardless of whether the **Apply** check box is selected.

The following figure indicates the nodes that are subject to a **Delete** operation.

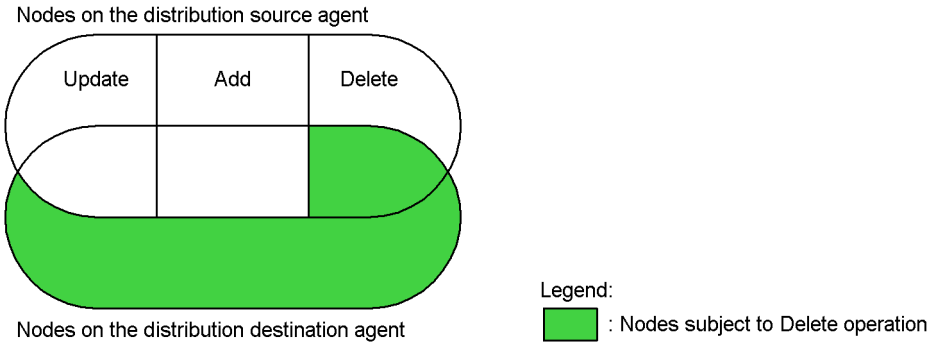


Hint:

The **Delete** operation does not delete the corresponding node from the distribution source agent. For this reason, the distribution source and distribution destination agents will have different tree structures after the batch distribution process.

9. To delete a node that exists on the distribution target agent but not on the distribution source agent, select the **Delete nodes that only exist at the distribution destination** check box.

   The following figure indicates the nodes that are subject to a **Delete** operation when the **Delete nodes that only exist at the distribution destination** check box is selected.



10. For nodes for which you selected **Update** in step 8, select the properties whose values you want to update.

    Select the node in the tree to display a list of properties.

    When the **Update** operation is selected, properties for which the **Apply** check box is selected in the properties list are included in the batch distribution process.

You can select all of the properties in the list by clicking the **Select All** button, and unselect all selected properties by clicking the **Unselect All** button.

11. Click the **Finish** button.

    After selecting the nodes for which to distribute properties and which properties to distribute, click the **Finish** button. The batch distribution process begins, and the Distribute Property > Progress Reports window appears.

    When batch distribution to a service has finished, **OK** appears in the **Property Distribution** column for that service.

    The **OK** button becomes available when batch distribution has finished for all services.

12. Click the **OK** button.

    The contents of the information frame are cleared.

Chapter

4. Managing Operation Monitoring Data

This chapter describes how to manage performance data and event data collected with Performance Management.

4.1 Managing performance data
4.2 Managing event data
4.3 Notes

4.1 Managing performance data

Performance data is collected by an Agent Collector or Remote Monitor Collector service on a monitoring agent and stored in a Store database managed by the Agent Store or Remote Monitor Store service.

You can perform the following operations on performance data (collected by the Agent Collector on the PFM - Agent host or the Remote Monitor Collector service on the PFM - RM host) and the Store database (managed by the Agent Store service on the PFM - Agent host or the Remote Monitor Store service on the PFM - RM host).

- Modify the recording options for performance data
- Modify the retention conditions for performance data (in Store 2.0)
- Modify the retention conditions for performance data (in Store 1.0)
- Distribute the recording options and retention conditions for performance data
- Export performance data
- Check the disk space used for performance data
- Erase performance data
- Initialize the settings for the Store database
- Import backup data (in Store 2.0)
- Convert the data model of backup data (in Store 2.0)
- Display information about the Agent Store and Remote Monitor Store services or backup directory (in Store 2.0)

The steps for each procedure are described below. For details on how to modify the storage location for performance data, see the chapters explaining installation and setup in each PFM - Agent or PFM - RM manual. For further details on the commands used in this section, see the chapter explaining commands in the manual *Job Management Partner 1/Performance Management Reference*.

4.1.1 Modifying the recording options for performance data

You can modify the recording options for performance data collected by Agent Collector and Remote Monitor Collector services. The recording options for performance data include:

- The data to be recorded
- The frequency of data collection
- The offset at which to start collecting data

- Conditional expressions for selecting records to be recorded in the Store database

Each record has specific recording options for performance data. For some records, however, you cannot modify the options. For details, see the description of properties in an appendix of the appropriate PFM - Agent or PFM - RM manual.

You can modify the recording options for performance data in one of two ways:

- By using the monitoring console
- By using commands

Each of these is described below.

(1) Modifying the recording options for performance data by using the monitoring console

To modify the recording options for performance data by using the monitoring console, use the Services window in PFM - Web Console.

To modify the recording options for performance data by using the monitoring console:

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

   You need to log on as a user with administrator user permissions. You must have administrator user permissions to use the Services window.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

   The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID. For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/ Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

   The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4. Expand the hierarchy under the folder with the name of the host for which you want to modify the recording options for performance data, and select a node for

which you want to modify the recording options for performance data.

For PFM - RM, select the node according to which performance data recording option you would like to change. The following table lists the corresponding node to select for the option to be changed.

Table 4-1: Items to be modified and nodes to be selected

Item to be modified	Node to be selected	
	Remote Monitor Collector service	Remote agent or group agent
The data to be recorded	No	Yes
The frequency of data collection	Yes	No
The offset at which to start collecting data	Yes	No
Specifies the condition for registering records in the store database.	Yes	No

Legend:

Yes: Can be selected.

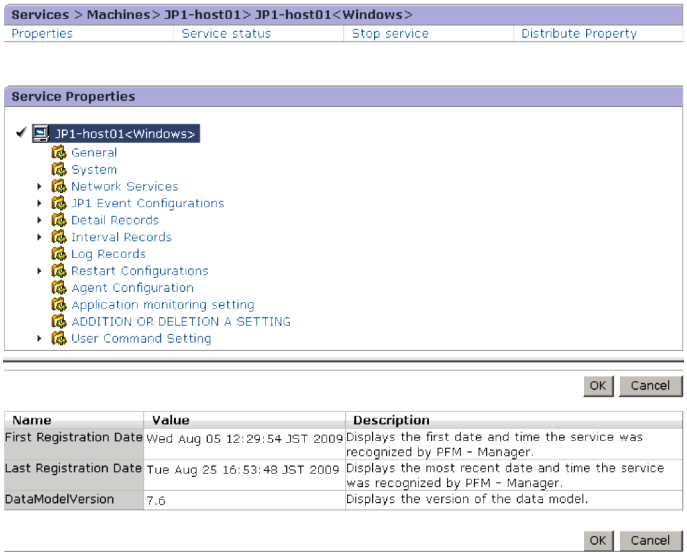
No: Cannot be selected.

The selected node is marked with a checkmark.

5. In the method frame, select **Properties**.

   The Properties window of the selected node is displayed with the properties shown hierarchically.

Figure 4-1: Example of the hierarchy of the properties of a node



The following table lists the record type corresponding to each node.

Table 4-2: Record type corresponding to each node

Node	Record type
Detail Records	PD record type
Interval Records	PI record type
Log Records	PL record type

6. Expand the hierarchy under the node containing the record for which you want to modify the recording options, and select the desired record.

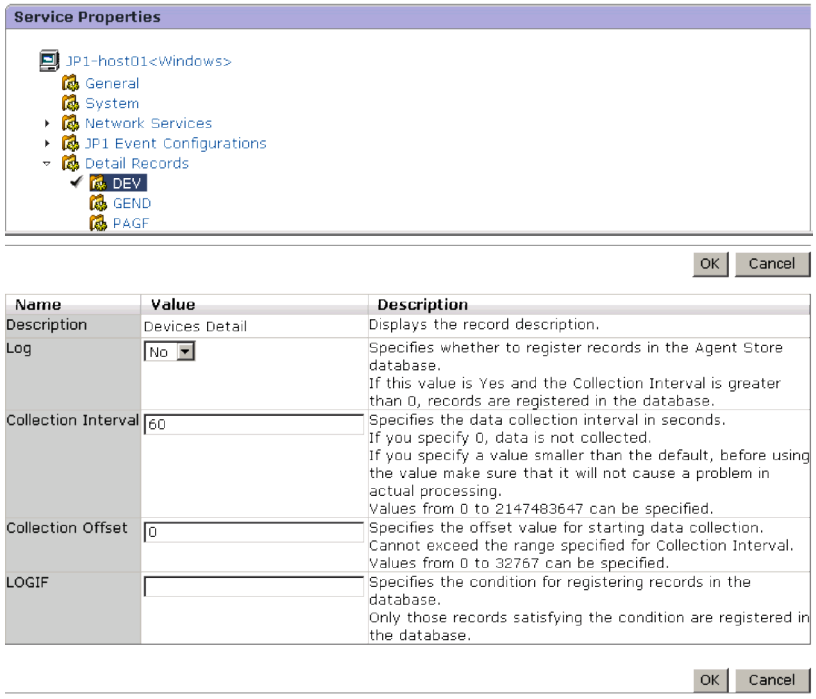
   When you expand the node for a record type, the nodes for records of that record type are displayed. The name of each record is represented by the corresponding record ID without the database ID.

   The selected record is marked with a checkmark and the settings of the specific recording options are displayed at the bottom of the information frame.

7. Modify the definitions of the recording options for the record.

   The properties of the selected record are displayed at the bottom of the information frame.

Figure 4-2: Example of settings for recording options



Modify the property settings. The following table lists descriptions, settings, and nodes that can be modified for each property.

Table 4-3: Description and settings and nodes that can be modified for each property

Property name	Description and settings	Node that can be modified.
Description	Displays the description for the selected record.	--
Log	Specifies whether to record collected records in the Store database. • `Yes`: Records • `No`: Does not record	• Agent Collector • Remote agent • Group agent
Collection Interval#	Specifies a numerical value from 0 to 2,147,483,647 for the interval time for collecting records. The time is in seconds. `0` means that records will not be collected.	• Agent Collector • Remote Monitor Collector

Property name	Description and settings	Node that can be modified.
Collection Offset#	Specifies a numerical value from 0 to 32,767 for the offset at which to start collecting records. The time is in seconds. For example, all records with the offset value of `0` are collected simultaneously each time. A record with the offset value of `20` is collected 20 seconds after the records with the value of `0`.	• Agent Collector • Remote Monitor Collector
Sync Collection With#	A record appears to synchronize collection with.	--
LOGIF	Allows you to specify the conditional expression to use for records to be recorded in the database. Records are recorded according to the condition specified here. Because the condition set here is applied to data stored in the Store database, it does not affect data collection performed by the Agent Collector service or the Remote Monitor Collector service. Click the text box to display the LOGIF Expression Editor window in a separate window. In the LOGIF Expression Editor window, you can create conditional expressions by specifying desired fields, operators, criteria values, and other items. Click the **OK** button to accept the settings, and the conditional expression you have just created is inserted in the LOGIF text box. For further details, see the description for the LOGIF Expression Editor window in the manual *Job Management Partner 1/ Performance Management Reference*.	• Agent Collector • Remote Monitor Collector

Legend:

--: Not applicable

#:

The Sync Collection With property and either the Collection Interval or Collection Offset property are mutually exclusive.

Notes:

- Increasing the number of records for which performance data is collected might affect your disk space or system performance. When you set up records to be collected, make sure you only set those items that are necessary

for monitoring, always considering your requirements for performance data collection, such as the required free disk space and the record collection interval. For information on the required free disk space, see the appendix describing system estimation in the appropriate PFM - Agent or PFM - RM manual. For details on disk space requirements, see the appendix describing system estimation in the appropriate PFM - Agent or PFM - RM manual.

- For the Collection Interval for record collection, either use the default value or specify a value that is both 60 seconds or more and a factor of 3,600. When you have to specify a value that is more than 3,600 seconds (one hour) for the Collection Interval, choose a number that is both a multiple of 3,600 and a factor of 86,400 (24 hours). If the Collection Interval is set to a value less than the default value or to less than 60 seconds, the Agent Collector and Agent Store services on the PFM - Agent host or the Remote Monitor Collector and Remote Monitor Store services on the PFM - RM host might be overloaded, which might make it impossible to save the collected performance data.
- When you modify the value for the Collection Offset, which is the offset value at which to start collecting records, choose a number with the overall load of the data collection in mind.
- Even if the Collection Interval for the PI record type is set to a value that is not a multiple of 60 seconds, the performance data is summarized together with other record types at the same collection times. The seconds portion is discarded and the data is saved with only the minute values.

  Examples:

  When 30 seconds is specified for the Collection Interval:

Collection time	Time of the performance data to be saved
12:01:00 12:01:30 12:02:00 12:02:30	12:01:00 12:01:00 12:02:00 12:02:00

When 90 seconds is specified for the Collection Interval:

Collection time	Time of the performance data to be saved
12:00:00 12:01:30 12:03:00 12:04:30	12:00:00 12:01:00 12:03:00 12:04:00

8. Click the **OK** button.

The settings that you have modified take effect.

Valid values or default values vary with each record. For details on valid values, ranges of values, or default values, see the chapter explaining records in each PFM - Agent or PFM - RM manual.

(2) Modifying the recording options for performance data by using commands

To modify the recording options for collecting performance data in the database, follow these general procedures:

1. Use the `jpcasrec output` command to output the current definitions of the recording options to an XML file.
2. Based on the resulting XML file, modify the definitions of the recording options.
3. Use the `jpcasrec update` command to update the definitions of the recording options with the modified XML file.

Each procedure is described below.

(a) Using the jpcasrec output command to output the definitions of the recording options

On the host where PFM - Web Console is installed, execute the `jpcasrec output` command. The `jpcasrec output` command connects to the agent to obtain the definition information of the recording options for the Store database, and outputs this information to an XML file.

To output the definition of the recording options by using the `jpcasrec output` command:

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

   You need to log on as a special user with special permissions, as shown below:

   - In Windows:

     Administrator permissions

   - In UNIX:

     root user permissions

2. Execute the `jpcmkkey` command.

   Execute the command to create an authentication key file.

   ```
   jpcmkkey -user administrator
   ```

3. Execute the `jpcasrec output` command.

   For example, if you want to output to the parameter file named `asrec.xml` the definition information of the recording options for the Store database of PFM -

Agent with the service ID of *TA1host1*, use the following command:

```
jpcasrec output -o asrec.xml TA1host1
```

When the command is executed, the definition information of the recording options is output to the specified XML file.

An example of this output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "asrec_params.dtd">
<pr-cli-parameters ver="0100">
<agent-store-db-record-definition>
<service id="TA1host1">
<record id="PD_DEV">
<!-- Description : Devices Detail -->
<log>Yes</log>
<collection-interval>60</collection-interval>
<collection-offset>0</collection-offset>
<logif> </logif>
</record>
<record id="PD_GEND">
<!-- Description : Generic Data Detail -->
<log>No</log>
<collection-interval>60</collection-interval>
<collection-offset>0</collection-offset>
<logif> </logif>
</record>
    ...
    ...
    ...
</service>
</agent-store-db-record-definition>
</pr-cli-parameters>
```

(b) Modify the definitions output by the jpcasrec output command

Modify the definitions of the recording options in the XML file generated by the `jpcasrec output` command. You can use any text editor or XML editor to edit the XML file.

The file format and the settings for each tag are described below. Edit the file if necessary.

- Format

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "asrec_params.dtd">
```

```
<pr-cli-parameters ver="0100">
<agent-store-db-record-definition>
    <service id="service-ID">
        <record id="record-ID">
            <!-- Description : Content Index Detail -->
            <log>whether-to-record-in-the-database</log>
            <collection-interval>collection-interval</
collection-interval>
            <collection-offset>offset-at-which-to-start-collection</
collection-offset>
            <logif>
              <and>
                <or>
                 <expression>field-condition-"value"</expression>
                 <expression>field-condition-"value"</expression>
                </or>
                <expression>field-condition-"value"</expression>
                  ...
              </and>
            </logif>
        </record>
          ...
    </service>
</agent-store-db-record-definition>
</pr-cli-parameters>
```

- Definitions

  The XML declaration goes on the first line, and the document type declarations go on the second and third lines. You must write them exactly as shown below:

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE pr-cli-parameters SYSTEM "asrec_params.dtd">
  <pr-cli-parameters ver="0100">
  ```

  The following table describes the tags defined on the forth line and below. These tags must be defined in the order listed in the table.

  Table 4-4: XML definitions

Tag name	Required	Description and settings
`<agent-store-db-record-definition> ... </agent-store-db-record-definition>`	Yes	The root tag of the definition information of the recording options for the Store database.

Tag name	Required	Description and settings
<service id="*service-ID*"> ... </service>	Yes	Specifies the service ID that identifies PFM - Agent or PFM - RM. The service ID of an Agent Collector or Remote Monitor Collector service has an **A** as the second character. For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. A <service> tag contains <record> tags. More than one <service> tag can be specified.
<record id="*record-ID*"> ... </record>	Yes	Specifies the record ID for which you want to modify the recording options. A <record> tag contains <log>, <collection-interval>, <collection-offset>, and <logif> tags. For further details, see *Table 4-5*. More than one <record> tag can be specified.

Legend:

Yes: Must be defined

The following table describes tags contained in a <record> tag (for recording options for a record) and their settings. More than one <record> tag can be specified. Tags contained in a <record> tag must be defined in the order listed in the table.

Table 4-5: Recording options for a record (<record> tag)

Tag name	Required	Settings
<log> ... </log>	No	Specifies whether to record collected performance data in the Store database. One of the following values can be specified: • Yes: Records • No: Does not record Only one <log> tag can be used in a <record> tag.

Tag name	Required	Settings
<collection-interval> ... </collection-interval>	No	Specifies a numerical value from 0 to 2,147,483,647 for the collection interval of performance data. The time is in seconds. 0 means that performance data will not be collected. Only one <collection-interval> tag can be used in a <record> tag.
<collection-offset> ... </collection-offset>	No	Specifies a numerical value from 0 to 32,767 for the offset at which to start collecting performance data. The time is in seconds. 0 means that all performance data will be collected simultaneously. Only one <collection-offset> tag can be used in a <record> tag.
<logif> ... </logif>	No	Allows you to specify a conditional expression to use for recording performance data in the database. For further details, see *Table 4-6*. Only one <logif> tag can be used in a <record> tag.

Legend:

No: Can be omitted

Note that the values for the omitted items are not updated.

Notes:

- Increasing the number of records for which performance data is collected might affect your disk space or system performance. When you set up records to be collected, make sure you only set those items that are necessary for monitoring, always considering your requirements for performance data collection, such as the required free disk space and the record collection interval. For details on the required disk space, see the description of system estimates in an appendix of each PFM - Agent or PFM - RM manual.
- For the Collection Interval for record collection, either use the default value or specify a value that is both 60 seconds or more and a factor of 3,600. When you have to specify a value that is greater than 3,600 seconds (one hour) for the Collection Interval, choose a number that is both a multiple of 3,600 and a factor of 86,400 (24 hours). Specifying a value less than the default value or 60 seconds might increase both the number of open files and the amount of memory use. That would prevent the Store database from functioning

normally, causing the collected performance data to be lost without being saved.

Valid values or default values vary with each record. For details on valid values, ranges of values, or default values, see the chapter explaining records in each PFM - Agent or PFM - RM manual.

- When you modify the value for the Collection Offset, which is the offset value at which to start collecting records, choose a number while keeping in mind the overall load of the data collection.

The following table describes tags contained in a <logif> tag (for conditional expressions for recording in the database), and their settings.

Table 4-6: Conditional expression for recording in the database (<logif> tag)

Tag name	Required	Settings
<and> ... </and>	No	Used to combine two <expression> tags with AND operation when more than one <expression> tag (logical expressions) is used. The two <expression> tags to be combined with AND operation are enclosed in an <and> tag pair. Conditional expressions consist of binary operations that can be nested. More than one <and> tag can be used when more than one <expression> tag is used.
<or> ... </or>	No	Used to combine two <expression> tags with OR operation when more than one <expression> tag (logical expressions) is used. The two <expression> tags to be combined with OR operation are enclosed in an <and> tag pair. Conditional expressions consist of binary operations that can be nested. More than one <or> tag can be used when more than one <expression> tag is used.

Tag name	Required	Settings
<expression> ... </expression>	No	Specifies the condition for determining whether to record to the database. Use the following format: Specifies field condition "*value*" (without any intervening spaces) *field*: Specifies the field to be compared. For details on available fields, see the chapter explaining the records in each PFM - Agent or PFM - RM manual. *condition*: Use one of the operators shown below. Note that you must use <lt; for < and > for > according to XML file conventions. • = The value of the field is equal to the *value*. • < The value of the field is less than the *value*. • <= The value of the field is equal to or less than the *value*. • > The value of the field is more than the *value*. • >= The value of the field is equal to or more than the *value*. • <> The value of the field is not equal to the *value*. *value* Specifies the criteria value to determine whether to record performance data. A valid value can be an integer value, a decimal, or characters of less than 2,049 bytes in length. A valid value varies with the specified field.

Legend:

No: Can be omitted

Note that the values for the omitted items are not updated.

(c) Using the jpcasrec update command to update the definitions of the recording options

On the host where PFM - Web Console is installed, execute the `jpcasrec update` command. The `jpcasrec update` command updates the definition information of the recording options for the Store database with the modified XML file.

To update the definition of the recording options by using the `jpcasrec update` command:

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

   You need to log on as a special user with special permissions, as shown below:

   - In Windows:

     Administrator permissions

   - In UNIX:

     root user permissions

2. Execute the `jpcasrec update` command.

   For example, when you want to update the definition of the recording options based on the contents of the file `asrec.xml`, use the following command:

   ```
   jpcasrec update asrec.xml
   ```

4.1.2 Modifying the retention conditions for performance data (in Store 2.0)

Store 2.0 allows you to modify the retention period for performance data in the retention conditions for performance data recorded in the database.

The following table describes the available retention conditions applicable to each record type.

Table 4-7: Available retention conditions by record type

Record type	Retention condition
PI record type	Retention period of records
PD record type	
PL record type	

You can modify the retention conditions for performance data in one of two ways:

- By using the monitoring console
- By using commands

Each of these is described below.

(1) Modifying the retention conditions for performance data from the monitoring console

To modify the retention conditions for performance data from the monitoring console, use the Services window in PFM - Web Console.

To modify the retention conditions for performance data from the monitoring console:

1. From the monitoring console browser, log on to PFM - Web Console.

   Log on to a user account that has administrator user permissions. You must have administrator user permissions to use the Services window.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

   The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID. The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4. Expand the hierarchy under the folder that has the same name as the host whose retention conditions you want to change, and select an Agent Store or Remote Monitor Store service.

   If the product name display function is enabled, the Agent Store or Remote Monitor Store service is indicated by *host-name*<*service-key*>(Store).

   If the product name display function is not enabled, select an Agent Store or Remote Monitor Store service with an ID that does not begin with a P and has an S as the second character. (Service IDs that begin with PS refer to a Master Store service.)

   For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

   The selected Agent Store or Remote Monitor Store service is marked with a checkmark.

5. In the method frame, select the **Properties** method.

   The Properties window of the Agent Store or Remote Monitor Store service appears with the properties shown hierarchically.

6. Select the **RetentionEx** node.

   At the bottom of the information frame, the properties of the **RetentionEx** node are displayed.

   Figure 4-3: Example of setting retention conditions

PI record

Name	Value	Description
Period - Minute Drawer (Day)	1	Specifies the retention period for minute-by-minute performance data in days. Values from 0 to 366 can be specified.
Period - Hour Drawer (Day)	7	Specifies the retention period for hourly performance data in days. Values from 0 to 366 can be specified.
Period - Day Drawer (Week)	54	Specifies the retention period for daily performance data in weeks. Values from 0 to 522 can be specified.
Period - Week Drawer (Week)	54	Specifies the retention period for weekly performance data in weeks. Values from 0 to 522 can be specified.
Period - Month Drawer (Month)	12	Specifies the retention period for monthly performance data in months. Values from 0 to 120 can be specified.
Period - Year Drawer (Year)	10	Displays the retention period for yearly performance data in years.

PD or PL record

Name	Value	Description
Period (Day)	10	Specifies the retention period for performance data in days. Values from 0 to 366 can be specified.

You can modify the property settings. The following table gives a description of each property and lists the available settings.

Table 4-8: Description and settings for each property

Record type	Node name	Property name	Settings
PI record type	Product Interval - *record-ID-of-PI-record-type*	Period - Minute Drawer (Day)	The retention period for performance data collected on a per-minute basis for each record ID of PI-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.
		Period - Hour Drawer (Day)	The retention period for performance data collected on an hourly basis for each record ID of PI-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.

Record type	Node name	Property name	Settings
		Period - Day Drawer (Week)	The retention period for performance data collected on a daily basis for each record ID of PI-type records. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
		Period - Week Drawer (Week)	The retention period for performance data collected on a weekly basis for each record ID of PI-type records. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
		Period - Month Drawer (Month)	The retention period for performance data collected on a monthly basis for each record ID of PI-type records. Specify the retention period (in months) as an integer in the range from 0 to 120.
		Period - Year Drawer (Year)	The retention period for performance data collected on a yearly basis for each record ID of PI-type records. No retention period applies to data collected on a yearly basis.
PD record type	Product Detail - *record-ID-of-PD-record-type*	Period (Day)	The retention period for performance data for each record ID of PD-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.
PL record type	Product Log - *record-ID-of-PL-record-type*	Period (Day)	The retention period for performance data for each record ID of PL-type records. Specify the retention period (in days) as an integer in the range from 0 to 366.

7. Click the **OK** button.

   The new settings take effect.

(2) Modifying the retention conditions for performance data by using commands

To modify the retention conditions for performance data by using commands, follow these general procedures:

1. Use the `jpcaspsv output` command to output the current definitions of the retention conditions to an XML file.
2. Based on the resulting XML file, modify the definitions of the retention conditions.
3. Use the `jpcaspsv update` command to update the definitions of the retention conditions from the modified XML file.

Each procedure is described below.

(a) Using the jpcaspsv output command to output the definition of the retention conditions

On a host where PFM - Web Console is installed, execute the `jpcaspsv output` command. The `jpcaspsv output` command connects to the agent to obtain the definition information for retention conditions in the Store database and outputs this information to an XML file.

To output the definition of the retention conditions by using the `jpcaspsv output` command:

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

   Log on as a user with the following permissions:

   - In Windows:

     Administrator permissions

   - In UNIX:

     root user permissions

2. Execute the `jpcaspsv output` command.

   For example, when you want to output the definition information of the retention conditions for the Store database of PFM - Agent with the service ID of `TS1host1` to the parameter file named `aspsv.xml`, use the following command:

   ```
   jpcaspsv output -o aspsv.xml TS1host1
   ```

   When the command is executed, the definition information of the retention conditions is output to the specified XML file.

   An example of this output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
<service id="TS1host1">
<ex-product-interval>
<ex-interval-record id="PI">
<minute-drawer-days period="10"/>
<hour-drawer-days period="10"/>
<day-drawer-weeks period="10"/>
<week-drawer-weeks period="10"/>
<month-drawer-months period="10"/>
<!-- year-drawer-years period="10" -->
</ex-interval-record>
                :
</ex-product-interval>
<ex-product-detail>
<ex-detail-record id="PD" period="10"/>
<ex-detail-record id="PD_THRD" period="10"/>
<ex-detail-record id="PD_ADRS" period="10"/>
<ex-detail-record id="PD_PDI" period="10"/>
<ex-detail-record id="PD_PEND" period="10"/>
</ex-product-detail>
<ex-product-log>
<ex-log-record id="PL" period="10"/>
<ex-log-record id="RM" period="10"/>
</ex-product-log>
</service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>
```

(b) Modify the definitions output by the jpcaspsv output command

Modify the definitions of the recording options in the XML file generated by the `jpcaspsv output` command. You can use any text editor or XML editor to edit the XML file.

The file format and the settings for each tag are described below. Edit the file as required.

- Format:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
    <service id="service-ID">
        <ex-product-interval>
            <ex-interval-record id="record-ID">
```

```
                <minute-drawer-days
period="retention-period-for-per-minute-data"/>
                <hour-drawer-days
period="retention-period-for-hourly-data"/>
                <day-drawer-weeks
period="retention-period-for-daily-data"/>
                <week-drawer-weeks
period="retention-period-for-weekly-data"/>
                <month-drawer-months
period="retention-period-for-monthly-data"/>
                <!-- year-drawer-years period="10" -->#
            </ex-interval-record>
        </ex-product-interval>
        <ex-product-detail>
            <ex-detail-record id="record-ID"
period="record-retention-period"/>
                :
                :
        </ex-product-detail>
        <ex-product-log>
            <ex-log-record id="record-ID"
period="record-retention-period"/>
                :
        </ex-product-log>
    </service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>
```

You cannot set a retention period for yearly records.

- Definitions:

The XML declaration goes on the first line, and the document type declarations go on the second and third lines. You must write them exactly as shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
```

The following table describes the tags defined on the forth line and below. These tags must be defined in the order listed in the table.

Table 4-9: XML definitions

Tag name	Required	Description and settings
<agent-store-db-preserve-definition> ...</ agent-store-db-preserve-definition>	Yes	The root tag of the definition information of the retention conditions for the Store database.
<service id="*service-ID*"> ... </ service>	Yes	Specifies the service ID that identifies PFM - Agent or PFM - RM. Specify a service with an ID that does not begin with a **P** but has an **S** as the second character. (Service IDs that begin with **PS** refer to a Master Store service.) For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. A <service> tag contains <ex-product-interval>, <ex-product-detail>, and <ex-product-log> tags. More than one <service> tag can be specified.
<ex-product-interval> ...</ ex-product-interval>	No	Specifies the retention period of PI-type records. It contains <minute-drawer-days period=*retention-period-for-per-minute-data*>, <hour-drawer-days period=*retention-period-for-hourly-data*>, <day-drawer-weeks period=*retention-period-for-daily-data*>, <week-drawer-weeks period=*retention-period-for-weekly-data*>, and <month-drawer-months period=*retention-period-for-monthly-data*> tags. For further details, see Table 4-10 Retention periods for PI-type records (<ex-product-interval> tag). You can specify more than one <ex-product-interval> tag in a <service> tag.
<ex-product-detail> ...</ ex-product-detail>	No	Specifies the maximum number of stored records for the PD record type. It contains <ex-detail-record> tags. Only one <ex-product-detail> tag can be used in a <service> tag. For further details, see Table 4-11 Retention periods for PD-type records (<ex-product-detail> tag).

Tag name	Required	Description and settings
<ex-product-log> ...</ ex-product-log>	No	Specifies the maximum number of stored records for the PL record type. It contains <ex-log-record> tags. For further details, see Table 4-12 Retention periods for PL-type records (<ex-product-log> tag). Only one <ex-product-log> tag can be used in a <service> tag.

Legend:

Yes: Must be defined

No: Can be omitted

Note that the values for any omitted items are not updated.

The following table describes the tags contained in an <ex-product-interval> tag (for the retention period of PI-type records) and their settings. Tags contained in an <ex-product-interval> tag must be defined in the order listed in the table.

Table 4-10: Retention periods for PI-type records (<ex-product-interval> tag)

Tag name	Required	Description and settings
<minute-drawer-days period="*retention-period-for-per-minute-data*">	No	Sets the retention period for performance data collected on a per-minute basis. Specify the retention period (in days) as an integer in the range from 0 to 366.
<hour-drawer-days period="*retention-period-for-hourly-data*">	No	Sets the retention period for performance data collected on an hourly basis. Specify the retention period (in days) as an integer in the range from 0 to 366.
<day-drawer-weeks period="*retention-period-for-daily-data*">	No	Sets the retention period for performance data collected on a daily basis. Specify the retention period (in weeks) as an integer in the range from 0 to 522.

Tag name	Required	Description and settings
<week-drawer-weeks period="*retention-period-for-weekly-data*">	No	Sets the retention period for performance data collected on a weekly basis. Specify the retention period (in weeks) as an integer in the range from 0 to 522.
<month-drawer-months period="*retention-period-for-monthly-data*">	No	Sets the retention period for performance data collected on a monthly basis. Specify the retention period (in months) as an integer in the range from 0 to 120.

Legend:

No: Can be omitted

Note that the values for any omitted items are not updated.

The following table describes the tags contained in an <ex-product-detail> tag (for the retention period of PD-type records) and their settings.

Table 4-11: Retention periods for PD-type records (<ex-product-detail> tag)

Tag name	Required	Description and settings
<ex-detail-record id="*record-ID*" period="*retention-period-for-specified-record*"/>	No	Specifies the retention period for a specific PD-type record. Specify the retention period (in days) as an integer in the range from 0 to 366. Only one <ex-detail-record> tag can be specified for each PD record.

Legend:

No: Can be omitted

Note that the values for any omitted items are not updated.

The following table describes the tags contained in an <ex-product-log> tag (for the retention period of PL-type records) and their settings.

Table 4-12: Retention periods for PL-type records (<ex-product-log> tag)

Tag name	Required	Description and settings
`<ex-log-record id="`*record-ID*`" period="`*retention-period-for-specified-record*`"/>`	No	Specifies the retention period for a specific PL-type record. Specify the retention period (in days) as an integer in the range from 0 to 366. Only one `<ex-log-record>` tag can be specified for each PL record.

Legend:

No: Can be omitted

Note that the values for any omitted items are not updated.

(c) Using the jpcaspsv update command to update the definitions of the retention conditions

On the host where PFM - Web Console is installed, execute the `jpcaspsv update` command. The `jpcaspsv update` command updates the definition information of the retention conditions for the Store database from the modified XML file.

To update the definitions of the retention conditions by using the `jpcaspsv update` command:

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

   Log on as a user with the following permissions:

   - In Windows:

     Administrator permissions

   - In UNIX:

     root user permissions

2. Execute the `jpcaspsv update` command.

   For example, if you want to update the definition information with the retention conditions specified in the file `aspsv.xml`, use the following command:

   ```
   jpcaspsv update aspsv.xml
   ```

4.1.3 Modifying the retention conditions for performance data (in Store 1.0)

In the retention conditions for performance data recorded in the database, you can modify the retention period of data or the maximum number of records. The kind of

retention condition allowed for performance data depends on the type of record.

The following table describes the available retention conditions applicable to each record type.

Table 4-13: Available retention conditions for each record type

Record type	Available retention condition
PI record type	Retention period of data
PD record type	Maximum number of records
PL record type	

You can modify the retention conditions for performance data in one of two ways:

- By using the monitoring console
- By using commands

Each of these is described below.

(1) Modifying the retention conditions for performance data by using the monitoring console

To modify the retention conditions for performance data by using the monitoring console, use the Services window in PFM - Web Console.

To modify the retention condition for performance data by using the monitoring console:

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

   You need to log on as a user with Administrator user permissions. You must have administrator user permissions to use the Services window.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

   The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by a service ID. The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance*

Management Planning and Configuration Guide.

4. Expand the hierarchy under the folder with the name of the host for which you want to modify the retention conditions, and select an Agent Store service.

   If the product name display function is enabled, the Agent Store service is indicated by *host-name*<*service-key*>(Store).

   If the product name display function is not enabled, select an Agent Store service with an ID that does not begin with a P and has an S as the second character. (Service IDs that begin with PS refer to a Master Store service.)

   For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent manual.

   The selected Agent Store service is marked with a checkmark.

5. In the method frame, select **Properties**.

   The Properties window of the Agent Store service is displayed with the properties shown hierarchically.

6. Select the **Retention** node.

   At the bottom of the information frame, the properties of the **Retention** node are displayed.

   Figure 4-4: Example settings for retention conditions

Name	Value	Description
Product Interval - Minute Drawer	Day	Specifies the minute-by-minute record retention period for PI-type records.
Product Interval - Hour Drawer	Week	Specifies the hourly record retention period for PI-type records.
Product Interval - Day Drawer	Year	Specifies the daily record retention period for PI-type records.
Product Interval - Week Drawer	Year	Specifies the weekly record retention period for PI-type records.
Product Interval - Month Drawer	Year	Specifies the monthly record retention period for PI-type records.
Product Interval - Year Drawer	Year	Displays the yearly record retention period for PI-type records.
Product Detail - PD	10000	Specifies the number of records retained for each PD-type record. Values from 0 to 2147483647 can be specified.
Product Detail - HC	10000	Specifies the number of records retained for each PD-type record. Values from 0 to 2147483647 can be specified.
Product Detail - HOST	10000	Specifies the number of records retained for each PD-type record. Values from 0 to 2147483647 can be specified.

   You can modify the property settings. The following table lists descriptions and settings for each property.

Table 4-14: Description and settings for each property

Record type	Property name	Settings
PI record type	Product Interval - Minute Drawer	Specifies a retention period (in minutes) for the stored performance data. You can select one of the following items in the pull-down menu: • **Minute** • **Hour** • **Day** • **2 Days** • **3 Days** • **4 Days** • **5 Days** • **6 Days** • **Week** • **Month** • **Year**
	Product Interval - Hour Drawer	Specifies a retention period (in hours) for the stored performance data. You can select one of the following items in the pull-down menu: • **Hour** • **Day** • **2 Days** • **3 Days** • **4 Days** • **5 Days** • **6 Days** • **Week** • **Month** • **Year**
	Product Interval - Day Drawer	Specifies a retention period (in days) for the stored performance data. You can select one of the following items in the pull-down menu: • **Day** • **2 Days** • **3 Days** • **4 Days** • **5 Days** • **6 Days** • **Week** • **Month** • **Year**

Record type	Property name	Settings
	Product Interval - Week Drawer	Specifies a retention period (in weeks) for the stored performance data. You can select one of the following items in the pull-down menu: • **Week** • **Month** • **Year**
	Product Interval - Month Drawer	Specifies a retention period (in months) for the stored performance data. You can select one of the following items in the pull-down menu: • **Month** • **Year**
	Product Interval - Year Drawer	The retention period, in years, for the stored performance data. The setting defaults to **Year** and cannot be modified.
PD record type	Product Detail - *record-ID-of-PD-record-type*	Specifies the maximum number of stored records for each record ID of PD record type. For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records. For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines.
PL record type	Product Log - *record-ID-of-PL-record-type*	Specifies the maximum number of stored records for each record ID of PL record type. For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records. For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines.

7. Click the **OK** button.

   Your settings are enabled.

(2) Modifying the retention condition for performance data by using commands

To modify the retention conditions for performance data recorded in the database, follow these general procedures:

1. Use the `jpcaspsv output` command to output the current definitions of the retention conditions to an XML file.
2. Based on the resulting XML file, modify the definitions of the retention conditions.
3. Use the `jpcaspsv update` command to update the definitions of the retention conditions with the modified XML file.

Each procedure is described below.

(a) Using the jpcaspsv output command to output the definition of the retention condition

On a host where PFM - Web Console is installed, execute the `jpcaspsv output` command. The `jpcaspsv output` command connects to the agent to obtain the definition information for retention conditions in the Store database and outputs this information to an XML file.

To output the definition of the retention condition by using the `jpcaspsv output` command:

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

   You need to log on as a special user with special permissions, as shown below:

   - In Windows:

     Administrator permissions

   - In UNIX:

     root user permissions

2. Execute the `jpcaspsv output` command.

   For example, when you want to output to the parameter file named `aspsv.xml` the definition information of the retention conditions for the Store database of PFM - Agent with the service ID of `TS1host1`, use the following command:

   ```
   jpcaspsv output -o aspsv.xml TS1host1
   ```

   When the command is executed, the definition information of the retention conditions is output to the specified XML file.

   An example of this output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
<service id="TS1host1">
<product-interval>
<minute-drawer>Day</minute-drawer>
<hour-drawer>Week</hour-drawer>
<day-drawer>Year</day-drawer>
<week-drawer>Year</week-drawer>
<month-drawer>Year</month-drawer>
<!-- year-drawer : Year -->
</product-interval>
<product-detail>
<detail-record id="PD" max-rec="10000"/>
<detail-record id="PD_PDI" max-rec="100000"/>
<detail-record id="PD_PEND" max-rec="10000"/>
<detail-record id="PD_PAGF" max-rec="10000"/>
<detail-record id="PD_GEND" max-rec="10000"/>
<detail-record id="PD_SVC" max-rec="10000"/>
<detail-record id="PD_DEV" max-rec="10000"/>
<detail-record id="PD_ELOG" max-rec="10000"/>
</product-detail>
</service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>
```

(b) Modify the definitions output by the jpcaspsv output command

Modify the definitions of the recording options in the XML file generated by the `jpcaspsv output` command. You can use any text editor or XML editor to edit the XML file.

The file format and the settings for each tag are described below. Edit the file if necessary.

- Format:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
<agent-store-db-preserve-definition>
    <service id="service-ID">
        <product-interval>
            <minute-drawer>retention-period-in-minutes</minute-drawer>
             <hour-drawer>retention-period-in-hours</hour-drawer>
             <day-drawer>retention-period-in-days</day-drawer>
             <week-drawer>retention-period-in-weeks</week-drawer>
```

```
            <month-drawer>retention-period-in- months</month-drawer>
            <!-- year-drawer : Year -->#
        </product-interval>
        <product-detail>
            <detail-record id="record-ID"
max-rec="maximum-number-of-records"/>
            ...
            ...
        </product-detail>
        <product-log>
            <log-record id="record-ID"
max-rec="maximum-number-of-records"/>
            ...
        </product-log>
    </service>
</agent-store-db-preserve-definition>
</pr-cli-parameters>

# The retention period in years defaults to Year and cannot be
modified.
```

■ Definitions:

The XML declaration goes on the first line, and the document type declaration goes on the second and third lines. You must write them exactly as shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pr-cli-parameters SYSTEM "aspsv_params.dtd">
<pr-cli-parameters ver="0110">
```

The following table describes the tags defined on the forth line and below. These tags must be defined in the order listed in the table.

Table 4-15: XML definitions

Tag name	Required	Description and settings
<agent-store-db-preserve-definition> ... </agent-store-db-preserve-definition>	Yes	The root tag of the definition information of the retention conditions for the Store database.

Tag name	Required	Description and settings
<service id="*service- ID*"> ... </service>	Yes	Specifies the service ID that identifies PFM - Agent. Specify a service with an ID that does not begin with a **P** but has an **S** as the second character. (Service IDs that begin with **PS** refer to a Master Store service.) For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*. A <service> tag contains <product-interval>, <product-detail>, and <product-log> tags. More than one <service> tag can be specified.
<product-interval> ... </product-interval>	No	The tag that specifies the retention period of records for the PI record type. It contains <minute-drawer>, <hour-drawer>, <day-drawer>, <week-drawer>, and <month-drawer> tags. For further details, see Table 4-16 Retention period of the records for the PI record type (<product-interval> tag). Only one <product-interval> tag can be used in a <service> tag.
<product-detail> ... </product-detail>	No	The tag that specifies the maximum number of stored records for the PD record type. It contains <detail-record> tags. Only one <product-detail> tag can be used in a <service> tag. For further details, see Table 4-17 The Maximum number of stored records for the PD record type (<product-detail> tag).
<product-log> ... </product-log>	No	The tag that specifies the maximum number of stored records for the PL record type. It contains <log-record> tags. For further details, see Table 4-18 The Maximum number of stored records for the PL record type (<product-log> tag). Only one <product-log> tag can be used in a <service> tag.

Legend:

Yes: Must be defined

No: Can be omitted

Note that the values for the omitted items are not updated.

The following table describes tags contained in a <product-interval> tag (for the retention period of records for the PI record type) and their settings. Tags contained in a <product-interval> tag must be defined in the order listed in the table.

Table 4-16: Retention period of the records for the PI record type (<product-interval> tag)

Tag name	Required	Settings
<minute-drawer> ... </minute-drawer>	No	Specifies a retention period (in minutes) for the stored performance data. One of the following values can be specified: • Minute: one minute • Hour: one hour • Day: one day • *n* Days: *n* days (*n* = 2-6) • Week: one week • Month: one month • Year: one year Only one <minute-drawer> tag can be used in a <product-interval> tag.
<hour-drawer> ... </hour-drawer>	No	Specifies a retention period (in hours) for the stored performance data. One of the following values can be specified: • Hour: one hour • Day: one day • *n* Days: *n* days (*n* = 2-6) • Week: one week • Month: one month • Year: one year Only one <hour-drawer> tag can be used in a <product-interval> tag.

Tag name	Required	Settings
<day-drawer> ... </day-drawer>	No	Specifies a retention period (in days) for the stored performance data. One of the following values can be specified: • Day: one day • *n* Days: *n* days (*n* = 2-6) • Week: one week • Month: one month • Year: one year Only one <day-drawer> tag can be used in a <product-interval> tag.
<week-drawer> ... </week-drawer>	No	Specifies a retention period (in weeks) for the stored performance data. One of the following values can be specified: • Week: one week • Month: one month • Year: one year Only one <week-drawer> tag can be used in a <product-interval> tag.
<month-drawer> ... </month-drawer>	No	Specifies a retention period (in months) for the stored performance data. One of the following values can be specified: • Month: one month • Year: one year Only one <month-drawer> tag can be used in a <product-interval> tag.

Legend:

No: Can be omitted.

Note that the values for the omitted items are not updated.

The following table describes tags contained in a <product-detail> tag (for the maximum number of stored records for the PD record type) and their settings.

Table 4-17: The Maximum number of stored records for the PD record type (<product-detail> tag)

Tag name	Required	Settings
`<detail-record id="`*record-ID*`" max-rec="`*maximum-number-of-records*`"/>`	No	Specifies the maximum number of stored records for each record ID of PD record type. For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records. For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines. Only one `<detail-record>` tag can be used for a PD record.

Legend:

No: Can be omitted

Note that the values for the omitted items are not updated.

The following table describes tags contained in a `<product-log>` tag (for the maximum number of stored records for the PL record type) and their settings.

Table 4-18: The Maximum number of stored records for the PL record type (<product-log> tag)

Tag name	Required	Settings
`<log-record id="`*record-ID*`" max-rec="`*maximum-number-of-records*`"/>`	No	Specifies the maximum number of stored records for each record ID of PL record type. For a single instance: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of stored records. For multiple instances: You can specify a numerical value from 0 to 2,147,483,647 for the maximum number of total stored record lines. Only one `<log-record>` tag can be used for a PL record.

Legend:

No: Can be omitted

Note that the values for the omitted items are not updated.

(c) Using the jpcaspsv update command to update the definitions of the retention conditions

On the host where PFM - Web Console is installed, execute the `jpcaspsv update` command. The `jpcaspsv update` command updates the definition information of the retention conditions for the Store database with the modified XML file.

To update the definitions of the retention conditions by using the `jpcaspsv update` command:

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

   You need to log on as a special user with special permissions, as shown below:

   - In Windows:

     Administrator permissions

   - In UNIX:

     root user permissions

2. Execute the `jpcaspsv update` command.

   For example, if you want to update the definition information with the retention conditions specified in the file named `aspsv.xml`, use the following command:

   ```
   jpcaspsv update aspsv.xml
   ```

4.1.4 Exporting performance data

You can export the performance data stored in the Store database to a text file. Use the `jpctool db dump` command to export data.

The purpose of this command is to output performance data to a text file. The file it creates cannot be imported using the `jpctool db import` command.

To export performance data:

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool service list` command to make sure that the Name Server, Master Manager, and Master Store services are running.
3. Execute the `jpctool db dump` command.

   For example, if you want to export to the file named `pcsr.out` that contains the performance data collected from 02:00:00 (GMT) to 14:59:00 (GMT) on July 10, 2006, which is stored in the Processor Overview (PI_PCSR) record on PFM - Agent for Platform (Windows) host *host02*, use the following command:

```
jpctool db dump -id TS* -host host02 -stime 2006/07/10 02:00
-etime 2006/07/10 14:59 -f pcsr.out -dbid PI -rec PCSR
```

When the command finishes normally, the export file for the performance data is created in the following location:

On physical hosts:

- In Windows:

  environment-directory\jp1pc\xxxx[#1]\store[*instance-name*][#2]\dump\pcsr.out

- In UNIX:

  environment-directory/jp1pc/xxxx[#1]/store[/*instance-name*][#2]/dump/pcsr.out

#1

xxxx indicates the service key of PFM - Agent or PFM - RM. Every PFM - Agent or PFM - RM has a specific service key, such as `agto` for PFM - Agent for Oracle and `agtt` for PFM - Agent for Platform (Windows). For details on service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

If PFM - Agent or PFM - RM is monitoring an application program that can start multiple service sets on a host, there is one more directory created under the `Store` directory bearing the same name as the instance name.

4.1.5 Checking the disk space used for performance data

You can use the Services window of PFM - Web Console to check the disk space used by the Store database.

To check the disk space used for performance data:

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

   You need to log on as a user with Administrator user permissions. You must have administrator user permissions to use the Services window.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **Machines** folder.

   The hierarchy displays folders with the same names as the hosts where Performance Management services are installed. When you expand one of these folders, the services installed on that host are displayed. The name of each service is represented by the service ID. The service ID format differs depending on whether the product name display function is enabled. For details on the product name display function, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4. Select an Agent Store or Remote Monitor Store service in the folder with the same name as the host for which you want to check the disk space.

   If the product name display function is enabled, the Agent Store or Remote Monitor Store service is indicated by *host-name*<*service-key*>(Store).

   If the product name display function is not enabled, an Agent Store or Remote Monitor Store service is indicated by the service with an ID that does not begin with a P and has an S as the second character. (Service IDs that begin with PS refer to a Master Store service.)

   For details on service IDs, see the description of the service naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide* and the list of identifiers described in the appropriate PFM - Agent or PFM - RM manual.

   The selected Agent Store or Remote Monitor Store service is marked with a checkmark.

5. In the method frame, select **Properties**.

   The Properties window of the Agent Store or Remote Monitor Store service appears with the properties shown hierarchically.

6. Select the **Disk Usage** node.

   The disk space used by the database under the control of the Agent Store or Remote Monitor Store service is displayed at the bottom of the Properties window.

   Figure 4-5: Example of disk space display (performance data)

Name	Value	Description
Product Interval	0	Displays the disk capacity used by PI-type records.
Product Detail	0	Displays the disk capacity used by PD-type records.
Product Alarm	4.0 KB	Displays the disk capacity used by PA-type records.
Product Log	0	Displays the disk capacity used by PL-type records.
Total Disk Usage	4.0 KB	Displays the disk capacity used by the entire database.

4.1.6 Erasing performance data

You can erase the performance data that you no longer need from the Store database. Use the `jpctool db clear` command to erase data in the Store database.

Note:

You must execute the `jpctool db clear` command on the host where PFM - Manager is installed.

To erase performance data:

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

   You need to log on with special user permissions, as shown below:

   - In Windows:

     Administrators or Backup Operators permissions

   - In UNIX:

     root user permissions

2. Execute the `jpctool service list` command to make sure that the Agent Store or Remote Monitor Store service managing the Store database from which you want to erase the performance data is up and running.

3. Execute the `jpctool db clear` command to erase the specified record type of data stored in the Store database.

   For example, if you want to erase all of the performance data stored in the Store database on the host `host02` of PFM - Agent for Platform (Windows), use the following command:

   ```
   jpctool db clear -id TS* -host host02 -dbid *
   ```

4.1.7 Initializing the settings for the Store database

If you have modified the settings for the Store database of the Agent Store or Remote Monitor Store service, you can restore the default values in one operation.

(1) Initializing the settings for the Collector service

To restore the default settings for the database, copy the `model` file (`jpcagt.ini.model`) for the Agent Collector or Remote Monitor Collector service startup initialization file.

To initialize the settings for the Store database:

1. Execute the `jpcspm stop` command to stop the PFM - Agent or PFM - RM service.

   Use the following command:

```
jpcspm stop -key XXXX#1
```

2. Delete the Agent Collector or Remote Monitor Collector service startup initialization file (`jpcagt.ini`).

   The `jpcagt.ini` file is located in the following directory:

   On physical hosts:

   - In Windows:

     installation-folder`\`*XXXX*#1`\agent[\`*instance-name*`]`#2
   - In UNIX:

     `/opt/jp1pc/`*XXXX*#1`/agent[/`*instance-name*`]`#2

   On logical hosts:

   - In Windows:

     environment-directory`\jp1pc\`*XXXX*#1`\agent[\`*instance-name*`]`#2
   - In UNIX:

     environment-directory`/jp1pc/`*XXXX*#1`/agent[/`*instance-name*`]`#2

3. Make a copy of the `model` file for the Agent Collector or Remote Monitor Collector service startup initialization file (`jpcagt.ini.model`) into a new file named `jpcagt.ini`.

   The `jpcagt.ini.model` file is located in the same directory as the `jpcagt.ini` file described in step 2.

4. Execute the `jpcspm start` command to start the PFM - Agent or PFM - RM service.

   Use the following command:

   ```
   jpcspm start -key XXXX#1
   ```

#1

xxxx indicates the service key of PFM - Agent or PFM - RM. Every PFM - Agent or PFM - RM has a specific service key, such as `Oracle` for PFM - Agent for Oracle and `Windows` for PFM - Agent for Platform (Windows). For details on service keys, see the description of the naming rules in an appendix of the *Job*

Management Partner 1/Performance Management Planning and Configuration Guide.

#2

If PFM - Agent or PFM - RM is monitoring an application program that can start a set of services on a host, there is one more directory created under the `Store` directory bearing the same name as the instance name.

(2) Initializing the Store database

To restore the default settings for the Store database, copy the model file (`jpcsto.ini.model`) for the service startup initialization files of the Agent Store and Remote Monitor Store services.

To restore the default settings for the Store database:

1. Execute the `jpcspm stop` command to stop the PFM - Agent or PFM - RM service.

   Use the following command:

   `jpcspm stop -key` *XXXX*#1

2. Delete the startup initialization file (`jpcsto.ini`) of the Agent Store and Remote Monitor Store services.

   The `jpcsto.ini` file is located in the following directory:

   On physical hosts:

   - In Windows:

     installation-folder`\`*XXXX*#1`\store[\`*instance-name*`]`#2

   - In UNIX:

     `/opt/jp1pc/`*XXXX*#1`/store[/`*instance-name*`]`#2

   On logical hosts:

   - In Windows:

     environment-directory`\jp1pc\`*XXXX*#1`\store[\`*instance-name*`]`#2

   - In UNIX:

     environment-directory`/jp1pc/`*XXXX*#1`/store[/`*instance-name*`]`#2

3. Make a copy of the `model` file for the Agent Store or Remote Monitor Store

service startup initialization file (`jpcsto.ini.model`) into a new file named `jpcsto.ini`.

The `jpcsto.ini.model` file is located in the same directory as the `jpcsto.ini` file described in step 2. When using Store 2.0, you need to execute the `jpcconf db vrset -ver 2.0` command after making the copy. Note that you must not start the Agent Store and Remote Monitor Store services before executing the `jpcconf db vrset -ver 2.0` command. If you do this, the performance data will be initialized.

4. Execute the `jpcspm start` command to start the PFM - Agent or PFM - RM service.

   Use the following command:

   `jpcspm start -key` *XXXX*[#1]

#1

xxxx indicates the service key of PFM - Agent or PFM - RM. Every PFM - Agent or PFM - RM has a specific service key, such as `Oracle` for PFM - Agent for Oracle and `Windows` for PFM - Agent for Platform (Windows). For details on service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

If PFM - Agent or PFM - RM is monitoring an application program that can start a set of services on a host, there is one more directory created under the `Store` directory bearing the same name as the instance name.

4.1.8 Importing backup data (with Store 2.0)

By importing backup data, you can make historical performance data available for reference. Use the `jpctool db import` command to import backup data, specifying either a full or additional import.

After the import process, the imported data can be viewed in parallel with the data in the Store database currently in use. When you import a unit database that covers a division period already represented in the Store database, the data in the Store database is given priority when performance data is displayed.

To import backup data:

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool service list` command to make sure that the Agent Store or Remote Monitor Store service is running.

3. Execute the `jpctool db import` command.

   Use the following commands:

   For a full import:

   When you execute the command, the files in the import directory are deleted and replaced with the backup files.

   ```
   jpctool db import -key XXXX#1 -d D:\backup01#2
   ```

   For an additional import:

   When you execute the command, data is added to the backup files that are stored in the import directory.

   ```
   jpctool db import -key XXXX#1 -d D:\backup01#2 -add
   ```

#1

xxxx indicates the service key of PFM - Agent or PFM - RM. Every PFM - Agent or PFM - RM has a specific service key, such as `Oracle` for PFM - Agent for Oracle and `Windows` for PFM - Agent for Platform (Windows). For details on service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

`D:\backup01` indicates the backup directory.

4.1.9 Converting the data model of backup data (with Store 2.0)

When you upgrade PFM - Agent or PFM - RM, you can also upgrade the data model of the backup data. You cannot import backup data into Store 2.0 if the data model of the backup data is different from that used by the Store database.

If the data model of the backup data is an older version than that used by the Store database, you can use the `jpctool db dmconvert` command to upgrade the data model of the backup data, and then you can import it. The `jpctool db dmconvert -d` command requires free disk space in the specified directory that is equal to twice the size of the data to be converted.

To convert the data model of backup data:

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool db dmconvert` command.

Use the following command:

```
jpctool db dmconvert -d D:\backup01#
```

`D:\backup01` indicates the backup directory.

4.1.10 Displaying information about the Agent Store and Remote Monitor Store services or backup directory (in Store 2.0)

You can check the version of the Store and the data model for the currently used service by viewing information on the Agent Store or the Remote Monitor Store service and the backup directory. Use the `jpcconf db display` command to display the information.

The following table lists the items that can be displayed by the `jpcconf db display` command.

Table 4-19: Items that can be displayed by the jpcconf db display command

Item	Without -d option		With -d option
	Single-instance agent	Multi-instance agent	
Service key	Yes	Yes	Yes
Instance name	No	Yes	No
Store version	Yes	Yes	Yes
Data model version	Yes	Yes	Yes

Legend:

Yes: Can be displayed.

No: Cannot be displayed.

To display information about the Agent Store service or backup directory:

1. Log on to the host that has PFM - Agent or PFM - RM installed.
2. Execute the `jpctool service list` command to make sure that the Agent Store or Remote Monitor Store service is running.
3. Execute the `jpcconf db display` command.

   Use the following command:

   To display information about the backup directory:

   ```
   jpcconf db display -d D:\backup01#
   ```

To display information about the Agent Store or Remote Monitor Store service:

```
jpcconf db display
```

#

`D:\backup01` indicates the backup directory.

4.2 Managing event data

Event data is stored in the Store database managed by the Master Store service of PFM - Manager. In the Store database, you can:

- Change the maximum number of records for event data
- Change the storage location of event data
- Export event data
- Check the amount of disk space used by event data
- Erase event data

Note:

You cannot initialize the settings for the Store database that stores event data.

The steps for each procedure are described below. For details on how to modify the storage location for event data, see the chapters explaining installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. For details on the commands used in this section, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

4.2.1 Changing the maximum number of records for event data

To change the maximum number of records for event data to store in the Store database, use the Services window in PFM - Web Console.

Note:

You need to have Administrator user permissions to use the Services window.

To modify the maximum number of records for alarm event data:

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

   You need to log on as a user with Administrator user permissions.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the **PFM - Manager** folder.

   Services provided by PFM - Manager are displayed. The name of each service is represented by the service ID.

4. Select the Master Store service.

   The name of the Master Store service begins with **PS** or is **<Master Store>**.

   The selected Master Store service is marked with a checkmark.

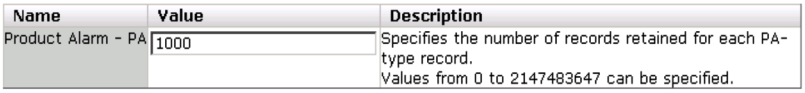
5. In the method frame, select **Properties**.

   The Properties window of the Master Store service is displayed with the properties shown hierarchically.

6. Select the **Retention** node.

   At the bottom of the information frame, the properties of the **Retention** node are displayed.

   Figure 4-6: Example settings for maximum number of records (event data)



   Modify the property settings. The following table gives a description and setting for the property.

   Table 4-20: Description and settings for each property

Record type	Property name	Settings
PA record type	Product Alarm - PA	Sets the maximum number of records to store for event data. You can specify a numerical value from 0 to 2,147,483,647.

7. Click the **OK** button.

   Your settings are enabled.

4.2.2 Exporting event data

You can export the event data stored in the Store database to a text file. Use the `jpctool db dump` command to export data.

To export the alarm event data:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool service list` command to make sure that the Name Server, Master Manager, and Master Store services are all up and running.
3. Execute the `jpctool db dump` command.

For example, of the events in the Store database of the monitoring manager, if you want to export the events collected from 02:00:00 (GMT) to 14:59:00 (GMT) on July 10, 2006 to the file `pa.out`, use the following command:

```
jpctool db dump -id PS* -stime 2006/07/10 02:00 -etime 2006/
07/10 14:59 -f pa.out -dbid PA -rec *
```

When the command finishes normally, the export file for the event data is created in the following location:

On physical hosts:

- In Windows:

  installation-folder`\mgr\store\dump\pa.out`

- In UNIX:

  `/opt/jp1pc/mgr/store/dump/pa.out`

On logical hosts:

- In Windows:

  environment-directory`\jp1pc\mgr\store\dump\pa.out`

- In UNIX:

  environment-directory`/jp1pc/mgr/store/dump/pa.out`

4.2.3 Checking the disk space used for event data

You can use the Services window of PFM - Web Console to check the disk space used by the Store database.

Note:

You need to have Administrator user permissions to use the Services window.

To check the disc space used for alarm event data:

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

   You need to log on as a user with Administrator user permissions.

   The main window of PFM - Web Console appears.

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

   The Services window appears.

3. In the navigation frame of the Services window, expand the hierarchy under the PFM - Manager folder.

Services provided by PFM - Manager are displayed. The name of each service is represented by the service ID.

4. Select the Master Store service.

   The name of the Master Store service begins with **PS** or is **<Master Store>**.

   The selected Master Store service is marked with a checkmark.

5. In the method frame, select **Properties**.

   The Properties window of the Master Store service is displayed with the properties shown in a tree.

6. Select the **Disk Usage** node.

   The disk space used by the database under the control of the Master Store service is displayed at the bottom of the Properties window.

   Figure 4-7: Example of displaying disk space (event data)

Name	Value	Description
Product Interval	4.0 KB	Displays the disk capacity used by PI-type records.
Product Detail	4.0 KB	Displays the disk capacity used by PD-type records.
Product Alarm	7.3 MB	Displays the disk capacity used by PA-type records.
Product Log	4.0 KB	Displays the disk capacity used by PL-type records.
Total Disk Usage	7.3 MB	Displays the disk capacity used by the entire database.

4.2.4 Erasing event data

You can erase the event data stored in the Store database if the data is no longer required. Use the `jpctool db clear` command to erase data in the Store database.

Note:

You must execute the `jpctool db clear` command on the host where PFM - Manager is installed.

To erase the alarm event data:

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

   You need to log on as a special user with special permissions, as shown below:

   - In Windows:

     Administrators or Backup Operators permissions

   - In UNIX:

     root user permissions

2. Execute the `jpctool service list` command to make sure that the Name Server, Master Manager, and Master Store services are all up and running.

3. Execute the `jpctool db clear` command.

To erase the event data stored in the Store database managed by the Master Store service, use the following command:

```
jpctool db clear -id PS* -dbid PA
```

4.3 Notes

This section gives cautionary notes on working with operation monitoring data in Performance Management.

4.3.1 Size limit of the Store database

(1) With Store 2.0

With Store 2.0, data is stored in multiple files, each covering a specific time period. Also, the data for each record type is stored in a different data file. For this reason, a size limit of 2 GB applies to each individual data file, rather than to the total amount of data in the database. Also, you cannot exceed the file size limit imposed by the `ulimit` command on UNIX systems or other restrictions on the file system.

You can calculate the size of each data file by using an expression to estimate the amount of disk space occupied by the Store database and setting the retention period for historical data to zero. For the expression used to estimate the amount of disk space occupied by the Store database, see the appendix describing the amount of disk space occupied by the Store database (Store version 2.0) for PFM - Agent 08-00 and later in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*, or an appropriate PFM - Agent manual.

Data for each record type is written to a data file in the Store database that is switched periodically. If the size of the data file reaches the limit within the allotted time period, the KAVE00227-W message is output, and no more data of that record type is written to the database. However, the Agent Store and Remote Monitor Store services continue to run.

When the allotted time period elapses and the data file is switched, the KAVE00228-I message is output and the Agent Store and Remote Monitor Store services resume writing data to the database.

(2) With Store 1.0

The maximum overall file size of the Store database used in Performance Management is 2 GB. Also, you cannot exceed the file size limit imposed by the `ulimit` command on UNIX systems or other restrictions on the file system.

The Store service stops when the file size of the Store database has reached the limit. In this case, the KAVE00182-E message is output to the system log (Windows Event Log in Windows or syslog on UNIX systems) and the common message log.

If the file size of the Store database has reached the limit, perform the following steps:

1. Access the Agent Collector properties from PFM - Web Console, and change the settings so that no records are collected.

(In this situation, only the Agent Store service has stopped. The Agent Collector service is still running.)

2. Use the `jpcspm start` command to restart the Agent Store service.

   For details on the `jpcspm start` command, see *2. Commands* in the manual *Job Management Partner 1/Performance Management Reference*.

3. Back up data.

   To do so, use the `jpctool db dump` or `jpcrpt` command, or output reports to a file in CSV or HTML format. For details on how to use the `jpctool db dump` command to back up performance data and event data, see *4.1.4 Exporting performance data* and *4.2.2 Exporting event data*, respectively.

   For details on the `jpcrpt` command, see *2. Commands* in the manual *Job Management Partner 1/Performance Management Reference*.

   For details on outputting reports to a CSV or HTML file, see *5.9.1 Exporting reports in CSV or HTML format by using a browser*.

4. Erase data.

   Erase the performance data. For details on how to erase performance data and event data, see *4.1.6 Erasing performance data* and *4.2.4 Erasing event data*, respectively.

5. Access the Agent Collector properties from PFM - Web Console.

   Configure the Agent Collector service to collect records, and then resume operation.

4.3.2 When the Agent Store or Remote Monitor Store service stopped abnormally

Note the following in the event of an abnormal termination of the Agent Store or Remote Monitor Store service:

- If the Agent Store or Remote Monitor Store service stops abnormally while writing to the Store database, an integrity check is performed as part of the startup process the next time the Agent Store or Remote Monitor Store service is started. Any invalid data found during the integrity check could be lost.
- If the Agent Store or Remote Monitor Store service could not finish normally (for example due to a power failure), the service reconstructs the index of the Store database at the next startup. In this case, the Agent Store or Remote Monitor Store service might take longer than usual to start.

4.3.3 When the disk capacity is insufficient

The Store database stops accepting more data when it cannot use sufficient required disk space. If this occurs, a KAVE00105-E message is output, and the Master Store,

Agent Store, or Remote Monitor Store service stops.

If you receive the above message, perform one of the following procedures:

- Reserve sufficient disk space
- Reduce the disk space occupied by the Store database

(1) Reserving sufficient disk space

Estimate how much disk space is used by the Store database and change the storage location of the Store database to a disk with enough free space. For details on how to estimate the amount of disk space occupied by the Store database, see the appendix describing system estimation in the appropriate PFM - Agent or PFM - RM manual. For details on how to change the storage location of the Store database for event data, see the chapter that describes installation and setup in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*. For details on how to change the storage location of the Store database for performance data, see the appropriate PFM - Agent or PFM - RM manual.

(2) Reducing the disk space occupied by the Store database (Store 1.0 only)

First, you must change the current settings to decrease the maximum size of the disk space occupied exclusively by the Store database. To decrease the maximum size of data, you can restrict the number or type of records to be collected by the Agent Collector service, or set shorter retention periods or smaller numbers of stored records to be kept by the Store database. For details on how to change which records are collected by the Agent Collector service, see *4.1.1 Modifying the recording options for performance data*. For details on how to change the retention conditions for the Store database, see *4.1.3 Modifying the retention conditions for performance data (in Store 1.0)* and *4.2.1 Changing the maximum number of records for event data*.

You cannot, however, reduce the disk space occupied exclusively by the Store database only by setting the maximum size of data. To reduce the occupied disk space, perform the following procedures:

- For the Store database of the Agent Store service:

  Follow steps 1-3 below:

  1. Delete the performance data for records in the Store database that are no longer needed.

     In the Store database, unnecessary data for a particular record is deleted when new performance data of that record is stored. If you configure the Agent Collector service to no longer collect particular records, the performance data for those records remains in the Store database, and the amount of disk space occupied by the Store database remains the same. Perform the following procedure to delete the performance data of records that are no longer being collected from the Store database. This procedure is

not required for the Store database of the Master Store service, or for when you have not configured any records not to be collected by the Agent Collector service.

The following procedure shows an example of how to delete data of unwanted records from the Store database.

For example, suppose you are using PFM - Agent for Platform, and want to change the collection settings from `Yes` for `PI_LOGD`, `Yes` for `PI_NIND`, and `Yes` for `PD_PD` to `No` for `PI_LOGD`, `Yes` for `PI_NIND`, and `No` for `PD_PD`

(1) Set `Yes` for records that you no longer want collected. Set `No` for all other records. In this example, set `Yes` for `PI_LOGD` and `PD_PD`, and `No` for the others.

(2) Modify the retention conditions as follows:

- For PD and PL record types, set the maximum number of records to 0.

- For the PI record type, set the retention period of records to the minimum for each collection period. For example, set `Minute` for performance data stored in minutes and `Hour` for performance data stored in hours.

(3) Store the performance data in the Store database at least once.

Note 1: For details on the timing when the performance data is stored in the Store database, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note 2: Tasks (1) to (3) invalidate the area in the Store database occupied by the records that you no longer want to collect (in this example, `PI_LOGD` and `PD_PD`). The invalidated areas can be eliminated from the database file by reorganizing the Store database. Note that you might be unable to invalidate the entire area occupied by the performance data if the record is a PI-type record or a Process Detail (PD) record of PFM - Agent for Platform. For details, see *[Notes about the data that cannot be deleted from the Store database even by storing the performance data of the record]*.

(4) Set `No` as the collection setting for all records.

(5) Set your desired retention conditions of the Store database.

(6) Set your desired collection configurations.

2. Deleting the extra performance data in the Store database

   If you reduce the number of records kept by the Store database or set shorter retention periods, you will have more performance data in the Store database than the retention conditions allow. This is because the data stored by using previous retention conditions still remains intact. If this is the case then you

must perform the following procedure to delete the extra performance data that does not match the new retention conditions. This procedure is only required when you have set shorter retention periods or smaller numbers of stored records to be kept by the Store database.

(1) Set your desired retention conditions of the Store database.

(2) In the Store database store, at least once, the performance data of the records for which you modified the retention conditions.

Note 1: For details on the timing when the performance data is stored in the Store database, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note 2: The area of the performance data for a record that no longer matches the retention conditions is invalidated when a new record is stored and performance data in the Store database is increased. The invalidated areas can be eliminated from the database file by reorganizing the Store database. Note that you might be unable to invalidate the entire area occupied by the performance data if the record is a PI-type record or a Process Detail (PD) record of PFM - Agent for Platform. For details, see *[Notes about the data that cannot be deleted from the Store database even by storing the performance data of the record]*.

3. Reorganizing the Store database

   Reorganize the Store database to reduce the disk space occupied exclusively by the Store database. For details on how to reorganize the Store database, see *4.3.4 Checking the size of, and reorganizing, the Store database*.

[Notes about the data that cannot be deleted from the Store database even by storing the performance data of the record]

When the performance data of a record is stored in the Store database, the area of the performance data for a record that does not match the retention conditions is invalidated when the performance data of the record increases in the Store database. There are, however, some records in the Store database where storing additional performance data for them does not increase the size of the data. None of the performance data for these records shall be invalidated. Records of PI record type or of the Process Detail (PD) of the PFM - Agent for Platform fall under this category.

In the case of the PI record type, in a summary block where new performance data is created by the process of storing performance data, the performance data for that summary block is deleted from the Store database. When new performance data is not created, the data remains in the Store database. Note that the performance data in the summary block of `year` always remains. For example, suppose that the Store database contains performance data for the

PI-LOGD record that was all collected before 16:00:00 on May 23, 2006 (Tuesday), and you store performance data for the PI_LOGD record at 10:00:00 on May 24, 2006 (Wednesday). The performance data in the summary block of year remains in the database. The performance data for May 2006 is consolidated into the performance data in the summary block of month, so no new performance data is created. Accordingly, all the performance data of the PI_LOGD record in the summary block of month remains in the Store database. Similarly, all the performance data in the summary block of week remains in the Store database. For the performance data in the summary block of day, the new performance data for May 24, 2006 is created, so all of the performance data of the PI_LOGD record in the summary block of day is invalidated in the Store database. Similarly, all of the performance data in the summary block of hour and minute is invalidated. Count all the remaining performance data in when you estimate the disk space occupied exclusively by the Store database.

In case of the Process Detail (PD) record of the PFM - Agent for Platform, when there is no difference between the data last collected and the one that has just been collected, the performance data remains in the Store database. For details on the Process Detail (PD) record of PFM - Agent for Platform, see the chapter explaining records in the manual *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference*. Either make differences so that the old performance data will be deleted, or add such space as required for the Process Detail (PD) record to the estimated disk space occupied exclusively by the Store database when you operate the system.

- For the Store database of the Master Store service:

  1. Set your desired retention conditions for the Store database.
  2. Store the event data in the Store database at least once.

     Note 1: For details on the timing when the event data is stored in the Store database, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

     Note 2: The area of the data that no longer matches the retention conditions is invalidated when event data for the record is stored in the Store database. The invalidated area can be deleted from the database file by reorganizing the Store database.
  3. Reorganize the Store database.

     Reorganize the Store database to reduce the disk space occupied exclusively by the Store database. For details on how to reorganize the Store database, see *4.3.4 Checking the size of, and reorganizing, the Store database*.

If the Master Store service or the Agent Store service does not start even after taking these actions, there might be some unrecoverable logical errors in the Store database. In this case, you must restore the Store database from the backup data, and then restart the Master Store service or the Agent Store service. If you have no backup data, you must initialize the Store database, and then start the Master Store service or the Agent Store service. To initialize the Store database, delete all the files indicated below from the storage directory of the Store database.

- Files with the extension `.DB`
- Files with the extension `.IDX`

The default storage directories of the Store database are listed below.

The storage directory of the Store database for performance data:

For details, see each of the PFM - Agent manuals.

The storage directory of the Store database for event data:

- In Windows:

  installation-folder`\mgr\store`

- In UNIX:

  `/opt/jp1pc/mgr/store`

You can change the storage directories of the Store database for event data in the `jpcsto.ini` file. For details on how to change the storage directories, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

4.3.4 Checking the size of, and reorganizing, the Store database

The Store database consists of the data files, which store the actual data, and the index files, which manage the data indices for faster access. With Store 1.0, deleting data in the data files only invalidates the area of that data, and the size of the files does not decrease automatically. Although the invalidated area in the data files is reused, the reusing rate might suffer when the number of instances to store performance data varies with each collection, causing the size of the Store database to exceed the estimated size of the exclusively occupied disk space. For this reason, when using Store 1.0, we recommend that you check the size of the Store database regularly and reduce the invalidated area by reorganizing the Store database when the total size exceeds 90% of the estimated disk space. You do not need to reorganize the database when using Store 2.0.

The following sections describe how to check the size of the Store database and reorganize the Store database.

(1) Checking the size of the Store database

Check the sizes of all the files with extensions `.DB` and `.IDX` in the storage location of the Store database, and calculate the total size of the files. With Store 1.0, when the total size exceeds 90% of the estimated disk space, perform the following procedure to reorganize the Store database.

(2) Reorganizing the Store database (Store 1.0 only)

To reorganize the Store database:

1. Start the Performance Management service that will manage the Store database you want to reorganize.

   By using the `jpcspm start` command, start the PFM - Agent or PFM - Manager service to manage the Store database you want to reorganize, if it is not running already.

2. Use the `jpctool db backup` command to back up the Store database.

   Execute the `jpctool db backup` command to back up the Store database that you want to reorganize. The `jpctool db backup` command extracts data from the data file, except in the invalidated area, and saves the data.

   Note:

   > For the `jpctool db backup` command to work properly, the corresponding backup file requires more than double the total size of the Store database calculated above. Make sure that you have enough free space before you run the command.

3. Stop the service of Performance Management that has been managing the Store database that you want to reorganize.

   By using the `jpcspm stop` command, stop the PFM - Agent or PFM - Manager service that has been managing the Store database that you want to reorganize.

4. Use the `jpctool db restore` command to restore the Store database.

   Execute the `jpctool db restore` command to restore the Store database from the backup you made in step 2.

5. Start the service of Performance Management.

   If necessary, start the service that you stopped in step 3 by issuing the `jpcspm start` command.

4.3.5 When files or folders are not deleted after their retention period expires

Records are automatically deleted only if they exceed the retention period and corresponding new records are collected. Therefore, if previously collected records are

set so that they are not to be collected again, the record data will not be deleted.

To delete such unnecessary records and folders:

1. Use the `jpcspm stop` command to stop the appropriate PFM - Agent or PFM - RM.
2. Search the appropriate directory in the Store database for DB/IDX files that contain the name of the record (*database-ID_record-type*, such as `PI_PI`) you want to delete.
3. Manually delete the files that were found by the search.
4. When the `DB/IDX` files are deleted in step 3, some folders with names that consist of dates (such as `1212` and `1219`) might be left empty. If so, delete these empty folders as well.

4.3.6 The default retention period of records in Store 2.0

Store 2.0 can be used with version 08-11 or later of PFM - Manager or PFM - Base combined with version 08-00 or later of PFM - Agent for Platform. The default retention period of records differs whether PFM - Agent 08-11 or later is used or PFM - Agent 08-00 is used.

When PFM - Agent 08-11 or later is used:

For details on the default retention period of records, see the appropriate PFM - Agent manual.

When PFM - Agent 08-00 is used:

For PD-type and PL-type records, the default retention period of all records will be set to 10 days. The following table describes the default retention period of the PI record type.

Table 4-21: The default retention period of the PI record type

Retention period before setup	Retention period after setup				
	Summarization category				
	Minute (unit: days)	Hour (unit: days)	Day (unit: weeks)	Week (unit: weeks)	Month (unit: months)
1 minute	1	--	--	--	--
1 hour	1	1	--	--	--
1 day	1	1	1	--	--

Retention period before setup	Retention period after setup				
	Summarization category				
	Minute (unit: days)	Hour (unit: days)	Day (unit: weeks)	Week (unit: weeks)	Month (unit: months)
2 days	2	2	1	--	--
3 days	3	3	1	--	--
4 days	4	4	1	--	--
5 days	5	5	1	--	--
6 days	6	6	1	--	--
1 week	7	7	1	1	--
1 month	31	31	5	5	1
1 year	366	366	54	54	12

Legend:

--: Item that cannot be specified

4.3.7 Performance data stored after a data model upgrade

Upgrading the data model can result in a new field being added to existing records. If this occurs, the default performance data is stored in the Store database that existed prior to the upgrade. The following table lists the performance data stored by default.

Table 4-22: Performance data to be stored by default

Data type of the field	Performance data to be stored
char	Empty
double	0
float	0
long	0
short	0
string	Empty
time_t	0

Data type of the field	Performance data to be stored
timeval	0
ulong	0
utime	0
word	0
(Not applicable)	0

Chapter

5. Creation of Reports for Operation Analysis

This chapter describes how to create reports, and how to display and output reports based on performance data collected by Performance Management.

5.1 Overview of reports
5.2 Process flow for creating a report
5.3 Creating reports by using a browser
5.4 Creating reports by using the Quick Guide
5.5 Creating reports by using commands
5.6 Creating and editing bookmarks by using a browser
5.7 Displaying reports
5.8 Displaying combination reports
5.9 Outputting reports
5.10 Notes on reports

5.1 Overview of reports

This section provides an overview of reports created by Performance Management.

5.1.1 About reports

Performance Management displays performance data collected by PFM - Agent or PFM - RM in the window of PFM - Web Console in graphical formats such as tables or graphs, allowing you to check and analyze the system operating status. Performance data represented in formats such as tables or graphs is called a *report*.

Define the information and conditions for displaying data in the report beforehand. There are several ways to define reports: use the *monitoring template* as is, use a customized monitoring template, or define a report by yourself.

5.1.2 Report types

There are two types of reports: *realtime report* and *historical report*.

Realtime report

Use this type of report to check the system status and problems at that time. You can specify settings so that a report is automatically updated at specified times and the latest data is displayed in the report. A realtime report collects performance data when the report is displayed, so realtime reports do not use the Store database.

Historical report

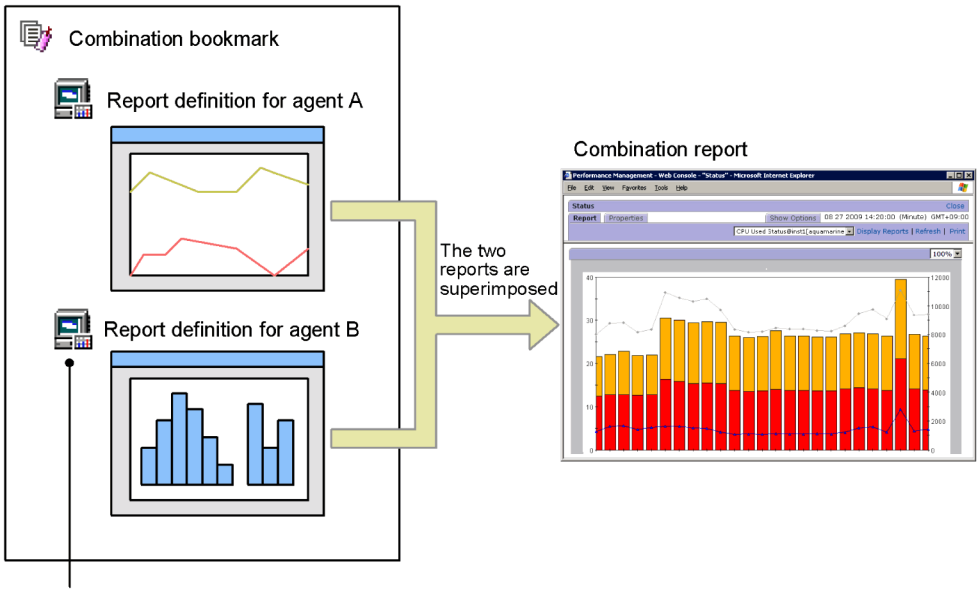
Create this type of report to analyze the trend of the system operating status from historical data until the present. Since past data must be retained, the historical report records performance data in the Store database. For details on how to record data into the Store database, see *4.1.1 Modifying the recording options for performance data*.

Performance Management provides both normal and combination reports. A *combination report* combines multiple historical reports in the same graph. By registering reports that combine report definitions from multiple agents in a bookmark or combination bookmark, you can display reports and combination reports right away without needing to select each agent individually.

In addition to registered reports, combination bookmarks allow you to save reports created during a specific period in the past as reference reports for validating registered reports. Reports used as reference reports for validating registered reports are called *baselines*. By defining and managing multiple registered reports and baselines in a combination bookmark, you can display them on the same graph as a combination report. Such combination reports allow you to ascertain the operating status of the system in its entirety.

The following figure shows the relationship between the definition of a combination bookmark and a combination report.

Figure 5-1: Relationship between combination bookmark definition and combination report



Each agent-specific report registered in a combination bookmark is called a *registered report*.

As shown in the figure, by creating a combination bookmark that contains report definitions for more than one agent, you can display multiple reports in one graph. For example, you can visually check the correlation between the number of transactions handled by the HTTP service and its response time by superimposing the two values in a combination report.

For details on how to display normal reports, see *5.7 Displaying reports*. For details on how to display combination reports, see *5.8 Displaying combination reports*.

5.1.3 Display formats of reports

You can display reports as *tables*, *lists*, or *graphs*, whichever best meets your purpose.

This section explains each display format.

(1) Tables

You can display historical data accumulated in a time sequence in table format. This format is suitable for seeing changes in each field value in a time series. The following figure shows an example of a table.

Figure 5-2: Example of a table

First Previous 1 - 20 OF 828 Next Last

Date and Time	CPU %	Page Faults/sec	User CPU %	Threads (Total)	Date and Time
06 05 2006 20:06:00	70.0738	1,700.0935	42.3339	940.0000	06 05 2006 20:06:00
06 05 2006 20:07:00	8.3464	256.6573	3.6255	949.0000	06 05 2006 20:07:00
06 05 2006 20:08:00	10.4551	81.6565	3.9272	946.0000	06 05 2006 20:08:00
06 05 2006 20:09:00	8.4996	87.1172	4.0425	949.0000	06 05 2006 20:09:00
06 05 2006 20:10:00	11.8752	102.5190	5.3161	952.0000	06 05 2006 20:10:00
06 05 2006 20:11:00	1.6385	50.7475	0.9623	948.0000	06 05 2006 20:11:00
06 05 2006 20:12:00	1.8466	83.1560	0.9623	945.0000	06 05 2006 20:12:00
06 05 2006 20:13:00	1.2484	42.2945	0.7802	942.0000	06 05 2006 20:13:00
06 05 2006 20:14:00	1.2741	39.0139	0.6760	941.0000	06 05 2006 20:14:00
06 05 2006 20:15:00	1.4824	43.2589	0.7542	942.0000	06 05 2006 20:15:00
06 05 2006 20:16:00	1.3524	42.2784	0.7802	941.0000	06 05 2006 20:16:00
06 05 2006 20:17:00	1.6645	76.2327	0.8062	938.0000	06 05 2006 20:17:00
06 05 2006 20:18:00	25.8518	134.0579	20.4161	947.0000	06 05 2006 20:18:00
06 05 2006 20:19:00	29.1027	52.1157	25.0715	944.0000	06 05 2006 20:19:00
06 05 2006 20:20:00	47.4642	287.1514	37.9194	947.0000	06 05 2006 20:20:00
06 05 2006 20:21:00	42.8497	68.1587	35.5694	944.0000	06 05 2006 20:21:00
06 05 2006 20:22:00	1.3210	34.9386	0.6605	936.0000	06 05 2006 20:22:00
06 05 2006 20:23:00	2.5748	78.0643	1.1183	941.0000	06 05 2006 20:23:00
06 05 2006 20:24:00	2.2627	52.4300	1.1704	940.0000	06 05 2006 20:24:00
06 05 2006 20:25:00	11.3595	157.0211	6.5506	944.0000	06 05 2006 20:25:00

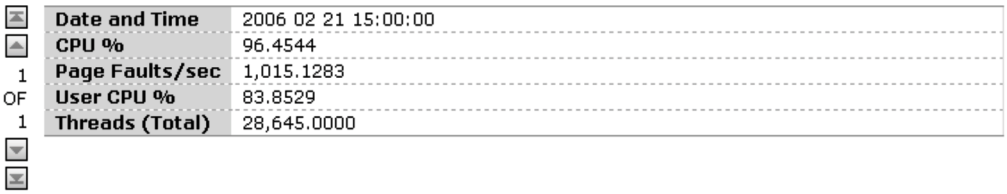
First Previous 1 - 20 OF 828 Next Last

(2) Lists

You can display field values for each agent or instance in list format. This format is especially suitable for displaying multiple agents or instances.

The following figure shows an example of a list.

Figure 5-3: Example of a list



The list data is displayed for each data group. A data group is a group in which data with different agents or instances are organized by time.

To display information about other agents or instances in the same data group, click the  or  button at the left of the list. To display information of another data group, click the  or  button on the menu bar in the Display Reports window.

(3) Graphs

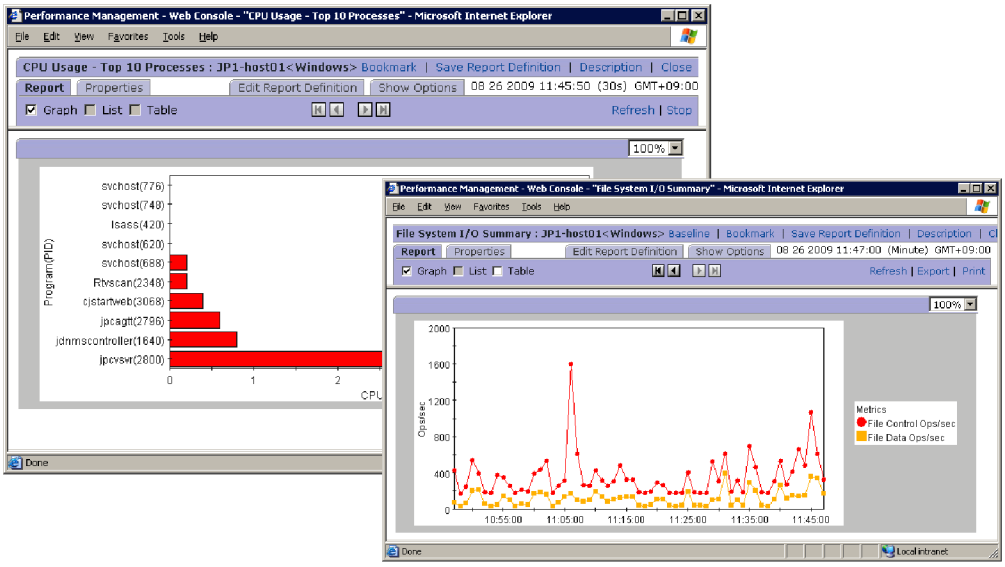
Reports can be displayed in a variety of graphs. You can specify the most appropriate graph depending on the graph characteristics, the number of data instances, and the number of agents to be handled. An element displayed in a graph is called a *field*. In a report definition, you can specify the fields to be displayed in a graph. You can set numerical fields only.

The graph types are as follows:

- Column graph
- Stacked column graph
- Bar graph
- Stacked bar graph
- Pie graph
- Line graph
- Area graph
- Stacked area graph

The following figure shows examples of graphs.

Figure 5-4: Examples of graphs



5.2 Process flow for creating a report

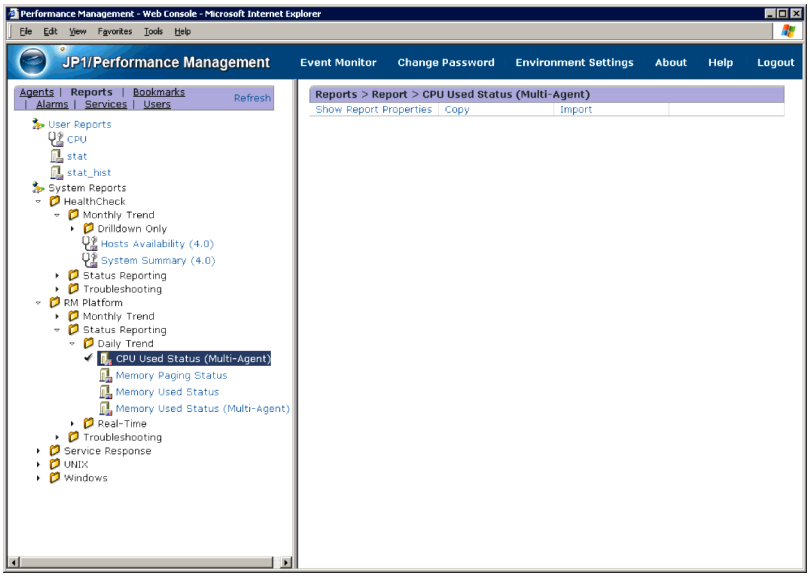
This section explains how to create reports and the process flow for creating reports.

(1) How to create reports

Create a report by using the Reports window of PFM - Web Console, the Quick Guide, or a command.

The following figure shows an example of the Reports window of PFM - Web Console.

Figure 5-5: Example of the Reports window



You can create a report in the following ways:

- Creating a new report

  To create a new report to match your system environment, define a new report. You can also create a simplified report by using the Quick Guide.

- Using an existing report

  You can use the following methods:

  - Use the monitoring template.

    The monitoring template is a set of reports, for which necessary information has been preset, included with each PFM - Agent or PFM - RM. When you use the monitoring template, at PFM - Agent or PFM - RM startup the system

can start collecting the performance data required for displaying a report of the monitoring template, and can create the report.

- Customize the monitoring template.

  You can copy the monitoring template and customize it to match your monitoring objectives.

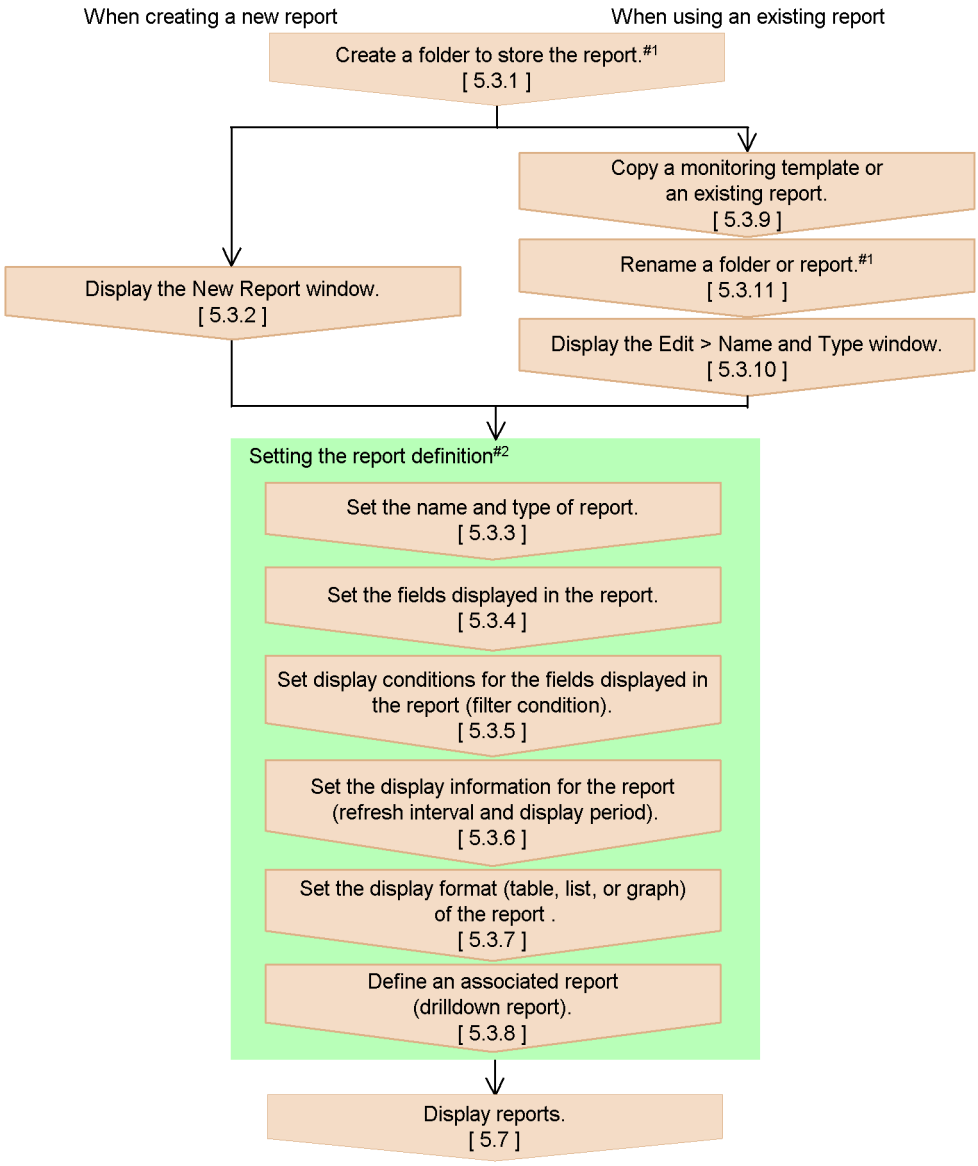
- Use a created report.

  You can copy and customize a created report.

(2) Process flow for creating reports

The following figure shows the process flow for creating a report. You can also use the Quick Guide to create reports. For details on how to create reports by using the Quick Guide, see *5.4 Creating reports by using the Quick Guide*.

Figure 5-6: Process flow for creating a report (from defining to displaying a report)



Legend: [ ] : See the indicated section.
#1 Perform as needed.
#2 Edit as needed when using an existing report.

5.3 Creating reports by using a browser

This section explains how to create reports in the window of PFM - Web Console.

For details on how to create a report by using commands, see *5.5 Creating reports by using commands*.

You can use the Quick Guide to create simplified reports. For details on how to create reports by using the Quick Guide, see *5.4 Creating reports by using the Quick Guide*.

5.3.1 Creating a report folder

To create a folder for storing reports:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select **User Reports** or a folder under **User Reports** for creating a folder in the Reports tree of the navigation frame.

   The selected folder is marked with a checkmark.

4. In the method frame, select **New Folder**.

   In the information frame, the New Folder window appears.

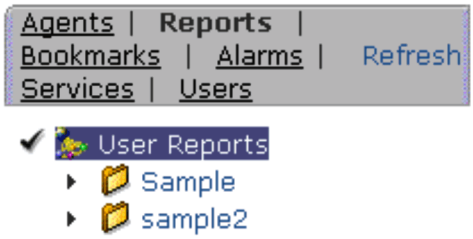
5. In **Name of new folder**, enter a folder name (1-64 characters).

6. Click the **OK** button.

   A folder is added in the **User Reports** folder selected in step 3 or below the folder.

   The following figure shows an example of creating a report folder:

   Figure 5-7: Example of creating report folder



5.3.2 Displaying the New Report window

Create a new report in the New Report window of the Reports window.

To display the New Report window:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select a folder for storing reports in the Reports tree of the navigation frame.

   The selected folder is marked with a checkmark.

4. In the method frame of the Reports window, select the **New Report** method.

   In the information frame, the New Report > Name and Type window appears. Go to *5.3.3 Setting the name and type of a report*.

5.3.3 Setting the name and type of a report

To set the name and type of a report:

1. In the New Report > Name and Type window, set **Report name** and **Product**.

   Report name

   Enter no more than 64 characters.

   Product

   Select the data model version to be used.

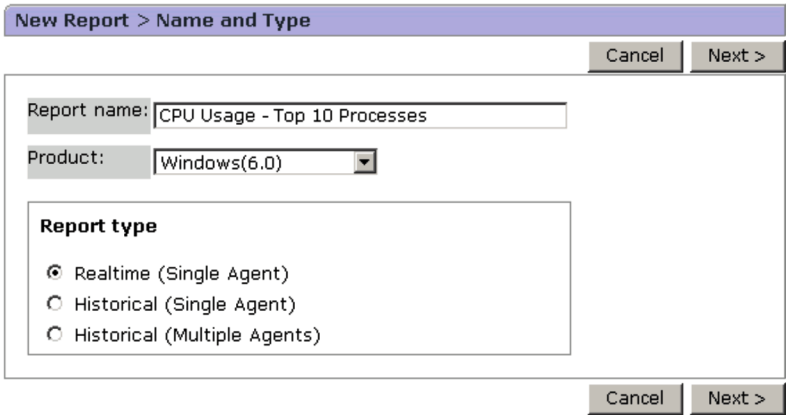
   For example, to define a realtime report of the top ten processes whose CPU usage ratio is high, whose Agent is PFM - Agent for Platform (Windows), and whose data model version is 6.0, specify the following settings:

   Report name: `CPU Usage - Top 10 Processes`

   Product: `Windows(6.0)`

   The following figure shows an example of defining a realtime report, whose Agent is PFM - Agent for Platform (Windows), and whose data model version is 4.0.

Figure 5-8: Example of input in the New Report > Name and Type window



2. Select **Report type**.

   Report type has the following three types:

   - **Realtime (Single Agent)**

     This is a realtime report for displaying the status of the system at that time. The report collects and displays the data of a single agent at that time, ranks collected values, and displays these rankings. However, past data is not stored in the Store database, so you cannot retrieve and display such data. Realtime (Single Agent) reports handle single-instance and multi-instance records.

   - **Historical (Single Agent)**

     This is a historical report for collecting and displaying the data of a single agent. A report is displayed in a single report window for a single agent. If you select multiple agents, as many report windows as selected agents are displayed. Historical (Single Agent) reports handle single-instance and multi-instance records

   - **Historical (Multiple Agents)**

     This is a historical report for collecting and displaying the data of multiple agents. A single report window is displayed regardless of whether one or more agents are selected. Historical (Multiple Agents) reports handle single-instance records only.

     If this item is selected, you cannot select multi-row records (multi-instance records) in the next New Report > Field window.

   The default is **Realtime (Single Agent)**.

   If this item is selected, you cannot select multi-row records (multi-instance

records) in the next New Report > Field window.

For details on single-instance records and multi-instance records, see the chapter that describes the Performance Management functions in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

3. Click the **Next >** button.

   The New Report > Field window appears. Go to *5.3.4 Setting fields displayed in a report*.

Note: Data model version and compatibility

The contents of the data model might vary according to the version, but upward compatibility is guaranteed. Therefore, if you create a report using an old data model, you can display a report in PFM - Agent or PFM - RM of a newer data model. For example, a report created in PFM - Agent for Platform Windows (3.0) can display the data of any version of PFM - Agent for Platform (Windows), but a report created in PFM - Agent for Platform Windows (4.0) can only display the data of version 07-00 and later of PFM - Agent for Platform (Windows). Depending on the PFM - Agent or PFM - RM, you can select multiple data model versions. For details on data model versions and compatibility, see the description of the compatibility among data model versions in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note: When selecting a historical report

As a historical report uses past data, you must specify that the records of the monitoring performance data be recorded into the Store database. Make sure that the monitoring records have been set up to be recorded. For details on how to record the data into the Store database, see *4.1.1 Modifying the recording options for performance data*.

5.3.4 Setting fields displayed in a report

The records and fields of the performance data set here might vary according to the agent. For details on records and fields for each agent, see the chapter describing the records in each PFM - Agent or PFM - RM manual.

To set the fields displayed in a report: If you want to use characters to search for a field, click the **Search fields** button in the New Report > Field window. For details on searching for fields, see *(1) Searching for fields*.

1. Select the records to be displayed in the report in **Record** of the New Report > Field window.

   If you select records, the fields of the selected records are displayed in **All fields**.

   Note:

In the New Report > Name and Type window, if **Historical (Multiple Agents)** is selected as a report type, only single-row records can be selected in **Record**.

Reference note: Description window for records

Click the **Description** button at the right of **Record** to display the description window for records belonging to the product selected in the New Report > Name and Type window.

Reference note: About single-row records and multi-row records

The description **(This is a single-instance record.)** or **(This is a multi-instance record.)** is displayed under **Record**. These messages indicate the record type. A single-row record indicates a single-instance record, and a multi-row record indicates a multi-instance record. For details on single-instance and multi-instance records, see the chapter describing Performance Management functions in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

2. In **All fields**, select the fields to be displayed in the report.

   Selected fields are displayed as selected. Use the **Shift** or **Ctrl** key to select multiple fields at a time.

3. Click the move button ().

   The fields selected in step 2 are moved to **Selected fields**.

   To undo a field already moved to **Selected fields**, select the fields to be undone in **Selected fields** and click the move button ().

   Also, select the fields in **Selected fields** and click the move button () or the move button () to sort the fields. The order to be specified here will also apply to the order of fields in tables, lists, and graphs.

   An example of settings in this window is as follows: For a realtime report of the top ten processes whose CPU usage ratio is high and whose agent is PFM - Agent for Platform (Windows), if you specify three for the fields of Process Detail (PD) records, namely CPU % (PCT_PROCESSOR_TIME), PID (ID_PROCESS), and Program (INSTANCE), set this window as follows:

   Record: `Process Detail (PD)`

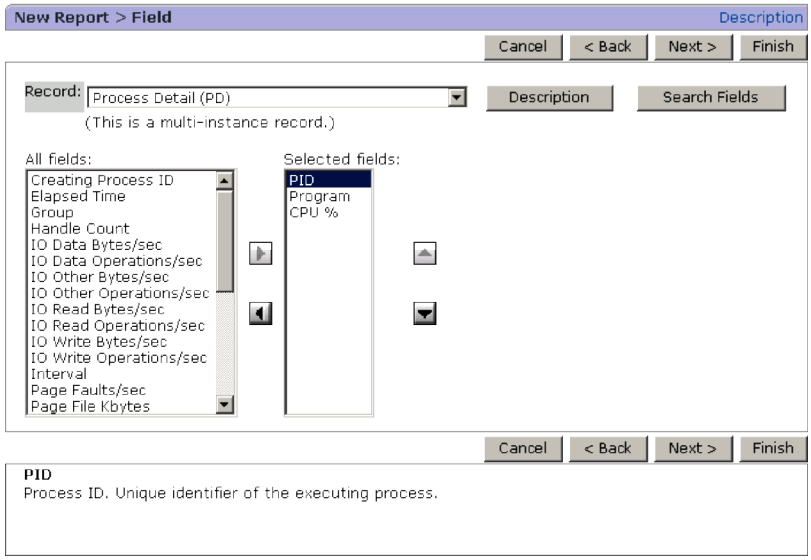
   Selected fields: `PID, Program, CPU %`

   The following figure shows an example of defining a realtime report of the top

ten processes in terms of CPU usage whose agent is PFM - Agent for Platform (Windows), with the following three fields selected from the Process Detail (PD) record:

- `CPU %` (PCT_PROCESSOR_TIME)
- `PID` (ID_PROCESS)
- `Program` (INSTANCE)

Figure 5-9: Example of input in the New Report > Field window



4. Click the **Next >** button.

   The New Report > Filter window appears. Go to *5.3.5 Setting display conditions for fields displayed in a report (filter condition)*.

(1) Searching for fields

This subsection describes how to use the New Report > Field window to search a field. The search results are included in **Selected fields** in the New Report > Field window.

1. Click the **Search fields** button in the New Report > Field window.

   The New Report > Field > Search Fields window appears.

2. Select the target records from the **Records to search** pull-down menu.

   The items of the pull-down menu are as follows:

   - **--All records--**

     Select this to search all records.

- A list of record names of the selected agent

  A list of record names of the selected agent is displayed in alphabetical order.

3. Enter in **Keywords to find** the characters that you want to search for in a field, and then click the **Search** button.

   The search results appear in the information frame.

   - If **--All records--** is selected as the target

     The search results are listed for each record in the Search results: record(s) window.

     If you click the anchor part of the relevant record, the search results are listed for each field in the New Report > Field > Search Field window.

   - If a record name is selected as the target

     The searched fields are listed in the New Report > Field > Search Fields window.

4. Select the check box of the fields that you want to select, and then click the **OK** button.

   The New Report > Field window from which you opened the New Report > Field > Search Fields window appears, and the selected fields are added to **Selected fields**.

5.3.5 Setting display conditions for fields displayed in a report (filter condition)

Setting the display conditions for fields displayed in a report allows you to filter the data to be displayed in the report so that the displayed data best matches your purpose. You can also set multiple filter conditions.

To set the display conditions for fields to be displayed in a report:

1. In **Field** of the New Report > Filter window, select the fields to be filtered.
2. Set the display conditions for the fields.

   For example, for a realtime report of the top ten processes whose CPU usage ratio is high and whose agent is PFM - Agent for Platform (Windows), if you specify the condition that the value of PID (ID_PROCESS) field is not 0 for Process Detail (PD) records, set as follows:

   Field: `PID`

   Condition: `<>`

   Value: `0`

3. Click the **Add** button.

The condition set in step 2 is added to **Conditional expression**.

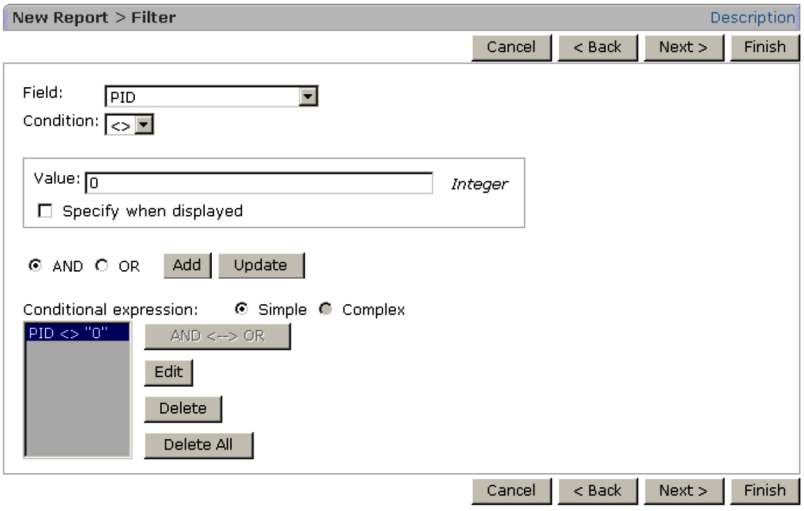
Conditional expression: `PID <> "0"`

If no conditional expression is set in **Conditional expression**, the report is registered as a report without any conditional expression.

The following figure shows an example of defining a realtime report of the top ten processes whose CPU usage ratio is high and whose agent is PFM - Agent for Platform (Windows), with the following filter condition specified for the Process Detail (PD) record:

The value of the PID (ID_PROCESS) field is not 0

Figure 5-10: Example of input in the New Report > Filter window



4. Click the **Next >** button.

   - When the report type is **Realtime (Single Agent)**:

     The New Report > Indication settings (Realtime) window appears. Go to *5.3.6 (1) Setting the display information for a realtime report*.

   - When the report type is **Historical (Single Agent)** or **Historical (Multiple Agents)**:

     The New Report > Indication settings (Historical) window appears. Go to *5.3.6 (2) Setting the display information for a historical report*.

Reference note: If you want to set filter conditions while displaying a report

If you select **Specify when displayed**, you can set filter conditions while displaying a report. Do not select **Specify when displayed** if you want to display

a report using conditions defined beforehand in the New Report > Filter window.

5.3.6 Setting the display information for a report (refresh interval and display period)

The settings for a report here might differ depending on whether the report type is realtime or historical.

- When a realtime report is selected:

  Make sure that the New Report > Indication settings (Realtime) window has been displayed, and then go to *(1) Setting the display information for a realtime report*.

- When a historical report is selected:

  Make sure that the New Report > Indication settings (Historical) window has been displayed, and then go to *(2) Setting the display information for a historical report*.

(1) Setting the display information for a realtime report

To set the display information for a realtime report:

1. Set the display information.

   For example, when defining a realtime report of the top ten processes whose CPU usage ratio is high in PFM - Agent for Platform (Windows), you could use the following conditions to set the display information for a realtime report of Process Detail (PD) records:

   Conditions:

   - The values of data displayed in the report are Delta values.
   - The automatic refresh interval of the report display is initially set to 60 seconds and has a minimum of 30 seconds.
   - Display the top ten data using the CPU % (PCT_PROCESSOR_TIME) field as the display criteria.

   Set as follows:

   Specify when displayed: Select

   Indicate delta value: Select

   Refresh interval

   Do not refresh automatically: Do not select

   Initial value: `60`

   Minimum value: `30`

   Display by ranking

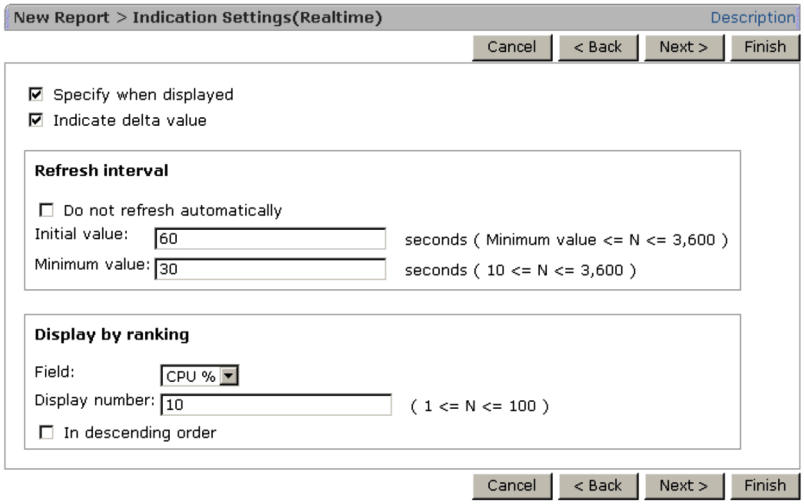
Field: `CPU%`

Display number: `10`

In descending order: Do not select

The following figure shows an example of entering information in the New Report > Indication Settings (Realtime) window.

Figure 5-11: Example of input in the New Report > Indication Settings (Realtime) window



2. Click the **Next >** button.

   The New Report > Components window appears. Go to *5.3.7 Setting the display format (table, list, or graph) of a report*.

(2) Setting the display information for a historical report

You can set the display information for a historical report.

Note: Performance information displayed in historical reports

- If you change the time of the host where PFM - Agent or PFM - RM is operating from the current time to the future time, the performance information from before the change to after the change is not displayed.
- If you change the time of the server where PFM - Agent or PFM - RM is operating from the current time to the past time, the overwritten performance information from after the change to before the change is displayed.

To set the display information for historical reports:

1. Set the display information.

For example, when defining a historical report that summarizes CPU usages for each minute for the most recent one hour period in PFM - Agent for Platform (Windows), you could use the following conditions to set the display information for a historical report of System Overview (PI) records.

Condition

- The collection period of performance data is specified when displaying the report.
- The display interval of the report is set to one hour.
- Only the data whose User CPU % (PCT_TOTAL_USER_TIME) field indicates the maximum value of the day is displayed.
- The maximum number of records displayable in the report is set to 1,440.

Set as follows:

Specify when displayed: optional

Settings for the report display period

Date range: `specify when displayed`

Report interval: `Hour`

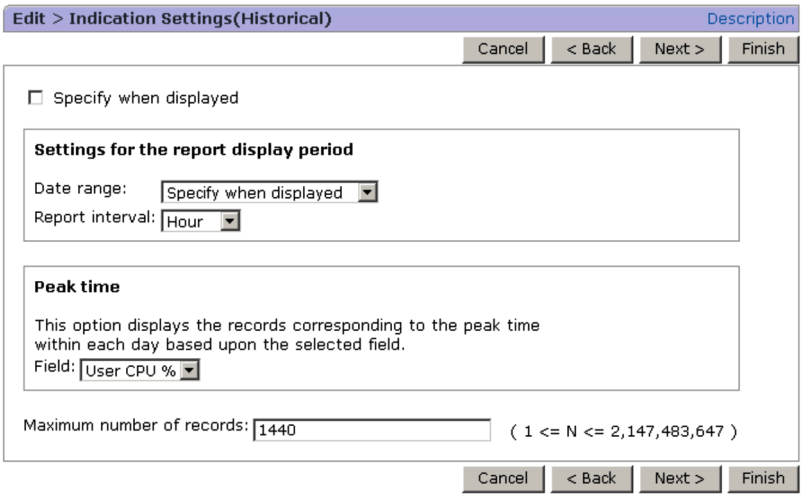
Peak time

Field: `User CPU%`

Maximum number of records: `1440`

The following figure shows an example of entering information in the New Report > Indication Settings (Historical) window.

Figure 5-12: Example of input in the New Report > Indication Settings (Historical) window



2. Click the **Next >** button.

   The New Report > Components window appears. Go to *5.3.7 Setting the display format (table, list, or graph) of a report*.

5.3.7 Setting the display format (table, list, or graph) of a report

You can select the report display style from the following three formats, and you can also display data in multiple formats for a single report.

- Table
- List
- Graph

(1) Setting components of a report

To set the display format of a report:

1. Set the necessary information for the display format.

   For example, when defining a realtime report of the top ten processes whose CPU usage ratio is high in PFM - Agent for Platform (Windows), if you want to display the report of each field of Process Detail (PD) records in table format and display the CPU % (PCT_PROCESSOR_TIME) fields report in graph format, specify the following settings:

   CPU%: Select **Table** and **Graph**

   PID: Select **Table**

Program: Select **Table**

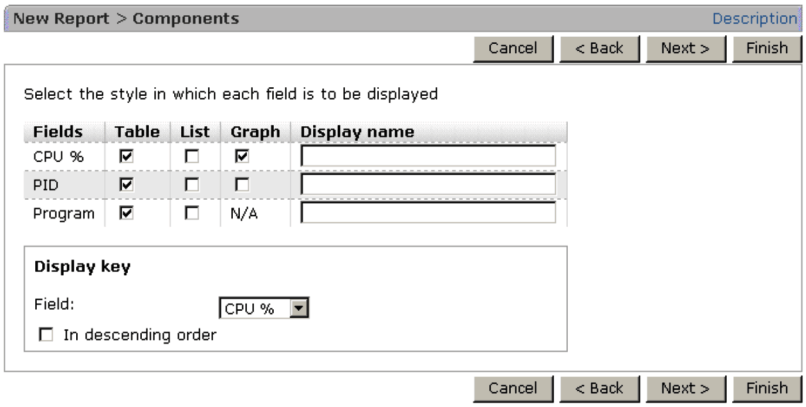
Display key

Field: `CPU%`

In descending order: Do not select

The following figure shows an example of entering information in the New Report > Components window.

Figure 5-13: Example of input in the New Report > Components window



2. Click the **Next >** button.

   - If **Graph** is selected one or more times in the New Report > Components window:

     The New Report > Graph window appears. Select a graph type. Go to *(2) Setting a graph type*.

   - If **Graph** is not selected in the New Report > Components window:

     The New Report > Drilldown windows appears. Go to *5.3.8 Associating a report with another report (drilldown report)*.

(2) Setting a graph type

If **Graph** is selected in the New Report > Components window, set the graph type and the display format.

To set the graph type:

1. Set the graph type and the necessary information for the display format.

   For example, when defining a realtime report of the top ten processes whose CPU usage ratio is high in PFM - Agent for Platform (Windows), you could use the following conditions to display the graph of CPU % (PCT_PROCESSOR_TIME)

fields report of Process Detail (PD) records:

Conditions:

- The CPU % (PCT_PROCESSOR_TIME) field value is set for the vertical axis.
- The program (INSTANCE) field name is set for the horizontal axis and PID (ID_PROCESS) field value is set for the data within the parentheses.
- The bar graph is set for the graph type.

Set as follows:

Graph types

Column: Select

Series direction

By row: Select

Axis labels

X-axis: `Program (PID)`

Y-axis: `CPU%`

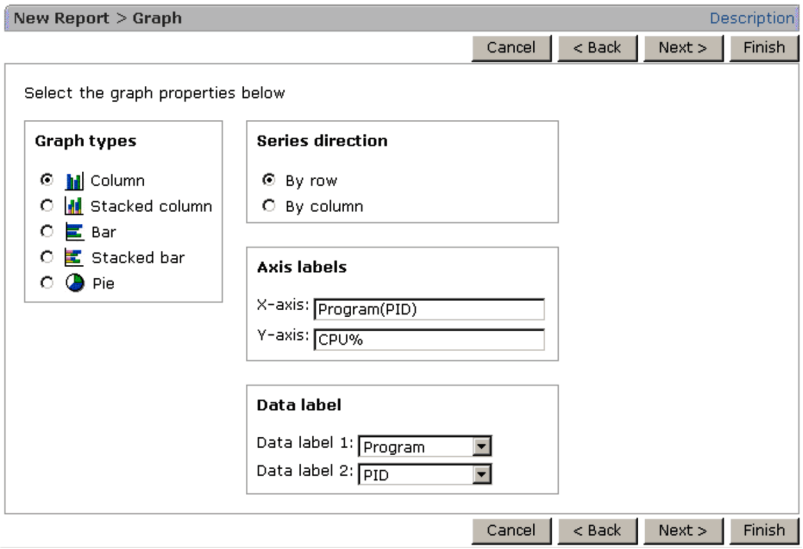
Data label

Data label 1: `Program`

Data label 2: `PID`

The following figure shows an example of entering information in the New Report > Graph window.

Figure 5-14: Example of input in the New Report > Graph window



2. Click the **Next >** button.

   The New Report > Drilldown windows appears. Go to *5.3.8 Associating a report with another report (drilldown report)*.

   Supplemental information:

   If you do not want to define a drilldown report, click the **Finish** button to close the report setting.

5.3.8 Associating a report with another report (drilldown report)

If necessary, set a drilldown report that is displayed by drilling down to the report, which is associated with the displayed report.

There are two types of drilldown reports that can be set according to which one best meets your purpose. You can also set both types.

- Setting a report-level drilldown report

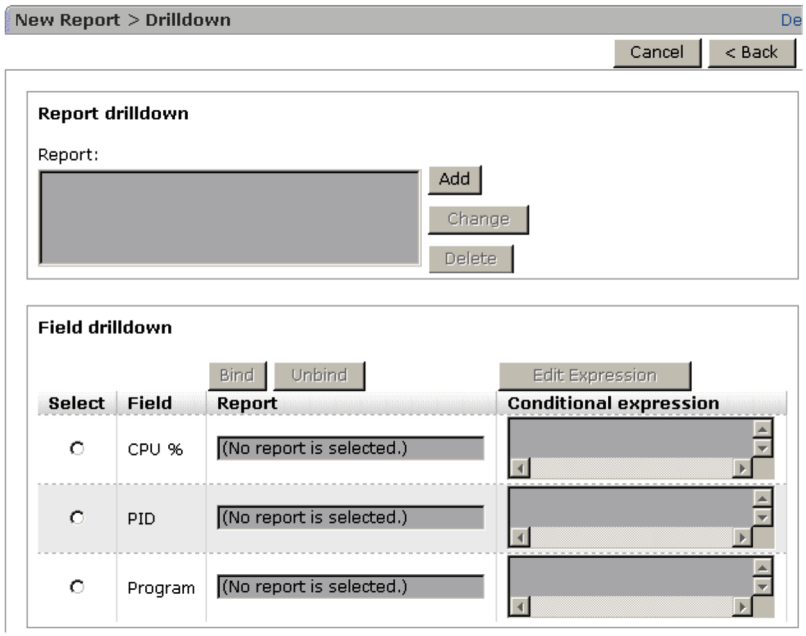
  To set this type of drill-down report, go to *(1) Defining a report-level drilldown report*.

- Setting a field-level drilldown report

  To set this type of drill-down report, go to *(2) Defining a field-level drilldown report*.

  The following figure shows an example of the New Report > Drilldown window.

Figure 5-15: New Report > Drilldown window



(1) Defining a report-level drilldown report

To define a report-level drilldown report:

1. Click the **Add** button in the New Report > Drilldown window.

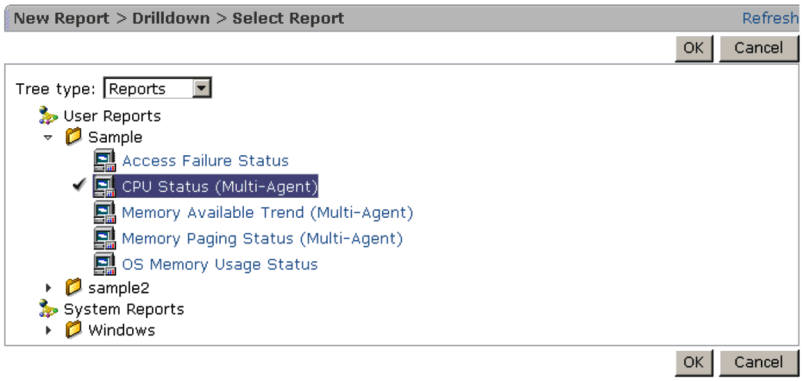
   The New Report > Drilldown > Select Report window appears.

2. Select a drilldown report to be associated with the report from the Reports tree.

   The selected report is marked with a checkmark. By selecting **Bookmarks** from the Tree type pull-down menu, you can assign a bookmark or combination bookmark as a drill-down report.

   The following figure shows an example of entering information in the New Report > Drilldown > Select Report window.

Figure 5-16: Example of using the New Report > Drilldown > Select Report window



3. Click the **OK** button.

   The drilldown report selected in step 2 is displayed in **Report** of the New Report > Drilldown window.

4. Click the **Finish** button.

   The New Report > Drilldown window closes and the report setting is finished.

(2) Defining a field-level drilldown report

To define a field-level drilldown report:

1. From **Field**, select the field you want to associate with the drilldown report.

   Click the **Select** option button of the field to be selected.

2. Click the **Bind** button.

   The New Report > Drilldown > Select Report window appears.

3. Select a drilldown report to be associated with the field from the Reports tree.

   The selected report is marked with a checkmark.

4. Click the **OK** button.

   The drilldown report selected in step 3 is displayed in **Report** of **Field drilldown** of the New Report > Drilldown window.

5. To set a conditional expression when displaying selected fields, click the **Edit Expression** button.

   The New Report > Drilldown > Edit Conditional Expression for Drilldown window appears.

6. Set the conditional expressions for the drilldown report.

For example, when displaying a drilldown report of the processes whose CPU usage ratio is higher than those of the processes displayed in the report window, set up the conditional expression as follows:

Conditional expression: `CPU % > CPU %`

`CPU %` at the left part indicates the CPU usage ratio displayed in the drilldown report. Specify this in the first **Field** of the New Report > Drilldown > Edit Conditional Expression for Drilldown window.

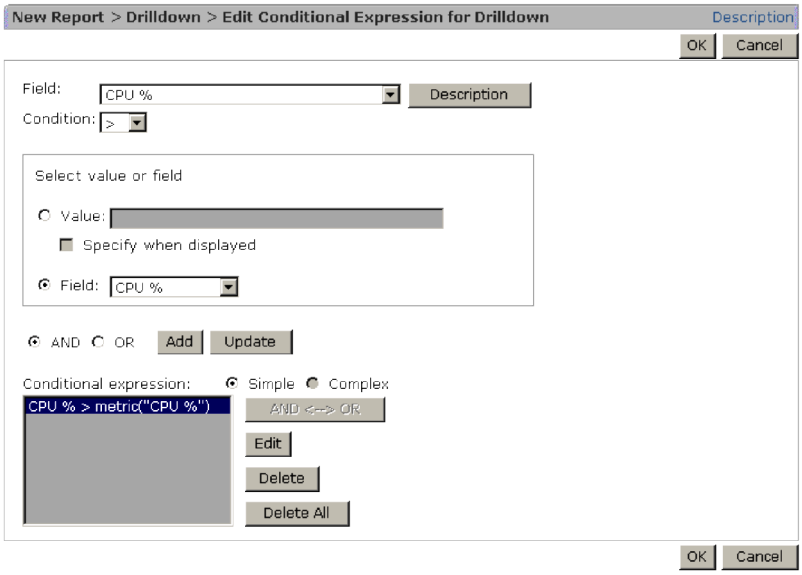
`CPU %` at the right part indicates the CPU usage ratio, as the source of drilldown report, displayed in the report window. Specify this in the **Field** of **Select value or field**.

7. Click the **OK** button.

   The New Report > Drilldown window appears. The conditional expression set in step 6 is displayed in **Conditional expression** of **Field drilldown**.

   The following figure shows an example of entering information in the New Report > Drilldown > Edit Conditional Expression for Drilldown window.

   Figure 5-17: Example of input in the New Report > Drilldown > Edit Conditional Expression for Drilldown window



8. Click the **Finish** button.

   The New Report > Drilldown window closes, and the report setting is finished.

5.3.9 Copying a report

To copy the monitoring template or an existing report:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select a report to be copied in the Reports tree of the navigation frame.

   The selected report is marked with a checkmark.

4. In the method frame, select the **Copy** method.

   In the information frame, the Copy window appears, and the Reports tree of the copy destination is displayed.

5. Select a folder as the copy destination or select **User Reports**.

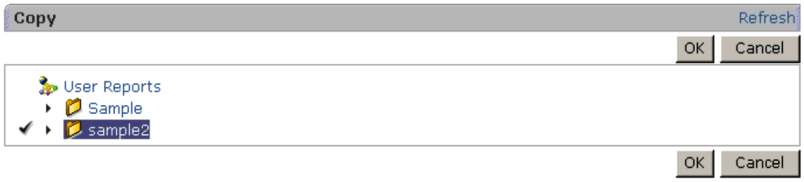
6. Click the **OK** button.

   The report selected in step 3 is copied to the folder or **User Reports** selected in step 5.

Reference note:

If a report with the same name already exists at the copy destination, a report named **Copy of** *report-name* is created.

Figure 5-18: Copy window



5.3.10 Editing a report

You can use the following two methods to edit a predefined report:

- Editing a report from the Reports window
- Editing a report from the report window

(1) Editing a report from the Reports window

To edit a predefined report from the Reports window:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.
2. In the navigation frame of the main window, choose the **Reports** tab.

   The Reports window appears.
3. Select a report to be edited in the Reports tree of the navigation frame.

   The selected report is marked with a checkmark.
4. In the method frame, select the **Edit** method.

   In the Information Frame, the Edit > Name and Type window appears.
5. Edit the report definition.

   The subsequent steps are similar to those when creating a new report.

   For details on the procedure, see from *5.3.3 Setting the name and type of a report* to *5.3.8 Associating a report with another report (drilldown report)*.
6. When you are finished editing, click the **Finish** button.

   Now the edited report definition is valid.

Notes:

- You cannot change reports provided as a monitoring template. If you want to customize the report definition of a monitoring template, copy the necessary report of the monitoring template, and edit the copied report definition.
- When modifying the created report, you cannot change **Product**. In addition, if **Report type** and **Record** are changed, definitions such as the filter condition and indication settings are reset, so you must set them again.

(2) Editing a report from the report window

To edit a report from the report window:

1. From the monitoring console browser, log on to PFM - Web Console.

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

   The Agents window is displayed.
3. From the navigation frame in the Agents tree window, select an agent.

   The selected agent is marked with a checkmark.
4. From the method frame, select **Display Reports**.

   A list of reports is displayed in the information frame.

5. Choose a report in the information frame.

   The report window appears in a new window.

6. Select the **Edit Report Definition** tab.

   You can edit the items listed below. For details on how to set each item, see *5.3.4 Setting fields displayed in a report* to *5.3.7 Setting the display format (table, list, or graph) of a report*. Note that you cannot edit **Name and Type** and **Drilldown**.

   - **Field** (Record names cannot be edited.)
   - **Filter**
   - **Indication settings**
   - **Components**
   - **Graph** (when a graph is selected)

7. When you are finished editing, click the **OK** button.

   Now the edited report definition is valid.

   If you want to save the edited report definition, display the report again, and then click the **Save Report Definition** anchor.

5.3.11 Renaming a folder or report

You can rename a report or a folder for storing reports.

(1) Renaming a report folder

To rename a folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select a folder to be renamed under **User Reports** in the Reports tree of the navigation frame.

   The selected folder is marked with a checkmark.

   You cannot rename **User Reports**.

4. In the method frame, select the **Rename** method.

   The Rename window appears in the information frame.

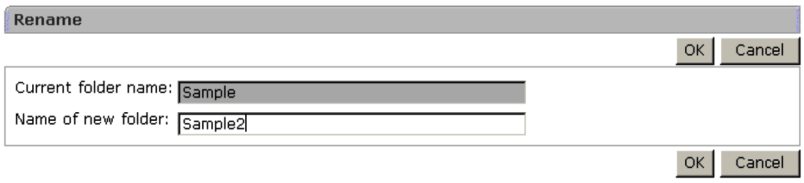
   The current folder name is displayed in **Current folder name**.

5. In **Name of new folder**, enter a new folder name (enter no more than 64

characters).

The following figure shows an example of the Rename window.

Figure 5-19: Rename window



6. Click the **OK** button.

   The folder selected in step 3 is renamed.

(2) Renaming a report

To rename a report:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select a report to be renamed under **User Reports** in the Reports tree of the navigation frame.

   The selected report is marked with a checkmark.

4. In the method frame, select the **Rename** method.

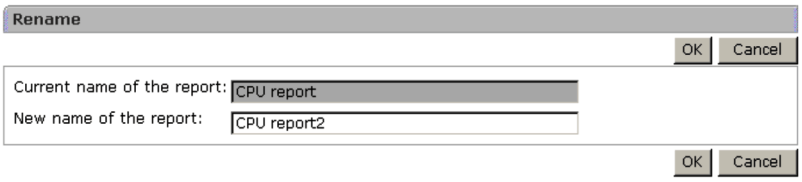
   The Rename window appears in the information frame,

   The current report name is displayed in **Current name of the report**.

5. In **New name of the report**, enter a new report name (enter no more than 64 characters).

   The following figure shows an example of the Rename window.

   Figure 5-20: Rename window



6. Click the **OK** button.

   The report selected in step 3 is renamed.

5.3.12 Deleting a folder or report

You can delete unnecessary folders or reports. When you delete a folder, folders and reports under the folder are also deleted.

(1) Deleting a report folder

To delete a report folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select a folder to be deleted under **User Reports** in the Reports tree of the navigation frame.

   The selected folder is marked with a checkmark.

4. In the method frame, select the **Delete** method.

   A message box appears to confirm the deletion.

5. Click the **OK** button in the message box.

   The folder selected in step 3 is deleted.

(2) Deleting a report

To delete a report:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. Select a report to be deleted under **User Reports** in the Reports tree of the navigation frame.

   The selected report is marked with a checkmark.

4. In the method frame, select the **Delete** method.

   A message box appears to confirm the deletion.

5. Click the **OK** button in the message box.

The report selected in step 3 is deleted.

5.3.13 Exporting reports

To export one or more reports:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.
2. In the navigation frame of the main window, choose the **Reports** tab.

   The Reports window appears.
3. Select the target to be exported in the Reports tree of the navigation frame.

   The report is exported according to the selected target as follows:

   - When the root **User Reports** is selected:

     Folders and all reports under **User Reports** are exported.
   - When a folder is selected:

   The selected folder and reports under it are exported.

   - When a report is selected:

     The selected report is exported.
4. In the method frame, select the **Export** method.

   The File Download window appears.
5. Click the **Save** button.

   The Save As window appears.
6. Specify the export destination and file name.

   The target selected in step 3 is output to the file specified here.
7. Click the **Save** button.

   The target selected in step 3 is exported.

Note:

You can export a report definition file from the PFM - Web Console window in binary format.

5.3.14 Importing a report

To import a report definition:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Reports window appears.

3. In the method frame, select the **Import** method.

   The Import window appears.

4. Click the **Browse** button of **Import file name**.

   The Choose File window appears.

5. Select the definition file of the report to be imported.

   The root, folders, and reports described in the definition file to be selected here are imported.

6. Click the **OK** button.

   A message box to confirm your replacement appears.

7. If you want to replace the report, click the **OK** button in the message box.

   The report is imported.

5.4 Creating reports by using the Quick Guide

You can use the Quick Guide to create a simplified report by setting the minimum items. For details on the default values of a report that was created by using the Quick Guide, see *5.4.3 Default values used for reports created with the Quick Guide*.

5.4.1 Procedure for creating reports by using the Quick Guide

(For details on how to create an alarm, see *6.5 Setting alarms by using the Quick Guide*.)

To create a report by using the Quick Guide:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window is displayed.

3. From the **Display format** pull-down menu in the navigation frame, choose the display format for the Agents tree.

   The Agents tree appears in the selected display format.

   - When **User Agents** is selected:

     The Agents tree that has **User Agents** (*logged-on-user-name*) as the root appears.

   - When **Products** is selected:

     The Agents tree that has **Products** as the root appears.

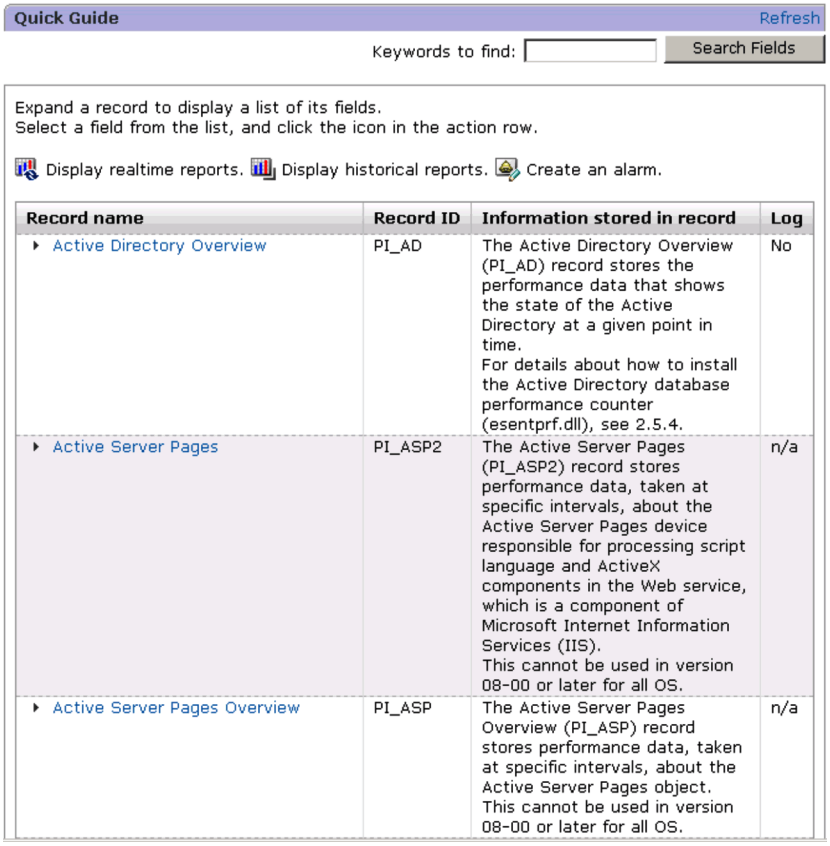
4. In the navigation frame, select the agent for which you want to create a report from the **Agents** tree.

   The selected agent is marked with a checkmark.

5. Choose the **Quick Guide** button in the method frame.

   The Quick Guide window appears.

Figure 5-21: Quick Guide window



6. View the fields used in creating the report.

   You can use either of the following methods to view fields:

   - Click and expand a record name anchor and select a field from the displayed list of fields.
   - Search the fields for a specific character string and select a field from the results.

     To search through fields, enter a character string into **Keywords to find:** and click the **Search Fields** button, or click the Search Fields window to display the Quick Guide > Search Fields window. For details on the searching fields, see *5.4.2 Searching fields*.

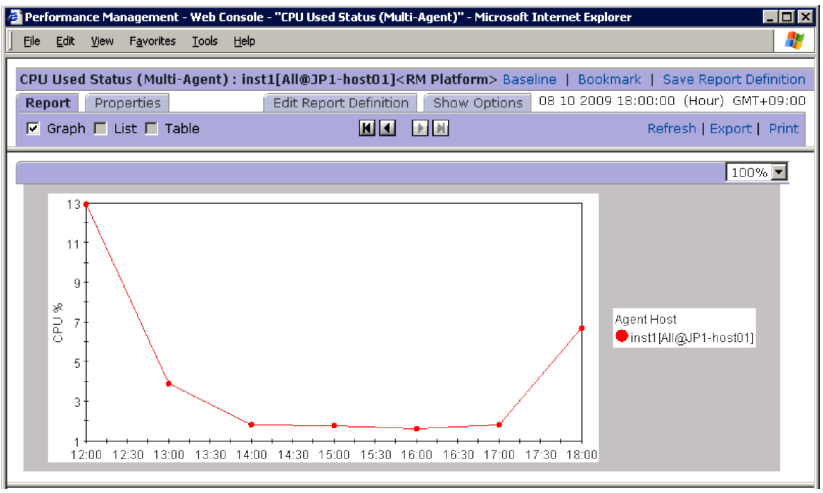
7. Click one of the report icons displayed in the field.

   When you select either the Realtime or Historical report icon, a Reports window

for reports created with the Quick Guide appears.

- Realtime report icon:
- Historical report icon:

Figure 5-22: Report window (Quick Guide)



8. Click the **Save Report Definition** anchor on the report window, specify a name for the report, and then save the report.

   The Save Report Definition window appears. Specify a destination folder and a name for the report, and then click the **OK** button to save the report.

5.4.2 Searching fields

(For details on operations that can be performed on the field search results, see the steps following field display in *5.4.1 Procedure for creating reports by using the Quick Guide*.)

To search for fields containing a particular character string using the Quick Guide window:

1. Click the **Search fields** button in the Quick Guide window.

   The Quick Guide > Search Fields window appears.

   If you entered a search keyword into **Keywords to find:** in the Quick Guide window the search results will be displayed. For details on the search results, see the description in step 3.

2. Select an option from the **Records to search:** pull-down menu.

The pull-down menu provides the following options:

- **--All records--**

  Select this option to search all records.

- **--Records where Log=Yes--**

  Select this option to search records with the Log property set to `Yes`. This option is available if the agent is running when the window opens.

- A list of record names for the selected agent

  A list of record names for the selected agent appears in alphabetical order.

3. Enter a character string for the field search into **Keywords to find** and click the **Search** button.

   The search results are shown in **Search Result:**.

   - If **--All records--** is selected for the record search

     Results are listed by record in the Search Results: record(s) window.

     Click a record name anchor to show a list of resulting fields.

   - If **--Records where Log=Yes--** is selected for the record search

     Results are listed by record in the Search Result: record(s) window.

     Click a record name anchor to show a list of resulting fields.

   - If a record name is selected for the record search

     A list of resulting fields appears.

5.4.3 Default values used for reports created with the Quick Guide

Default values used for reports created with the Quick Guide are shown below. The same default values are used for reports displayed when you click the Display Preview icon on the Quick Guide > Create Alarm window.

Table 5-1: Default values used for reports created with the Quick Guide

Item		Default value	Edition
Name and Type	Report name	(New report)	--
	Product	Product type of the selected agent	--
	Report type	Report type of the selected agent	Y[#1]
Field	Record	Record to which the field that was selected in the window for selecting fields belongs	Y

Item		Default value	Edition
	Whether the field is selected	The field that was selected in the window for selecting fields (If there is an ODBC key field, all of the ODBC key fields are also included.)	Y#2
Filter		None	--
Indication settings	Realtime report	Specify when displayed: Off Indicate delta value: On Refresh interval Do not refresh automatically: Off Initial value: 60 Minimum value: 60 Display by ranking Field: None In descending order: Off	
	Historical report	Specify when displayed: Off Maximum number of records: 1440 Settings for the report display period Date range: Within the past hour Report interval: None (Minute when the specified record is the PI record) Field in Peak time: None	
Components	Field	Table: On List: Off Graph: On only if the value stored in the selected field is numerical.	
	Display key	Display name: Off Display key: Off	
Drilldown		None	

Legend:

Y: You need to specify the setting for this item.

--: You can omit this item.

#1:

You can use the Quick Guide to create historical reports and realtime reports only.

#2:

You cannot select multiple fields.

5.5 Creating reports by using commands

In PFM - Web Console, you can perform the following report operations using commands:

- Output and customize report definition information
- Delete unnecessary reports

5.5.1 Outputting and customizing report definitions

To output and customize existing report definitions and to register the report with PFM - Web Console:

1. Describe the report whose definition you want to output in the report definition file (XML format).

   For example, to output report definitions of `report1` and `report2` stored in the `report_win` folder under **User Reports**, describe the report as follows:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE pr-cli-parameters SYSTEM
   "rdef_output_params.dtd">
   <pr-cli-parameters ver="0110">
   <report-definitions>
   <report-definition name="report1" parent-folder="/
   report_win"/>
   <report-definition name="report2" parent-folder="/
   report_win"/>
   </report-definitions>
   </pr-cli-parameters>
   ```

2. Save the report definition file in step 1.
3. Execute the `jpcrdef output` command.

   For example, to output the report definition described in the report definition file `rdef_input_win.xml` to the destination report definition file `rdef_output_win.xml`, the specification could be as follows:

   ```
   jpcrdef output -o rdef_output_win.xml rdef_input_win.xml
   ```

   For details on the `jpcrdef output` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
4. Edit the report definition file output in step 3.

For details on how to edit a definition file for a report, see the topic that describes the `jpcrdef create` command in the manual *Job Management Partner 1/ Performance Management Reference*.

5. Save the report definition file edited in step 4.
6. Register the report definition edited in step 4 by executing the `jpcrdef create` command.

   For example, to use the report definition file `rdef_output_win.xml`, the specification could be as follows:

   ```
   jpcrdef create rdef_output_win.xml
   ```

   For details on the `jpcrdef create` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

Note:

You need to edit the report definition file in the prescribed format. Note that if you edit or create it in any format other than the prescribed one, it might not operate normally.

5.5.2 Deleting an unnecessary report

To delete an unnecessary report by using a command:

1. Describe the report to be deleted in the definition file used by the command (XML format).

   For example, to delete report definitions of `report1` and `report2` stored in the `report_win` folder under **User Reports** folder, describe the report as follows:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE pr-cli-parameters SYSTEM
   "rdef_delete_params.dtd">
   <pr-cli-parameters ver="0110">
   <report-definitions>
   <report-definition name="report1" parent-folder="/
   report_win"/>
   <report-definition name="report2" parent-folder="/
   report_win"/>
   </report-definitions>
   </pr-cli-parameters>
   ```

   For details on how to edit a definition file for a report, see the topic that describes the `jpcrdef create` command in the manual *Job Management Partner 1/*

Performance Management Reference.

2. Save the report definition file in step 1.
3. Delete the report by executing the `jpcrdef delete` command.

   For example, to use the report definition file `rdef_del_win.xml`, the specification could be as follows:

   ```
   jpcrdef delete -y rdef_del_win.xml
   ```

   For details on the `jpcrdef delete` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

Note:

You need to edit the report definition file in the prescribed format. Note that if you edit or create it in any format other than the prescribed one, it might not operate normally.

5.6 Creating and editing bookmarks by using a browser

This section describes how to register reports with a bookmark, and how to display a combination report by registering a baseline in a combination bookmark.

5.6.1 Creating bookmarks

The following describes how to register a bookmark with a report.

(1) Creating and registering a new bookmark (new registration)

To create a new bookmark and register a report with it:

(a) To display and register a report

1. Display the report window for the report to be registered with a bookmark.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

   For details on how to display the report window for reports created by using the Quick Guide, see *5.4 Creating reports by using the Quick Guide*.

2. Click the **View Report** tab.

3. Select the **Bookmark** menu on the menu bar.

   The Bookmark window appears, and the Bookmarks tree is displayed.

4. To create a new folder for storing bookmarks, select the location where you want to create the folder, and click the **New Folder** button.

   A window appears where you can enter a name for the new folder.

   If you do not want to create a new folder, select the location where you want to create the bookmark, and go to step 7.

5. Enter a name for the new folder.

   Name

   Enter no more than 64 characters.

6. Click the **OK** button.

   The created folder is added and displayed as selected in the Bookmarks tree of the Bookmark window.

7. In **Type a name of the bookmark**, enter the name of the bookmark with which you want to register the report.

   Type a name of the bookmark

   Enter no more than 64 characters.

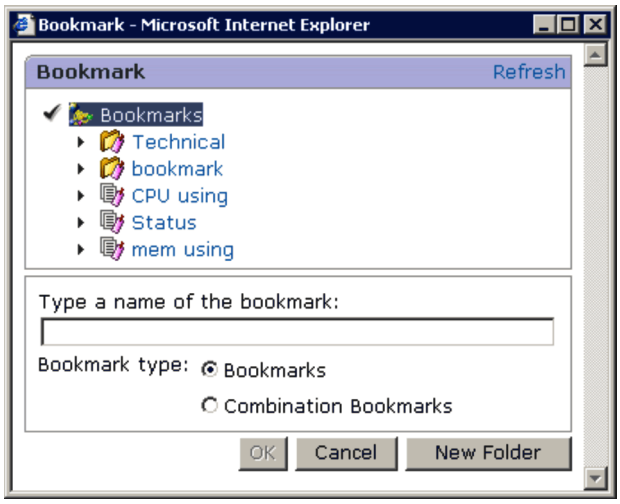
8. In **Bookmark type**, select the type of bookmark.

   To register the report with a bookmark, select **Bookmarks**. To register the report with a combination bookmark, select **Combination Bookmarks**.

   Note that you cannot register a realtime report with a combination bookmark.

   The following figure shows an example of the Bookmark window.

   Figure 5-23: Bookmark window 1



9. Click the **OK** button.

   The report is registered with the bookmark you entered in step 7.

(b) To register a report without displaying it

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select an agent whose reports you want to display.

   The selected agent is marked with a checkmark.

   If you select **Multiselect**, you can select multiple agents simultaneously.

4. In the method frame, select the **Register Bookmark** method.

   The Register Bookmark > Select Report window appears in the information frame. When you click a report definition in the reports tree, the Bookmark window appears with the Bookmarks tree displayed.

5. Go to step 4 of *(a) To display and register a report* in *(1)* above.

(2) Registering a report with an existing bookmark (additional registration)

To register a report with an existing bookmark:

(a) To display and register a report

1. Display the report window for the report to be registered with a bookmark.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. Click the **View Report** tab.

3. Select the **Bookmark** menu on the menu bar.

   The Bookmark window appears.

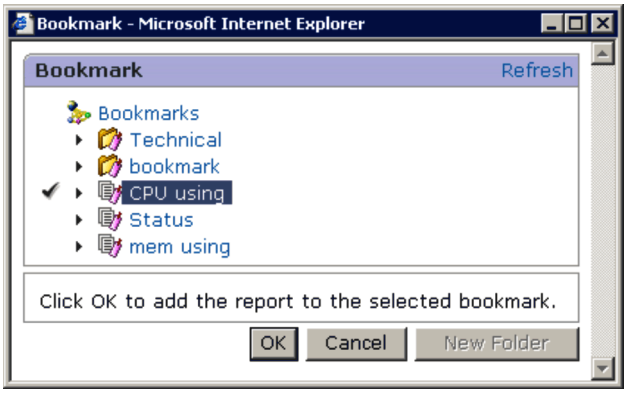
4. In the Bookmarks tree, select the bookmark with which you want to register the report.

   Click OK to add the report to the selected bookmark appears in the Bookmark window, and the selected bookmark is marked with a checkmark.

   You cannot register the following types of report with a combination bookmark:

   - Realtime reports
   - Reports that do not display graphs
   - Reports for which a display key field is specified

   Figure 5-24: Bookmark window 2



5. Click the **OK** button.

   The report is registered with the bookmark you selected in step 4.

Note:

If a bookmark is used to view reports, each of the registered reports is displayed

in a separate window. As the number of reports to display increases, it takes correspondingly longer to display the reports. For this reason, we recommend that you register no more than 10 reports with any one bookmark.

(b) To register a report without displaying it

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select an agent whose reports you want to display.

   The selected agent is marked with a checkmark.

   If you select **Multiselect**, you can select multiple agents simultaneously.

4. In the method frame, select the **Register Bookmark** method.

   The Register Bookmark > Select Report window appears in the information frame. When you click a report definition in the reports tree, the Bookmark window appears with the Bookmarks tree displayed.

5. Go to step 4 of *(a) To display and register a report* in *(2)* above.

(3) Updating a report registered with an existing bookmark (update registration)

To register an updated version of a report already registered with an existing bookmark:

(a) To display and register a report

1. Display the report window for the updated report.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. Click the **View Report** tab.

3. Select the **Bookmark** menu on the menu bar.

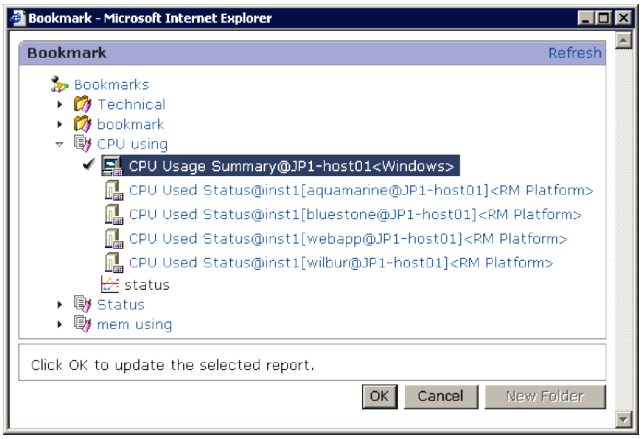
   The Bookmark window appears.

4. In the Bookmarks tree, select the registered report that you want to overwrite with the updated version.

   Click OK to update the selected report appears in the Bookmark window, and the selected bookmark is marked with a checkmark.

   The following figure shows an example of the Bookmark window.

Figure 5-25: Bookmark window 3



5. Click the **OK** button.

   The registered report you selected in step 4 is updated.

(b) To register a report without displaying it

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select an agent whose reports you want to display.

   The selected agent is marked with a checkmark.

   If you select **Multiselect**, you can select multiple agents simultaneously.

4. In the method frame, select the **Register Bookmark** method.

   The Register Bookmark > Select Report window appears in the information frame. When you click a report definition in the reports tree, the Bookmark window appears with the Bookmarks tree displayed.

5. Go to step 4 of *(a) To display and register a report* in *(3)* above.

5.6.2 Adding a bookmark folder

To add a folder for storing bookmarks:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

2. In the navigation frame of the main window, select the **Bookmarks** tab.

The Bookmarks window appears.

3. In the navigation frame, select **Bookmarks** or a folder under **Bookmarks** as the location for the folder.

   The selected folder is marked with a checkmark.

4. In the method frame, select the **New Folder** method.

   In the information frame, the New Folder window appears.

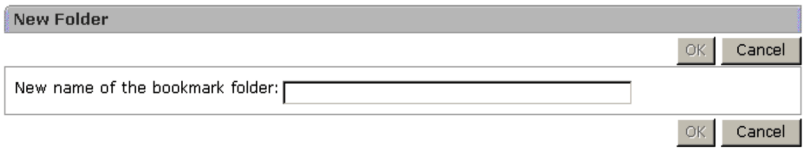
5. In **Name of new folder**, enter a name for the folder.

   Name of new folder

   Enter no more than 64 characters.

   The following figure shows an example of the New Folder window.

   Figure 5-26: New Folder window



6. Click the **OK** button.

   A folder is added just below the **Bookmarks** folder or the folder selected in step 3.

5.6.3 Renaming folders and bookmarks

You can rename bookmarks and the folders where bookmarks are stored.

(1) Renaming a bookmark folder

To rename a folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

3. Select a folder to rename in the Bookmarks tree of the navigation frame.

   The selected folder is marked with a checkmark.

4. In the method frame, select the **Rename** method.

   The Rename window appears in the information frame.

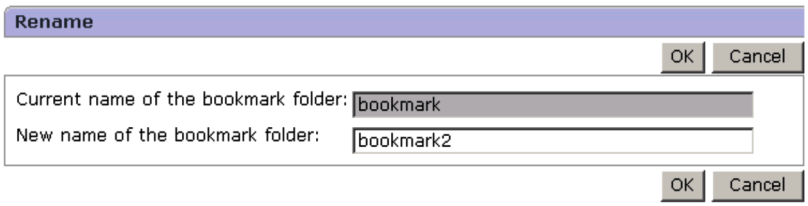
   The folder name selected in step 3 is displayed in **Current folder name**.

5. In **Name of new folder**, enter a new folder name.

   Name of new folder

   Enter no more than 64 characters.

   Figure 5-27: Rename window 1



6. Click the **OK** button.

   The folder selected in step 3 is renamed.

(2) Renaming a bookmark

To rename a bookmark:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

3. Select a bookmark to rename in the Bookmarks tree of the navigation frame.

   The selected bookmark is marked with a checkmark.

4. In the method frame, select the **Rename** method.

   The Rename window appears in the information frame.

   The name of the bookmark selected in step 3 is displayed in **Current name of the bookmark**.

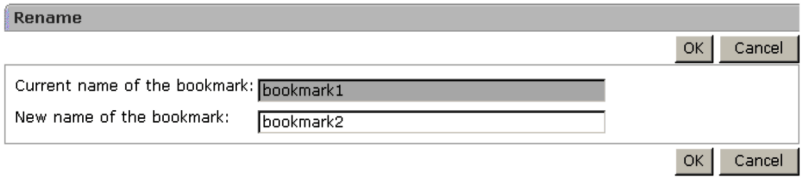
5. In **New name of the bookmark**, enter a new bookmark name.

   New name of the bookmark

   Enter no more than 64 characters.

   The following figure shows an example of the Rename window.

Figure 5-28: Rename window 2



6. Click the **OK** button.

   The bookmark selected in step 3 is renamed.

Note:

When you rename a bookmark, any drilldown reports will still reference the old bookmark name. Reconfigure the drilldown reports in the Edit > Drilldown window for each report definition.

5.6.4 Deleting folders, bookmarks, and reports

You can delete unnecessary folders, bookmarks, and reports. When you delete a folder, everything under the folder is deleted. When you delete a bookmark, any reports registered under the bookmark are also deleted.

(1) Deleting a bookmark folder

To delete a bookmark folder:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

3. Select the folder to delete in the Bookmark tree of the navigation frame.

   The selected folder is marked with a checkmark.

4. In the method frame, select the **Delete** method.

   A message box appears prompting you to confirm the deletion.

5. Click the **OK** button in the message box.

   The folder selected in step 3 is deleted.

(2) Deleting a bookmark

To delete a bookmark:

1. From the monitoring console browser, log on to PFM - Web Console.

The main window appears.

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

   The Bookmarks window appears.

3. Select the bookmark to delete in the Bookmark tree of the navigation frame.

   The selected bookmark is marked with a checkmark.

4. In the method frame, select the **Delete** method.

   A message box appears prompting you to confirm the deletion.

5. Click the **OK** button in the message box.

   The bookmark selected in step 3 is deleted.

(3) Deleting a report from a bookmark

To delete a report:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

3. Select the report to delete in the Bookmark tree of the navigation frame.

   The selected report is marked with a checkmark.

4. In the method frame, select the **Delete** method.

   A message box appears prompting you to confirm the deletion.

5. Click the **OK** button in the message box.

   The report selected in step 3 is deleted.

Supplemental information:

When you delete the last report registered with a bookmark, the bookmark is also deleted. In this case, a message appears prompting you to confirm deletion of the bookmark.

5.6.5 Checking the properties of a bookmark

To check the properties of a bookmark:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

The Bookmarks window appears.

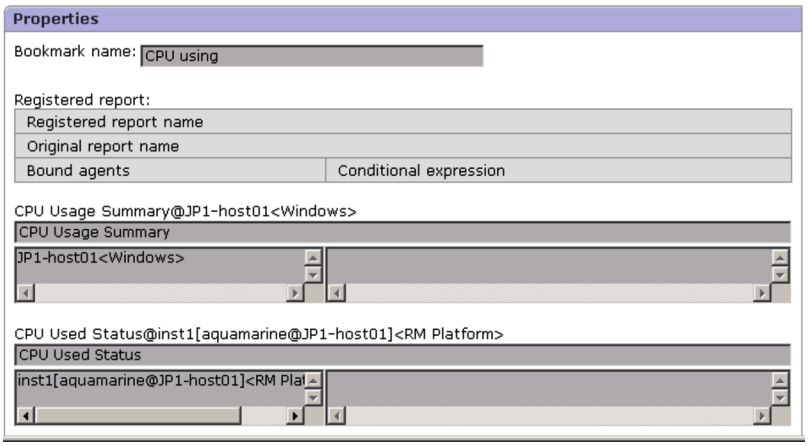
3. Select the bookmark whose properties you want to check in the Bookmarks tree of the navigation frame.

   The selected bookmark is marked with a checkmark.

4. In the method frame, select the **Properties** method.

   The Properties window appears in the information frame.

   Figure 5-29: Properties window



5.6.6 Tiling display of reports registered in bookmarks

You can display side-by-side graphs of multiple historical reports, which are managed using a bookmark, in an information frame by using the tiling display. You can also rearrange displayed graphs or click a displayed graph to view the report for the graph.

Tiled display of graphs is only valid for historical reports that have graph display enabled. It cannot be used for historical reports that have graph display disabled or for realtime reports.

(1) Procedure for displaying graphs in tiling display

To display graphs in tiling display:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

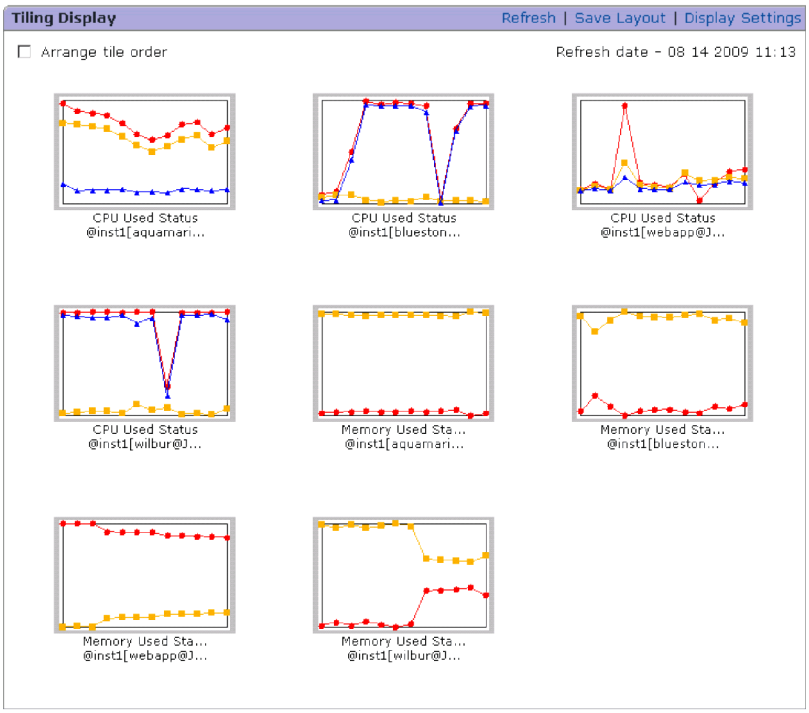
3. Select a bookmark for which you want to display graphs in tiling display in the Bookmarks tree of the navigation frame.

The selected bookmark is marked with a checkmark.

4. Select the **Tiling Display** method in the method frame.

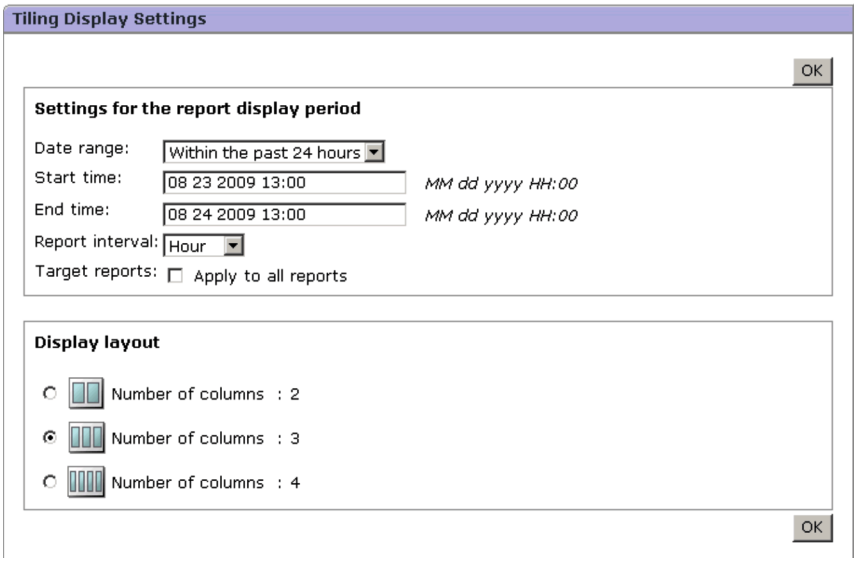
When you specify something other than **Specify when displayed** for the date range of historical reports that are registered in a bookmark, the Tiling Display window is displayed in the information frame. The following figure shows an example of the Tiling Display window.

Figure 5-30: Tiling Display window



If you select **Specify when displayed** when the date range for a bookmarked historical report is displayed, the Tiling Display Settings window appears. The Tiling Display Settings window can also be displayed using the Display Settings menu in the Tiling Display window. The following figure shows an example of the Tiling Display Settings window.

Figure 5-31: Tiling Display Settings window



5. Set the individual items for the Tiling Display Settings window.

   Set display conditions for the following items, if necessary:

   Settings for the report display period

   Date range

   From the pull-down menu, select the date range for the data to be displayed in graphs that are displayed in tiling display. The selectable values are as follows:

   - Specify when displayed

   - Within the past hour

   - Within the past 24 hours

   - Within the past 7 days

   - Within the past month

   - Within the past year

   The default is **Within the past 24 hours**.

   When you select something other than **Specify when displayed**, the dates and times corresponding to the **Start time** and **End time** are automatically set.

Start time and **End time**

When you select **Specify when displayed** in **Date range**, set the start time and end time of the date range for graphs that are displayed in tiling display.

Specify the **Start time** and **End time** in *YYYY MM DD hh:mm* format (*YYYY* = year, *MM* = month, *DD* = day, *hh* = hour, *mm* = minute).

The range of dates and times you can specify is from 1971/01/01 00:00 to 2035/12/31 23:59. For the **End time**, specify a date and time after the **Start time** you specified.

Note that when you select something other than **Specify when displayed**, the appropriate date and time is automatically set. Additionally, if you change the date and time that are automatically displayed, settings for the **Date range** change to **Specify when displayed**.

Report interval

From the pull-down menu, select a report interval from the ones listed below. The default is displayed according to the date range selected in **Date range**.

- **Minute**
- **Hour**
- **Day**
- **Week**
- **Month**
- **Year**

Target reports

Use the **Apply to all reports** check box to switch the target of the settings specified in **Settings for the report display period**. The default is that the check box is cleared.

If the check box is selected, the settings will be applied to all reports regardless of the report definitions.

If the check box is cleared, the settings will only be applied to reports for which **Specify when displayed** is specified for **Date range**.

Display layout

Specify the maximum number of graphs to be arranged next to in the Tiling Display window. The selectable values are as follows:

- **Number of columns: 2**
- **Number of columns: 3**
- **Number of columns: 4**

6. After you finish specifying the settings, click the **OK** button.

   The Tiling Display window is displayed with the specified settings applied.

Note

If the value specified in **Display Layout** is changed, the default graph layout (in the order of the report names) is used.

(2) Rearrange graphs

By using the tiling display, you can rearrange graphs that are displayed in the information frame.

To rearrange graphs:

1. Display the Tiling Display window.
2. In the Tiling Display window, select the **Arrange tile order** check box.

   In the Tiling Display window, a grid frame is displayed.
3. Select the display area of the source graph that is surrounded by a grid frame.

   From the selected area, the graph will be moved. You can also select an area where no graph is displayed.
4. Select the destination area enclosed with grid lines.

   The area selected as the source is replaced with the area selected as the destination. You can also select an empty area with no graph as the destination.
5. Repeat steps 3 and 4 until the change in layout is complete, and then clear the **Arrange tile order** check box.

   The grid lines disappear from the Tiling Display Settings window.

(3) Saving a layout

You can save settings for the Tiling Display window specifying the maximum number of graphs to be displayed side-by-side and the sorting order of the graphs.

To save the settings:

1. Display the Tiling Display window.
2. Change the maximum number of graphs displayed side-by-side or the layout of the graphs, as required.
3. Select the **Save Layout** menu in the Tiling Display window.

A message appears asking you to confirm whether to save the layout. If a layout already exits, the existing layout is overwritten.

Note:

If any of the bookmarked reports is deleted or if a new report is registered with the bookmark, the saved layout becomes invalid. In this case, the value for the maximum number of graphs to be displayed side-by-side becomes the default value of three, and the graphs are displayed in the order of the report names registered with the bookmark.

(4) Display a report

You can view the report for a specific graph by clicking the graph in tiled display.

The displayed report window and report display date range depend on conditions such as the tiled display settings and the settings for the report display data ranges of reports registered with the bookmark. The conditions affecting the displayed report window and display date range are described below.

Displayed report window

If **Specify when displayed** is selected as the data range for reports registered with the bookmark, the window of the **Show Options** tab appears.

If **Specify when displayed** is not selected as the data range for reports registered with the bookmark, the window of the **View Report** tab appears.

Date range for report display

For a report window displayed when a graph in tiled display is clicked, the data range specified in the Tiling Display Settings window supersedes the date ranges for the reports registered with the bookmark.

5.7 Displaying reports

This section describes the following operations regarding displaying reports:

- Displaying a report
- Checking the report properties (definitions)
- Changing the display conditions of a report
- Displaying a drilldown report

5.7.1 Displaying reports

You can display a report in the following ways:

- Displaying a report by specifying a specific agent
- Displaying a report associated with an alarm
- Displaying a report from the Event Monitor window
- Displaying a report from the Bookmarks window
- Displaying a report from the tiling display in the Bookmarks window

Each procedure is described below.

(1) Displaying a report by specifying a specific agent

To display one or more reports by specifying a specific agent:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select an agent whose report you want to display.

   The selected agent is marked with a checkmark.

   If you select **Multiselect**, you can select multiple agents simultaneously.

Hint:

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the object.

4. In the method frame, select the **Display Reports** method.

   In the information frame, the Reports window appears.

The contents of the View Report > Select Report window depends on the selected tree type.

If **Report** is selected as the tree type, see *(a) When the tree type is Report*, described below. If **Bookmark** is selected as the tree type, see *(b) When the tree type is Bookmark*, described below.

Note:

When no report is displayed:

If no historical report is displayed, check the record setting of the Store database as a target item of the report.

- The value of Log is `Yes`
- The value of Collection Interval is 1 or more

Make sure the setting is the same as above. Because historical reports use and display collected past data, if the target records are not set to be recorded in the Store database, they cannot be displayed.

If no combination report is displayed, the target registered reports might not be set. In this case, set registered reports by editing the combination bookmark.

Reference note:

Reports are displayed as described below.

When the tree type is Report:

- If a single agent is selected

  If more than one report is selected, each report is displayed in a separate window.

- If more than one agent is selected and **Historical (single agent) report** or **Realtime (single agent) report** is selected

  A report window is displayed for each of the agents.

- If more than one agent is selected and **Historical (multiple agents) report** is selected

  A single report window is displayed for all the agents.

When the tree type is Bookmark:

- One or more agents selected when the bookmark was registered are used, regardless of how many agents (single or multiple) are specified.
- If a bookmark (a non-combination bookmark) is selected

  A report is displayed in a separate window for each of the reports registered with the bookmark.

(a) When the tree type is Report

1. Select a report from the reports tree.

   The reports tree shows reports for the same product as those for an agent selected from the navigation frame of the Agents tree window.

   - Viewing a single report

     When a report is selected from the reports tree, the report is displayed in a separate window.

     If **Specify when displayed** is selected as the field display condition when creating the report, the Show Options window appears as a separate window. When you complete editing the Show Options window, click the **OK** button to display the report.

   - Viewing multiple reports

     You can select more than one report from the reports tree by selecting **Multiselect**. This option is not available if more than one monitoring agent is selected from the navigation frame in the Agents tree window.

     Select more than one report from the reports tree and click the **OK** button.

Each report is displayed in a separate window.

If **Specify when displayed** is selected as the field display condition when creating a report, the Show Options window appears as a separate window. When you complete editing the Show Options window, click the **OK** button to display the report.

(b) When the tree type is Bookmark

1. Select a bookmark or registered report from the Bookmark tree.

   When a bookmark or registered report is selected from the bookmarks tree, the report is displayed in a separate window.

(2) Displaying a report associated with an alarm

You can display a report associated with an alarm and analyze the cause of the generated alarm.

To display a report associated with an alarm:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select an agent whose report you want to display.

   The selected agent is marked with a checkmark.

Hint:

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the object.

4. In the method frame, select the **Display Alarm Status** method.

   In the information frame, the Alarm Status window appears. For an alarm with an associated report, the report icon (for Agent for Platform,  or ) is displayed next to the alarm icon ().

   For details on how to associate a report with an alarm, see *6.4.6 Associating a report with an alarm*.

5. Select the report icon whose report you want to display.

   The report window of the selected report icon is displayed in a separate window.

Supplemental information: When the window of the Show Options tab is displayed:

If the display conditions are set to be set when displaying the report, the window of the **Show Options** tab is displayed when initially displaying the report window. In this case, if you set display conditions as needed and click the **OK** button, the window of the **View Report** tab is displayed.

(3) Displaying a report from the Event Monitor window

The window which displays events of Performance Management system in a list is called an *Event Monitor* window. In the Event Monitor window, you can display a report previously associated with an alarm.

For details on how to display a report in the Event Monitor window, see *7.1.2 Displaying a report associated with an alarm*.

For details on how to associate a report with an alarm, see *6.4.6 Associating a report with an alarm*.

(4) Displaying a report from the Bookmarks window

You can register reports with a bookmark. For details on how to do this, see *5.6.1 Creating bookmarks*.

To display a report registered with a bookmark:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

3. Select reports from the Bookmark tree of the navigation frame.

   The selected report is marked with a checkmark.

4. From the method frame, choose the **Display Reports** method.

   The report window of the report selected in step 3 is displayed in a separate window.

(5) Displaying a report from the tiling display of a bookmark

By using the tiling display in the Bookmarks window, you can display reports from the thumbnail of the historical report being displayed.

For details on how to display reports from the thumbnail in the tiling display, see *5.6.6 Tiling display of reports registered in bookmarks*.

5.7.2 Checking the report properties (definition)

You can check the report definition by the following methods:

- Checking the report definition in the **Properties** tab of the report window
- Checking the report definition from the Reports tree

(1) Displaying the report definition in the Properties tab of the report window

To check the report definition in the **Properties** tab of the report window:

1. Display the report window for checking the properties (definition) in the window of PFM - Web Console.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. Select the **Properties** tab of the report window.

   The report definition is displayed in the **Properties** tab.

Note:

The **Properties** tab of the report window displays report definition information, but not display settings information. Therefore, even if you change the display conditions in the **Report Display Settings** tab, the displayed information of the properties will not be changed.

(2) Displaying the report definition from the Reports tree

To check the report definition from the Reports tree:

1. In the navigation frame of the Reports tree, select the report definition that you want to display.
2. In the method frame, select the **Properties** method.

   The properties window for the selected report definition appears.

5.7.3 Setting the display conditions for a report

You can set the display conditions for a report in the following two ways:

- Set the display conditions when defining the report

  Set the report display conditions when defining the report by using the window of PFM - Web Console or by using the `jpcrdef create` command.

  The display conditions set when defining a report are permanently registered in the PFM - Web Console system. This will not be affected with operations such as opening or closing of the window, startup, and exit from the system. These conditions are permanently registered until deleted from the PFM - Web Console system in the window of PFM - Web Console or through the `jpcrdef delete` command.

- Set the display conditions when or while displaying the report

  Set the report display conditions in the **Show Options** tab of the report window when you first display the report or while it is displayed.

  The report display conditions set in the **Show Options** tab are restricted to the window where the display conditions are set or changed, and are not permanent. For example, even if the same report is displayed in a separate window at the same time, the contents set in the **Show Options** tab are applied only to the window where the operation is carried out. In addition, display conditions that are set or changed in one window are retained until the window closes.

This subsection describes how to set display conditions in the **Show Options** tab of the report window when first displaying the report or while displaying the report. Note that you can set the report display conditions by using the function for editing the displayed report. For details on the function for editing the displayed report, see *5.3.10 Editing a report*.

(1) Setting display conditions when first displaying a report

To set display conditions when first displaying the report, set the following when defining the report:

- When setting the collection interval and retrieval interval of data

  Report definition in the PFM - Web Console window:

  Select **Specify when displayed** in the New Report > Indication Settings window.

  Report definition in command input:

  Specify `TRUE` for the `specify-when-displayed` attribute of the `indication-settings` parameter. Alternatively, omit the child element `date-range` of the `indication-settings` parameter.

- When setting the data filter conditions

  Report definition in the PFM - Web Console window:

  Select **Specify when displayed** in the New Report > Filter window.

  Report definition in command input:

  Specify `TRUE` for the `Specify-when-displayed` attribute of the `record - condition-expression - expression` parameter.

  The sign - (hyphen) indicates a layer when defining the report. `record - condition-expression` means to specify `condition-expression` for a child element of the `record` parameter.

- When setting the collection interval and retrieval interval of data and filter conditions

Report definition in the PFM - Web Console window:

Select **Specify when displayed** in the New Report > Indication settings window.

Also, select **Specify when displayed** in the New Report > Filter window.

Report definition in command input:

Specify `TRUE` for the `specify-when-displayed` attribute of `indication-settings` parameter. Alternatively, omit the child element `date-range` of `indication-settings` parameter.

Specify `TRUE` for the `Specify-when-displayed` attribute of the `record - condition-expression - expression` parameter.

The sign - (hyphen) indicates a layer when defining the report. `record - condition-expression` means to specify `condition-expression` for a child element of the `record` parameter.

To set the display conditions when first displaying the report:

1. Display the report window to set display conditions.

   In the initial display of the report window, the **Show Options** tab window is displayed automatically.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. Set the display condition.
3. Click the **OK** button.

   The report window affected by the display conditions of step 2 is displayed.

(2) Setting display conditions while displaying a report

Use this procedure if you want to change display conditions each time you display the report.

To set display conditions while displaying a report:

1. Display the report window to set display conditions.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. Click the **Show Options** tab in the report window.

   The window of the **Show Options** tab is displayed.

3. Set the display condition.
4. Click the **OK** button.

   The report window affected by the display conditions of step 3 is displayed.

5.7.4 Displaying a drilldown report

This subsection describes how to display a drilldown report associated with the displayed report based on drilldown report types.

The drilldown report types are as follows:

Report-level drilldown report

This displays a report from another report.

Field-level drilldown report

This displays the details of a report.

This also displays a drilldown report that is automatically set for time item fields.

About displaying a drilldown report:

A drilldown report is displayed in a separate window from that of the parent report. You can further open another drilldown report from a parent report while displaying a drilldown report, and can open a drilldown report from the drilldown report itself. If you close the parent report window by using **Close**, the drilldown report window also closes accordingly. However, processing other than closing the window is not reflected in the drilldown report window.

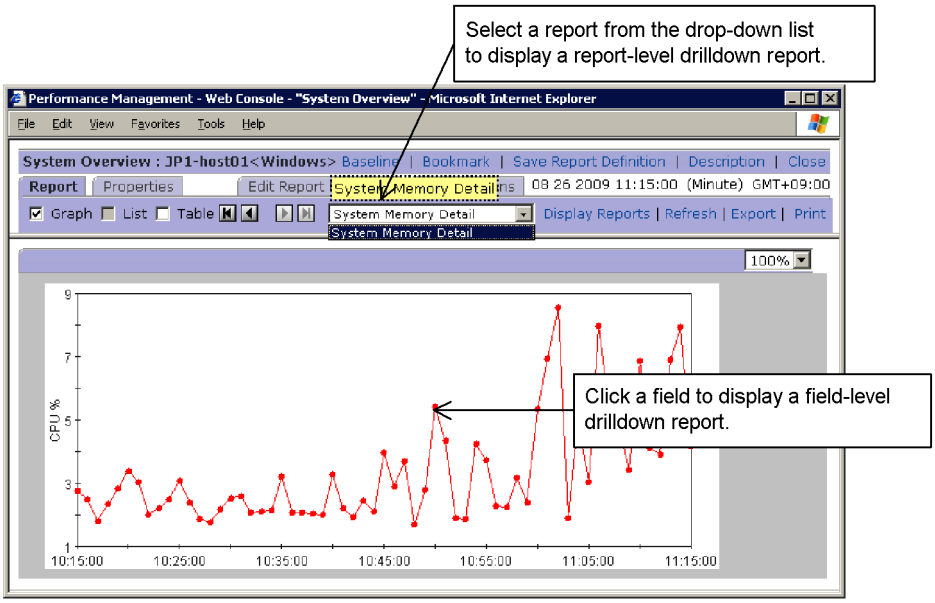
(1) Displaying a report-level drilldown report by specifying the report name

If a report-level drilldown report is set, the pull-down menu and the **Display Reports** menu are displayed on the menu bar of the report window. The number of drilldown reports displayed in the pull-down menu might vary according to the parent report.

To display a report-level drilldown report, select the report from the pull-down menu and click the **Display Reports** menu. Note that the reports registered in bookmarks and combination bookmarks appear as drilldown reports in the pull-down menu.

The following figure shows an example of a report for which a drilldown report is set:

Figure 5-32: Example of a report for which a drilldown report is set



(2) Displaying a field-level drilldown report from the report area

Clicking the field of a table, list, or graph in the report window, displays the field-level drilldown report associated with that field.

This subsection describes how to display a field-level drilldown report from a table, list, and graph.

(a) Displaying a field-level drilldown report from a table

Click a table value to display the field-level drilldown report. The available table values are displayed as linked.

(b) Displaying a field-level drilldown report from the item name of a list

Click an item name in a list to display the field-level drilldown report. The available item names of the list are displayed as linked.

(c) Displaying a field-level drilldown report from a graph area

Click a graph area to display a field-level drilldown report. To display a field-level drilldown report from a graph area, when you define the report you need to define the drilldown report for a field displayed in the graph.

(d) Information inherited from the parent to a drilldown report

When displaying the drilldown report from the report area, information inherited from the parent by a drilldown report might differ according to the combination of report

types. Tables 5-3 and 5-4 describe the information inherited from the parent by a drilldown report.

Table 5-2: Inherited information (parent report consists of multiple agents)

Drilldown report	When multiple agents are specified (historical reports only)	When a single agent is specified
Data collection period	**Date and Time** information of the clicked data row	Historical report: Same as shown on the left Realtime report: Does not inherit information
Agent type	Clicked row of the table, page of list, or agent of the graph area	Agent selected when displaying the parent report
Report interval	• Report definition of the drilldown report • Changed value when changed by specify-when-displayed setting	Historical report: Same as shown on the left Realtime report: Does not inherit information

Note: Information is only inherited by a drilldown report when the parent is a report. Information is not inherited by reports registered in bookmarks and combination bookmarks.

Table 5-3: Inherited information (parent report is a single agent)

Drilldown report	When multiple agents are specified (historical reports only)	When a single agent is specified
Data collection period	**Date and Time** information of the clicked data row	Historical report: Same as shown on the left Realtime report: Does not inherit information
Agent type	Agent selected when displaying the parent report#	
Report interval	• Report definition of the drilldown report • Changed value when changed by specify-when-displayed setting	Historical report: Same as shown on the left Realtime report: Does not inherit information

Note: Information is only inherited by a drilldown report when the parent is a report. Information is not inherited by reports registered in bookmarks and combination bookmarks.

#

When the drilldown report is of a single agent, even if both parent and drilldown reports are multi-instances, the instances are not automatically inherited. If the instance needs to be inherited, set the field value in the drilldown condition settings of the parent report.

(3) Displaying a drilldown report (automatic settings) with the time item specification

When a table is displayed, the **Date and Time** field (**Record Time** field for a realtime report) is added to the first and last columns. If the report target record is a PI record and the data retrieval interval is defined other than in minutes, you can display the drilldown report (automatic settings) by selecting the time in the **Date and Time** or **Record Time** field.

The drilldown report (automatic settings) displayed by the time item specification is the same as the report definition of the parent report. However, the value of the selected **Date and Time** or **Record Time** is set for the **Start time** of the drilldown report, the **Report interval** is one step more detailed than the parent report. For example, if the **Report interval** of the parent report is **Hour**, the **Report interval** of the drilldown report is **Minute**.

Note:

Only historical reports allow you to display the drilldown report from a time item.

(4) Displaying the conditions for a drilldown report

The drilldown report is displayed after filtering with the following display conditions:

1. Filter conditions defined in the parent report for the drilldown report display
2. Filter conditions defined in the drilldown report for the drilldown report display
3. Report display conditions defined as **Specify when displayed** (`SPECIFY_WHEN_DISPLAYED`) in the drilldown report

   The first and second conditions have a different priority. Even if the second filter condition is defined with fixed value in the drilldown report, the first filter condition defined in the parent report has precedence.

5.8 Displaying combination reports

Combination reports are a feature that allows you to combine multiple historical reports in the same graph. Although normal reports allow you to display reports from multiple agents in a single graph, they must refer to the same records in a historical report. By using a combination report, you can display multiple historical reports in the same graph regardless of the agent used or the type of record in the report. You can also compare one report with another by displaying it as reference data (a *baseline*) in the graph.

The following table describes whether or not a combination report can be displayed, for each combination of graph type and graph options.

Table 5-4: Whether a combination report can be displayed

Graph type	Graph options		
	Normal	Show 3D graph	Show gridlines
Column graph	Yes	Yes	Yes
Stacked column graph	Yes	Yes	Yes
Bar graph	No	No	No
Stacked bar graph	No	No	No
Pie graph	No	No	No
Line graph	Yes	No#	Yes
Area graph	Yes	No#	Yes
Stacked area graph	Yes	No#	Yes

Legend:

Yes: Can be displayed.

No: Cannot be displayed.

#

Can be set, but the setting is ignored.

The following figures show examples of displaying a combination report.

Figure 5-33: Example of displaying a combination report (column graph)

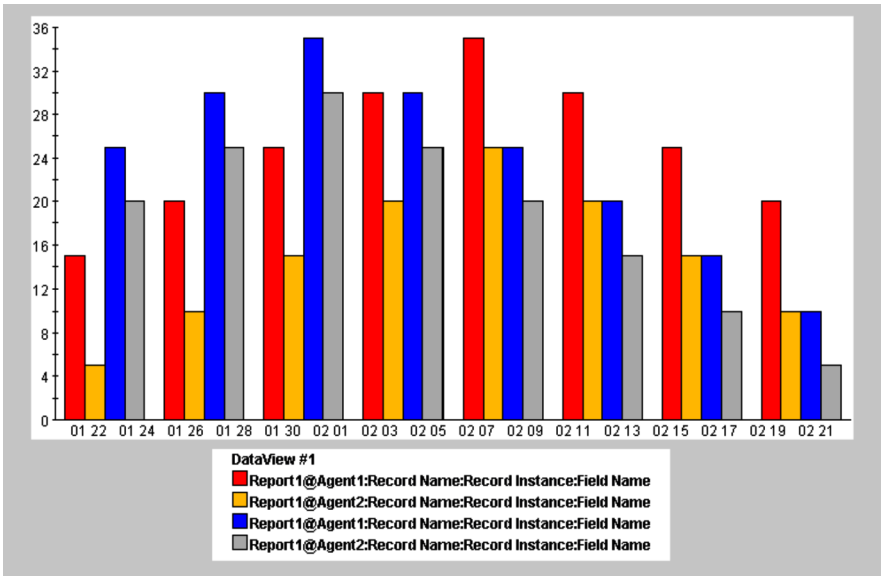


Figure 5-34: Example of displaying a combination report (stacked column graph)

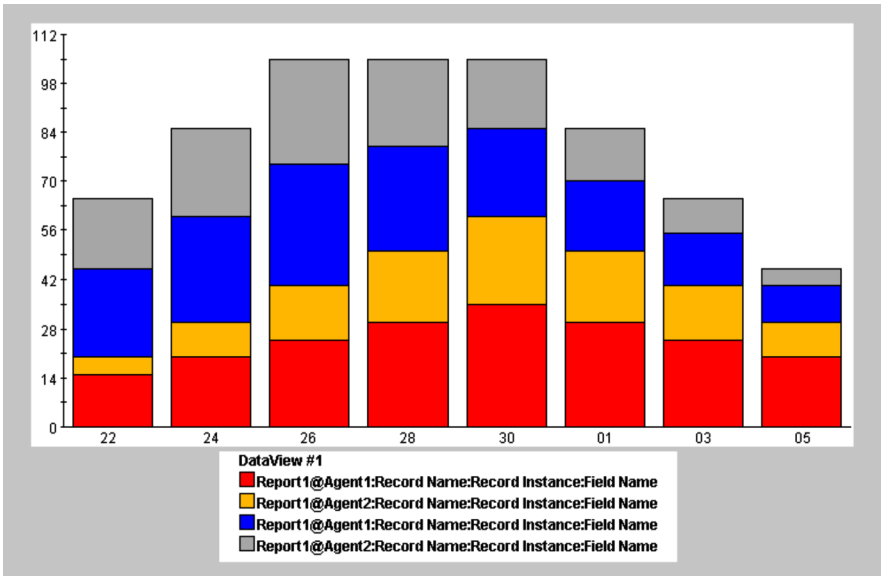


Figure 5-35: Example of displaying a combination report (line graph)

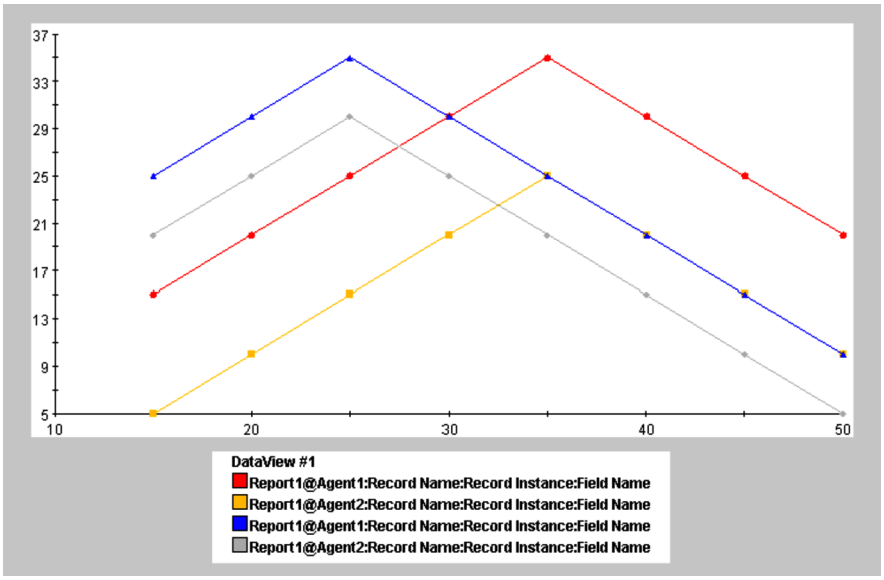


Figure 5-36: Example of displaying a combination report (area graph)

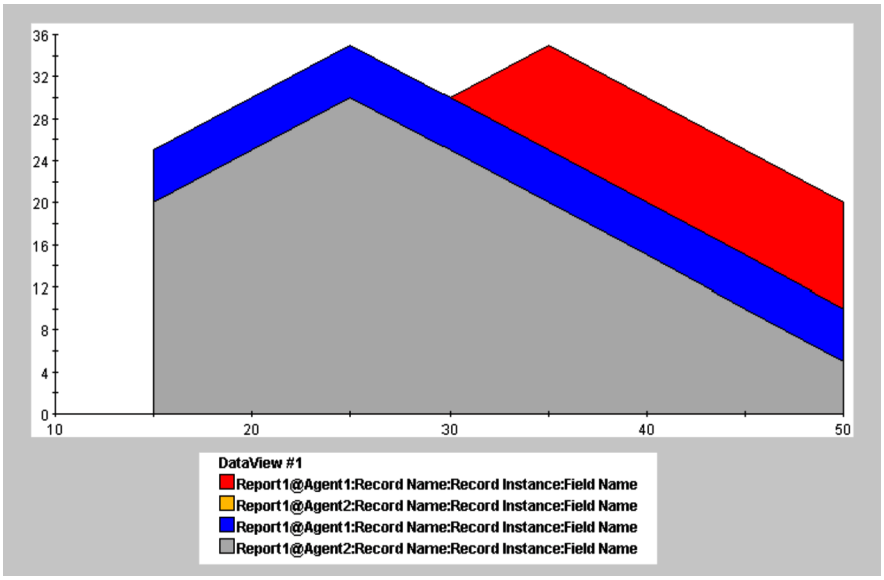
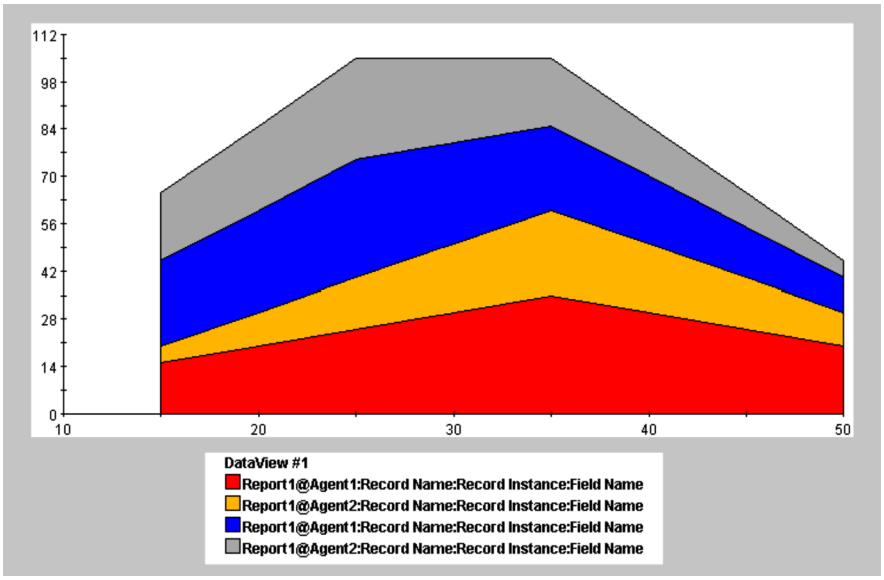


Figure 5-37: Example of displaying a combination report (stacked area graph)



This section describes the following operations regarding combination reports:

- Preparing to display a combination report
- Displaying a combination report
- Checking the properties (combination bookmark definition) of a combination report
- Applying combination reports to real situations

5.8.1 Preparing to display combination reports

The following preparations are required before you can display a combination report:

- Create a report to display in a combination report.
- Register a report in a combination bookmark
- Register a baseline in a combination bookmark
- Setting the display format of a combination report

For details on how to create reports to display in a combination report, see *5.2 Process flow for creating a report*. For details on how to register reports with a combination bookmark, see *5.6.1 Creating bookmarks*. This subsection describes how to register a baseline in a combination bookmark, and how to set the display format of a combination report.

(1) Registering a baseline in a combination bookmark

To register a baseline in a combination bookmark:

1. Display the report window for registering a baseline in a combination bookmark in the window of PFM - Web Console.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. Select the **Baseline** in the report window.

   The Baseline window appears in a new window.

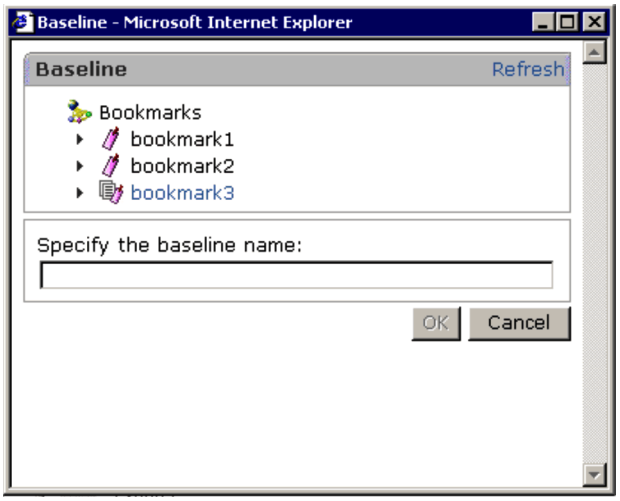
3. Select a combination bookmark from the Bookmarks tree, and enter the name of the baseline in **Specify the baseline name**.

   Specify the baseline name

   Enter the name using no more than 64 characters.

   The following figure shows an example of the Baseline window.

   Figure 5-38: Baseline window



4. Click the **OK** button.

   The baseline is registered in the combination bookmark.

(2) Setting the display format of a combination report

To set the display format of a combination report, edit the display conditions for combination bookmarks:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Bookmarks window appears.

3. Select the combination bookmark you created from the Bookmark tree of the navigation frame.

   The selected combination bookmark is marked with a checkmark.

4. From the method frame, choose the **Edit** method.

   In the information frame, the Edit window appears.

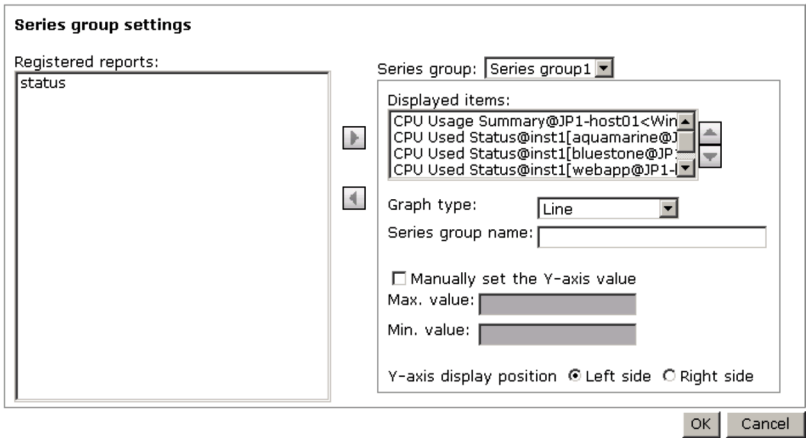
5. Edit the display conditions as required.

   You can group the reports of a combination report in the **Series group settings** area of the Edit window, as a *series group*. You can set and modify the following settings for each series group:

   - Graph type
   - Series group name
   - Maximum and minimum values of the Y-axis
   - Y-axis display position

   The following figure shows an example of the Edit window.

   Figure 5-39: Edit window



6. Click the **OK** button.

   The series group settings take effect as the display settings for the combination report.

5.8.2 Displaying combination reports

You can display the reports registered in a combination bookmark from the Agents tree or the Bookmarks tree. The procedures for displaying combination bookmarks from each tree are described below.

Note:

Some preparation is required before you can display a combination report. The first step is creating the combination bookmark, after which you can perform such tasks as registering a baseline and editing the display conditions and other aspects of the combination bookmark. For details on how to do so, see *5.6.1 Creating bookmarks* and *5.8.1 Preparing to display combination reports*.

(1) Displaying a combination report from the Agents tree

To display a combination report from the Agents tree:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select an agent.

   The selected agent is marked with a checkmark.

Hint:

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the object.

4. In the method frame, select the **Display Reports** method.

   By default, the reports tree appears in the information frame.

5. In the information frame, select **Bookmark** from the **Tree type** drop-down list box.

   The bookmarks tree appears in the information frame.

6. Select a combination bookmark from the bookmarks tree.

   The registered reports associated with the combination bookmark appear as a combination report in a new window.

(2) Displaying a combination report from the Bookmarks tree

To display a combination report from the bookmark tree:

1. From the monitoring console browser, log on to PFM - Web Console.
2. The main window appears.
3. In the navigation frame of the main window, choose the **Bookmarks** tab.

   The Bookmarks window appears.
4. Select the combination bookmark whose reports you want to display from the bookmarks tree in the navigation frame.

   The selected combination bookmark is marked with a checkmark.
5. In the method frame, select the **Display Reports** method.

   The registered reports associated with the combination bookmark selected in step 4 appear as a combination report in a new window.

5.8.3 Checking the properties (definitions) of combination bookmarks

On the **Properties** tab of the combination report window, you can check the definition of a combination bookmark. You cannot check the definitions of the registered reports themselves.

To check the definition of a combination bookmark:

1. In PFM - Web Console, display the reports window for the report whose properties (definition) you want to check.

   For details on how to display the report window, see *5.7.1 Displaying reports*.
2. Select the **Properties** tab in the report window.

   The combination bookmark definition is displayed in the **Properties** tab.

Note

The information displayed on the **Properties** tab is the definition information of the combination bookmark, but not display settings information. Therefore, even if you change the display conditions in the **Show Options** tab, the displayed information of the properties will not be changed.

5.8.4 Examples of using combination reports in real-world situations

This subsection provides examples of using combination reports in real-world situations.

(1) Displaying reports that include different fields from the same record

When displaying a graph that presents different fields from the same record, you need to ensure that there is not a large disparity between the fields in terms of scale or units

of measurement.

Normal reports and combination reports deal with such a disparity in different ways:

- For normal reports

  The highest value among the fields is used as the maximum value of the Y axis. For this reason, displaying reports whose fields contain significantly different values might result in a graph that is difficult to comprehend.

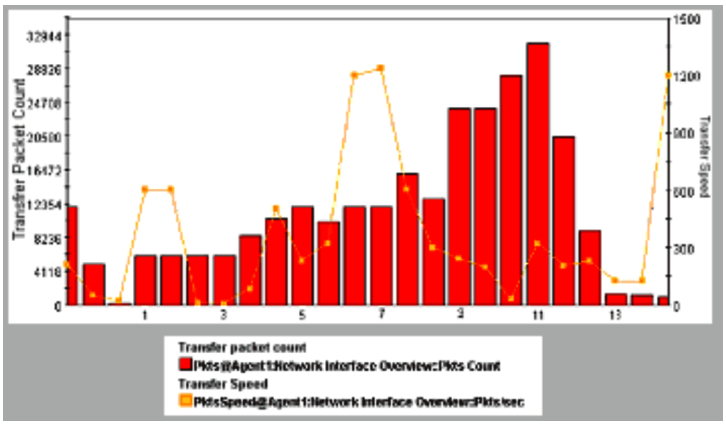
- For combination reports

  By assigning each report to a different series group, you can adjust the following aspects of how each report is displayed:

  - The maximum value of the Y axis
  - Whether the Y axis appears at the left or right of the graph
  - The type of graph

The following figure shows an example of a graph created from a combination report. This graph plots two fields, **Transfer packet count** (maximum value: 33,000 pkt) and **Transfer speed** (maximum value: 1,500 ms), in a single graph.

Figure 5-40: Displaying a report that includes different fields from the same record



To register the combination report:

1. Register multiple reports in a combination bookmark.

   The reports used in this example are assumed to meet the following conditions:

   - The data fields displayed in the graph (can be more than one) have the same scale
   - The data in the graph has the same collection interval

2. Edit the combination bookmark as follows:
   - Assign each report to a different series group
   - For each series group, set a suitable maximum value for the Y axis
   - Between series groups, ensure that the Y axes are displayed at opposite sides of the graph

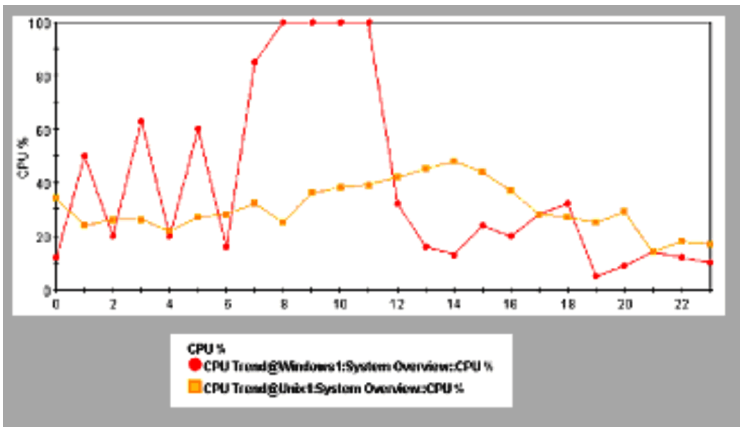
(2) Displaying reports that gather related records from different agent types

You can compare the values of related records from different agent types by displaying them in a single graph. However, you cannot display information from different agents in a graph based on a normal report.

With combination reports, you can display information from records from different agents in the same graph by editing a combination bookmark to place the relevant reports into the same series group. By choosing stacked column or bar as the graph type, you can visually check the total of the data from the different agents.

The following figure shows an example of a graph created from a combination report. This graph displays the value of CPU usage (as a percentage) for the fields Windows1 and UNIX1 in a single graph.

Figure 5-41: Displaying a report that includes related records from different agent types



To register the combination report:

1. Register multiple reports in a combination bookmark.

   The reports used in this example are assumed to contain data fields that are similar in scale and content.

2. Edit the combination bookmark to assign each report to the same series group.

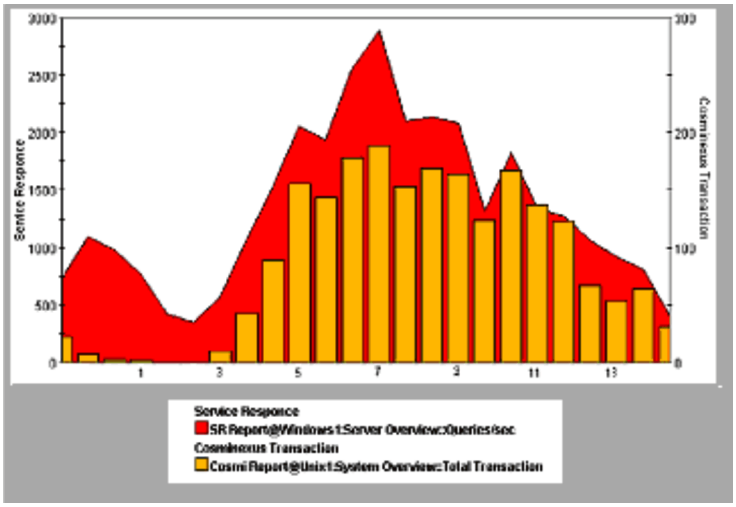
(3) Displaying reports that gather different records from different agent types

With combination reports, you can display different records from different agents in the same graph. This is a useful feature as it allows you to visually check how changes in a given record correlate to changes in another.

The following figure shows the results of creating a graph from a combination report. In this example, the following two fields, which exhibit a correlation, are displayed in the same graph.

- Response time of HTTP service (maximum value: 3,000 ms)
- Number of transactions handled by Cosminexus (maximum value: 200 transactions)

Figure 5-42: Displaying a report that includes different records from different agents



To register the combination report:

1. Register multiple reports in a combination bookmark.

   The reports used in this example are assumed to differ in scale and originate from different agents, but show a correlation.

2. Edit the combination bookmark as follows:

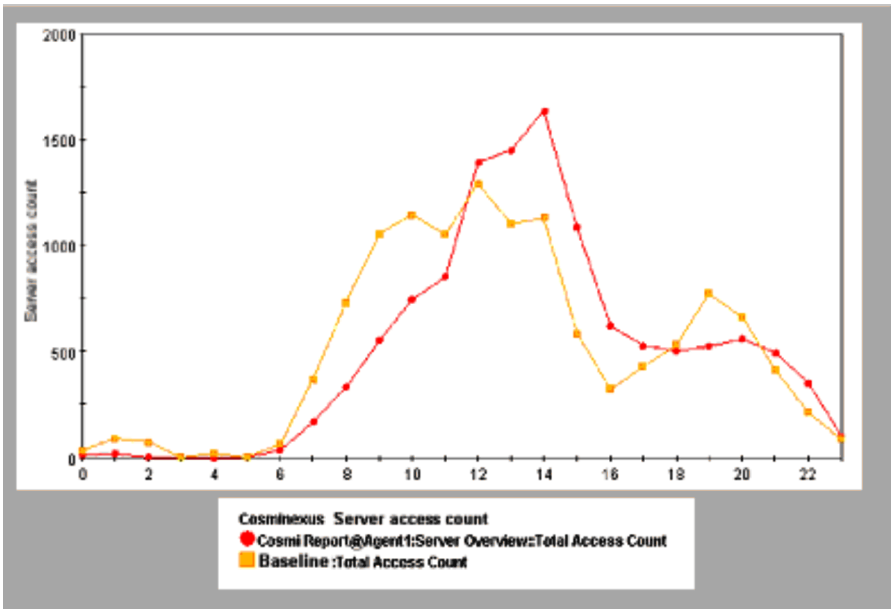
   - Assign each report to a different series group
   - For each series group, set the graph type and Y axis value according to the scale and data of the report it contains.
   - Between series groups, ensure that the Y axis are displayed at opposite sides of the graph

(4) Displaying a report together with a baseline

With combination reports, you can display past periodic data or data obtained during stable operation of the system in the graph as a baseline. By comparing this baseline with a current report, you can ascertain whether the system is operating normally and identify trends in the operation of the system.

The following figure shows the results of creating a graph showing the number of times the server was accessed over a 24-hour period (maximum value: 2000), together with a baseline consisting of the same data from a historical report.

Figure 5-43: Displaying a report together with a baseline



To register the combination report:

1. Register the report to be compared with the baseline as a combination bookmark.

   In this example, this report is configured to collect data periodically.

2. Add a baseline to the combination bookmark.

   In this example, the report registered as the baseline covers the same period or has the same collection interval as the report registered in step 1.

3. Edit the combination bookmark.

   Assign the registered report and the baseline to the same series group.

(5) Combining various types of combination report

By applying the steps described in (1) through (4) above, you can create graphs that allow you to judge the status of the entire system from an integrated perspective. When a more detailed monitoring approach is called for, you can change perspective by drilling down to a separate report that focuses on specific data in the combination report.

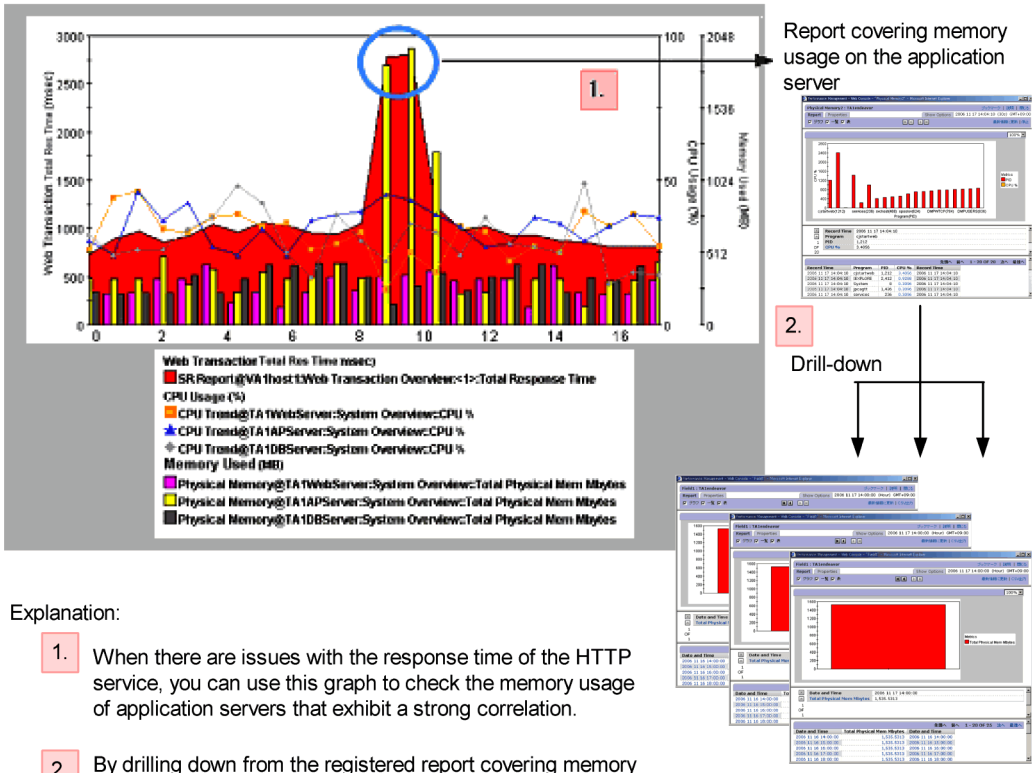
The figure below shows an example of monitoring the operation of a three-tiered Web system comprising a Web server, application server, and database server. In this example, the following aspects of the system are monitored:

- The response time of the HTTP service as collected by PFM - Agent for Service Response, giving an indication of the status of the system in its entirety
- The following two items, which can affect the response time of the HTTP service:
  - CPU usage of each server tier (percentage)
  - Memory usage (MB)

Each set of data is assigned to a series group and displayed as a combination report in a single graph. The ability to set the scale of the vertical axis individually for each series group allows trends in the operating status of the system to be compared.

The following figure shows the resulting graph.

Figure 5-44: Example combining various types of report



Explanation:

1. When there are issues with the response time of the HTTP service, you can use this graph to check the memory usage of application servers that exhibit a strong correlation.

2. By drilling down from the registered report covering memory usage on the application server you are analyzing, you can identify the underlying cause of the bottleneck.

To register the combination report:

1. Create reports featuring the following data:
   - Response time of the HTTP service
   - CPU usage of the Web server
   - Memory used by the Web server
   - CPU usage of the application server
   - Memory usage of the application server
   - CPU usage of the database server
   - Memory usage of the database server

   Associate the appropriate drilldown reports for the Web server, application server, and database server.

2. Register these reports in a combination bookmark.

   Set the display conditions for the series groups as follows:

   - Response time of the HTTP service: Area graph, maximum 3,000 ms
   - CPU usage: Line graph, maximum 100
   - Memory usage: Column graph, maximum 2,048MB

5.9 Outputting reports

You can output reports in CSV or HTML format by using the PFM - Web Console window or a command.

Each procedure is described below.

5.9.1 Exporting reports in CSV or HTML format by using a browser

You can output a report displayed in the window of PFM - Web Console in CSV format.

(1) Outputting reports in CSV format using a browser

You can output a report displayed in the PFM - Web Console window in CSV format.

1. Display the report window for the report you want to output in CSV format.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. If the report you want to output is a realtime report, click the **Stop** menu on the **View Report** tab of the report window.

   This stops the realtime report from refreshing automatically. When you click the **Stop** menu, the **Export** menu appears.

   For historical reports, the **Export** menu appears as soon as you display the report window.

3. Choose the **Export** menu on the **View Report** tab of the report window.

   The File Download window appears.

4. Click the **Save** button.

   Specify the save destination, and save the report.

(2) Outputting reports in HTML format using a browser

You can display the results of a report in a format suitable for printing or saving to disk.

To output a report in HTML format:

1. Display the report window for the report you want to output in HTML format.

   For details on how to display the report window, see *5.7.1 Displaying reports*.

2. If the report you want to output is a realtime report, click the **Stop** menu on the **View Report** tab of the report window.

   This stops the realtime report from refreshing automatically. When you click the **Stop** menu, the **Print** menu appears.

For historical reports, the **Print** menu appears as soon as you display the report window.

3. Choose the **Print** menu on the **View Report** tab of the report window.

   The results of the report appear in a new window in a format suitable for printing or saving to disk.

4. Print or save the report using your browser.

   When saving the report, use the option that saves the complete web page.

Note:

If you intend to print the list area and table area in color, make sure that your browser is set up to print background colors and images.

5.9.2 Exporting reports in CSV or HTML format by using a command

By using the `jpcrpt` command, you can implement batch processing that outputs a report to a file regularly at a predetermined time, or outputs multiple reports to a file in one operation. The `jpcrpt` command outputs reports in CSV or HTML format. The report types that the `jpcrpt` command can output depend on the version of PFM - Web Console. The following table describes which report types can be output by which versions of PFM - Web Console.

Table 5-5: Report output capabilities by version

Type of output		08-00	08-11 or later
Report	CSV output	Yes	Yes
	HTML output	No	Yes
Registered report	CSV output	No	Yes
	HTML output	No	Yes
Combination report	HTML output	No	Yes

Legend:

Yes: Can be output

No: Cannot be output

For details on the `jpcrpt` command, see the manual *Job Management Partner 1/ Performance Management Reference*.

5.9.3 CSV format

(a) CSV data output format

CSV data is output in the order of data header 1st, data header 2nd, and data sections. This subsection describes the display format for each section.

- Data header 1st section

  One blank row + report name + one blank row are displayed.

- Data header 2nd section

  A field header is output.

  A field schema name is output as a field column header. However, if **Display name** is set for a field in definition, the **Display name** is displayed.

- Data section

  This is output as one row per record.

(b) Character set of text used for exporting

Set as `characterCode` in `config.xml`#. Available character sets are US-ASCII, windows-1252, ISO-8859-1, UTF-8, UTF-16, UTF-16BE, and UTF-16LE.

The default setting is US-ASCII.

(c) Linefeed code

Set as `lineSeparator` in `config.xml`#. The default setting is `CRLF` in Windows, `LF` in UNIX.

If the linefeed code is `CRLF`, `0D0A` is output. If it is `LF`, `0A` is output.

Note:

If the setting is other than `CRLF` or `LF`, an error is output to the log file during initialization, and `CRLF` is used as the setting value.

(d) File end code

After the last data is output, `<EOF>` is output.

(e) Delimiter between items

The delimiter between items is represented by a comma (`,`). If either a comma, double quotation mark (`"`), or linefeed is in the data value, the data value itself is surrounded with double quotation marks.

5.9.4 HTML format

(1) Format when output by a command

A report in HTML format is composed of three parts: a report header area, a graph area, and a table area. The following table lists the content displayed in each part, and the conditions under which the part is displayed, for each type of report or bookmark.

Table 5-6: Content and display conditions for each part (when output by a command)

Part	Subject of output operation		
	Report	**Registered report**	**Combination bookmark**
Report header area	Displays the report name, agent name#1, date format, and command line, in a colon-separated format.	Displays the report name, agent name#1, date format, and command line, in a colon-separated format.	Displays the bookmark name, date format, and command line, in a colon-separated format.
Graph area	The same image of the graph is displayed as appears in the report window. This part is displayed when graph display is enabled in the report definition and the `show-graph` tag is specified in the input file.	The same image of the graph is displayed as appears in the report window. This part is displayed when graph display is enabled in the report definition for the registered report and the `show-graph` tag is specified in the input file.	The same image of the graph is displayed as appears in the report window for the combination report.
Table area	All data is displayed on one page in table format.#2 This part is displayed when table display is enabled in the report definition and the `show-table` tag is specified in the input file.	All data is displayed on one page in table format.#2 This part is displayed when table display is enabled in the report definition for the registered report and the `show-table` tag is specified in the input file.	Not displayed (combination reports do not include output in table format)

#1

When more than one agent name is specified, the names are separated by commas.

#2

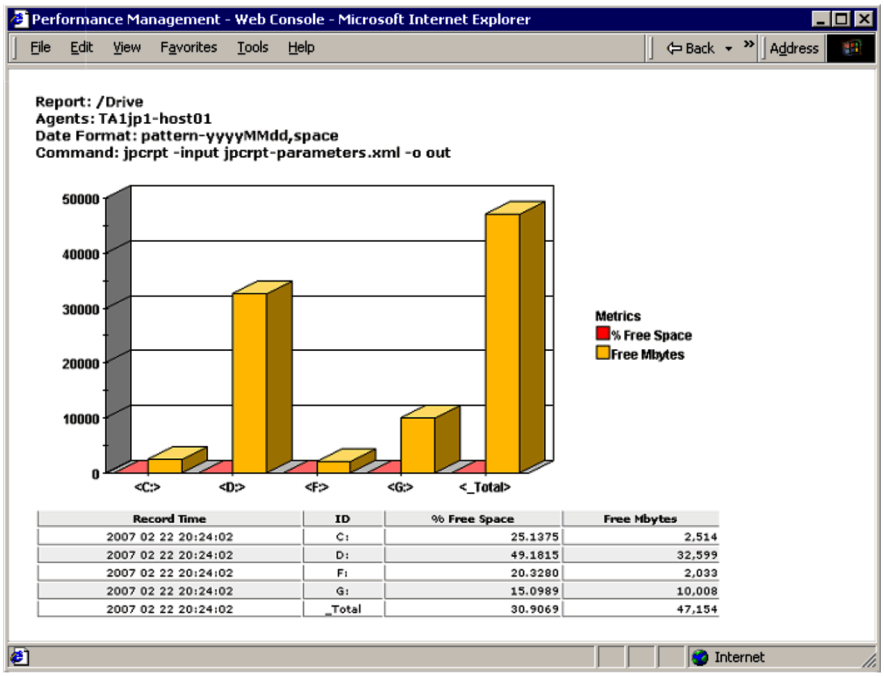
The columns appear in the table in the order in which they are defined in the report definition, with the exception of the Date and Time field. When the Date and Time field is not defined, it is added at the left of the table. When defined, the Date and Time field appears at the position defined in the report definition.

If there are no items in the data set or the agent(s) are stopped, only the report header area is output.

The HTML is output in UTF-8 encoding, ignoring the character set and linefeed code settings in the section of the `config.xml` file that describes the export format.

The following figure shows an example of outputting a report in HTML format using a command.

Figure 5-45: Example of outputting a report in HTML format using a command



(2) Format when output from the GUI

A report in HTML format is composed of four parts: a report header area, a graph area, a list area, and a table area.

The following table lists the content displayed in each part, and the conditions under which the part is displayed, for each type of report or bookmark.

Table 5-7: Content and display conditions for each part (when output from the GUI)

Part	Subject of output operation		
	Report (bookmark)	**Combination report**	**Event history report**
Report header area	Displays the name of the report definition, the folder where the report definition is stored[#1], the name of the agent[#2], and the data acquisition time[#4].	Displays the name of the combination bookmark, the path of the bookmark in the bookmarks tree[#3], and the data acquisition time[#4].	Displays the string **Event History**, and the data acquisition time[#4].
Graph area	The same image of the graph is displayed as appears in the report window.	The same image of the graph is displayed as appears in the report window for the combination report.	Not displayed
List area	Displays the list data and instance numbers that appear in the report window.	Not displayed (combination reports do not include output in list format)	Not displayed
Table area	All data is displayed on one page in table format.	Not displayed (combination reports do not include output in table format)	All data is displayed on one page in table format.

#1

The folder where the report definition is stored appears in the format **ParentFolder** *folder-path-name*, and is displayed as an absolute path.

#2

Agent names appear in the format **Agents** *agent-name*. When more than one agent name is specified, the names are separated by commas. No agent name is displayed for combination reports.

#3

The path of the bookmark in the bookmarks tree is shown as an absolute path.

#4

The data acquisition time appears in the format **Time** (*time*). This is the same information that appears in the menu bar frame of the report window.

The HTML is output in UTF-8 encoding, ignoring the character set and linefeed code

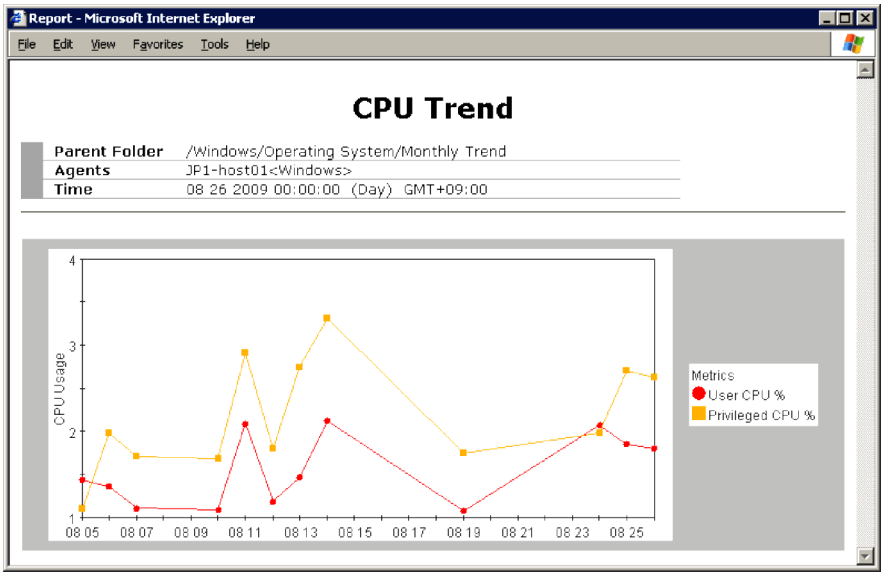
settings in the section of the `config.xml` file that describes the export format.

Reference note:

Each time you choose the **Print** menu, a new window opens. Any print windows that have already been opened continue to display the same data. The print windows close when you close the parent window.

The following figure shows an example of outputting a report in HTML format using the GUI.

Figure 5-46: Example of outputting a report in HTML format from the GUI



5.10 Notes on reports

This section gives cautionary notes on reports.

5.10.1 Notes on creating reports

The following gives cautionary notes on creating reports:

- About the setting for the refresh interval

  If you want to display multiple realtime reports simultaneously, set the refresh interval so that the automatic refreshes of respective windows are not performed at the same time.

- Separation between realtime and historical reports

  If you want to view trends in long-time performance data, use a historical report instead of displaying a realtime report for a long time.

- Reports with a lot of displayed data

  For reports with a lot of displayed data (for example, a report of Process Detail Interval (PD_PDI) records of PFM - Agent for Platform), use data filters or a ranking display so that only the necessary data is displayed.

5.10.2 Notes on displaying reports

The following gives cautionary notes on displaying reports:

- About stacked area graph

  If multiple series of records are stacked in a stacked area graph, only the records that have exactly the same time will be stacked.

  Therefore, if you want to display stacked records from more than one agent in a historical (multiple agents) report, set the collection interval and offset value so that they match all of the agents.

  If this condition is satisfied, a collection time difference might occur due to a delay caused by collection load and the stacked area graph might not display as expected. To avoid this, you can use an optional PFM - Web Console function to adjust the record collection time for the graph display.

  For details, see the description of the `<graph-time-correction>` tag of the Windows initialization file (`config.xml`) in an appendix of the manual *Job Management Partner 1/Performance Management Reference*.

- Maximum number of report windows displayed in the PFM - Web Console browser

  - The maximum number of report windows displayed in the PFM - Web

Console browser is about four.

- For report windows that display the PFM - Agent or PFM - RM information (report window displaying realtime reports), the maximum number of windows is roughly 10 for one Performance Management system. If 11 or more windows are displayed, you might fail to retrieve data.

- Maximum number of data items displayed in a report

  In realtime reports, data from 30 collection times can be displayed. When displaying data over 31 collection times, the data will be deleted in the order from oldest to newest data. If you want to change this maximum number, change the `maxRealtimeCache` in `config.xml`.

  For historical reports, the maximum amount of displayed data of a data group is up to the maximum number of records or the maximum number set in the Windows initialization file (`config.xml`). If you want to change this maximum number, change the `maxFetchCount` (under the `<vsa>` tag).

  Note that you cannot use the GUI to change a report that has too many records to display. Use the CSV output function of the `jpcrpt` command for such a report.

- About data acquisition performance

  If multiple realtime reports are displayed at the same time, data acquisition performance might be degraded.

- Limitation of realtime report display

  If multi-instance records are collected in PFM - Agent or PFM - RM, the maximum number of instances handled by a collection is 32,767. Therefore, when displaying the realtime report of multi-instance records in the browser, you can display no more than 32,767 instances. You cannot display 32,768 or more instances.

- Displaying a report with a large number of records

  If you use the GUI to display a report with a large number of records, the report might not be displayed due to insufficient memory. To avoid this, use the CSV output function of the `jpcrpt` command for such a report. For details on the `jpcrpt` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

- Too many graph legends to display

  Although there are no restrictions on the number of fields in a report, the system might be unable to display the graph or legend in part or in its entirety if the report contains too many fields. We recommended that you limit the number of displayed fields to approximately 20.

  If there are too many items in a graph legend, and some cannot be displayed,

change the magnification of the graph to check whether all the legend information can be displayed. If some still cannot be displayed, add a field to the report table for each item in the legend that is not displayed.

5.10.3 Notes on combination reports

This subsection gives cautionary notes on combination reports.

(1) Notes on graph types and graph options

The **Show 3D graph** option can be set for any graph, but is ignored for graph types other than column or stacked column. To show a graph in 3D, the following conditions must be met:

- The graph is based on one or two series groups, each group having an opposite **Y-axis display position** setting.
- The graph types of the series groups to be displayed present one of the following combinations:
  - One series with the graph type column/stacked column
  - Two series with the graph types column/stacked column and line
  - Two series with the graph types column/stacked column and area/stacked area

The graph might not be drawn correctly in 3D if these conditions are not satisfied.

- The **Show gridlines** option can be set for any graph, but applies only to the first series group. This setting is ignored for all other series groups.

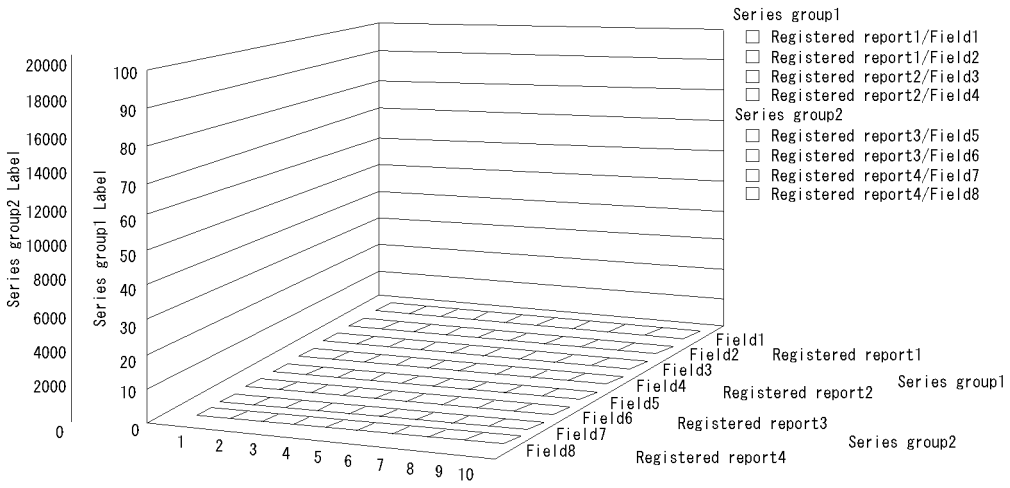
(2) Notes on the order in which graphs are drawn

The graphs in a combination report are drawn in the following order:

1. Series groups are drawn in order from the first series group, with subsequent series groups being drawn over the earlier ones.
2. Registered reports in a series group are displayed in the order in which the report is registered in the series group, with subsequent registered reports being drawn over the top of the earlier ones.
3. Fields in a registered report are displayed in the order in which they appear in the report, with subsequent fields being drawn over the top of the earlier ones.

The following figure describes the order in which graphs are drawn.

Figure 5-47: Image showing the order in which graphs are drawn



The specific order for 1. and 2. above is determined by the series group settings you specify when defining the combination bookmark. Make sure that the settings you specify do not cause graphs to become hidden behind other graphs. The order of the fields described in 3. is determined by the settings in the report definition window.

The following exceptions apply to series groups that feature certain graph types:

- The graph for a series group with the graph type *Line* is drawn at the very front of the graph.
- The graph for a series group with the graph type *Column* or *Stacked column* and the **Show 3D graph** option specified is drawn at the very front of the graph.

(3) Notes on the horizontal axis (X-axis) and vertical axis (Y-axis) of the graph

- You cannot use common settings that apply across the entire combination report.

  For the Y-axis of each series group in a combination report, you can use either automatic scale adjustment (where the axis is adjusted to the maximum and minimum values of the actual data) or manual scale adjustment (where the maximum and minimum values are specified by the user). You can also choose whether to display the axis label on the left or right side of the graph.

- The X-axis for a combination report is a single fixed time series.

  Data collected over a date range or with an interval that does not match the X-axis is assumed to be missing some information and the system attempts to compensate it. This might compromise the integrity of the graph. If a misalignment in the collection interval occurs when PD records are collected, a stacked graph might not be displayed normally. We recommend that you use a line

graph when the data includes PD records.

To avoid this, you can use an optional PFM - Web Console function to adjust the record collection time for the graph display. For details, see the description of the `<graph-time-correction>` tag of the Windows configuration file (`config.xml`) in an appendix of the manual *Job Management Partner 1/ Performance Management Reference*.

(4) Notes on the number of fields in a report

- Although there are no restrictions on the number of fields in a combination report, the system might be unable to display the graph or legend in part or in its entirety when the report contains too many fields. In this case, either increase the magnification of the graph, or use the following methods to restrict the number of fields displayed in the graph (we recommend that graphs display no more than approximately 20 fields).
  - Edit the combination bookmark to remove some of the reports from the graph.
  - Edit the report definitions to contain fewer fields, and then recreate the registered reports.
  - Edit the report definitions to apply filter conditions, and then recreate the registered reports.
  - Recreate the registered reports using shorter display names for the fields than the default field names.

  In environments where the number of lines in the legend exceeds the allowances given below, the graph or legend might be missing or cut off, or the graph might appear alongside the legend.
  - 100% magnification: Legend approx. 20 lines
  - 200% magnification: Legend approx. 30 lines
  - 400% magnification: Legend approx. 40 lines
  - 600% magnification: Legend approx. 50 lines
  - 800% magnification: Legend approx. 60 lines
- When the legend for a combination report contains too many characters, part of the legend might be cut off. In this case, either increase the magnification of the graph, or use the following methods to restrict the number of characters displayed in the legend.
  - Shorten the report names and then recreate the registered reports.
  - Recreate the registered reports using shorter display names for the fields than the default field names.

- Reduce the number of bound agents and then recreate the registered reports.

In environments where the number of characters in the legend exceeds the allowances given below, the legend might be cut off:

- 100% magnification: Approx. 80 characters
- 200% magnification: Approx. 120 characters
- 400% magnification: Approx. 160 characters
- 600% magnification: Approx. 200 characters
- 800% magnification: Approx. 240 characters

(5) Notes on series group settings

At least one registered report must be assigned to a series group. No graph is displayed if none of the series groups contain any registered reports, or when the combination bookmark contains only a baseline.

(6) Notes on the date range of records

When you set the date range of a report to a **Within the past** ... option (for example **Within the past hour**), the report is updated with the data from that time period up to the present time when you choose **Refresh** in the report window. The start time of the baseline remains unchanged.

If you choose **Specify when displayed** as the date range, the **Start time** and **End time** set for the report and the start time of the baseline remain unchanged when you choose **Refresh** in the report window.

(7) Baseline display periods

- The **Start time** setting for the baseline display period is determined automatically based on the current time when the combination report was started and the **Date range** and **Report interval** settings for the report display period. When you change these settings, the **Start time** setting for the baseline display period is set to the **Start time** setting for the report display period.
- When you choose **Refresh** in the report window, the **Start time** and **End time** of the settings for the report display period might change according to the **Date range** setting. However, the **Start time** setting for the baseline display period will remain unchanged.
- Changes to the **Start time** setting for the baseline display period or the baseline data do not affect the starting points and ending points of graphs created from combination reports. However, when the report displayed with the baseline contains only one piece of data (data with the same starting point and ending point), the graph's starting point and ending point might be set to the range of the data collected as the baseline. The starting point and ending point of the actual display period for the graph is determined based on the data present in the range

from the **Start time** to the **End time** in the report display period settings.

- The **Start time** setting for the baseline display period applies to the individual baseline. When a baseline contains data from multiple fields each with different start times, the field data with the earliest start time in the time series after the **Start time** setting for the baseline display period serves as the starting point. All other fields are displayed according to the start times determined when the baseline data was saved.
- When data from multiple fields with different start times is registered as a baseline, the graph is drawn with the field data earliest in the time series after the **Start time** setting for the baseline display period serving as the starting point. In this case, the relative start positions of each subsequent field are preserved.

Chapter

6. Monitoring Operations with Alarms

In Performance Management, an *alarm* is used to notify the user when collected performance data has exceeded a user-defined threshold.

This chapter explains how to create alarms and use them to notify the user of problems.

6.1 Overview of alarms
6.2 Process of setting up and operating alarms
6.3 Procedures before setting alarms
6.4 Setting alarms by using the browser
6.5 Setting alarms by using the Quick Guide
6.6 Operating alarms by using the browser
6.7 Setting alarms by using commands
6.8 Operating alarms by using commands
6.9 Notes on alarms

6.1 Overview of alarms

Performance Management can be set up to notify the user of when performance data monitored by a monitoring agent exceeds a user-defined threshold.

A definition of how the system should behave when data reaches a threshold value is called an *alarm*. A set of alarms is called an *alarm table*. Each PFM - Agent type or PFM -RM type has a *folder* in which it stores alarm tables.

The folder is displayed on the second level of the Alarms tree. You can display the Alarms tree by selecting the **Alarms** tab from the navigation frame of the PFM - Web Console Main window.

When the data reaches a threshold value, the monitoring agent reports the information by issuing an *alarm event*. Performance Management receives the alarm event, and then performs one or more tasks, which are called *actions*. Performance Management can perform the following actions:

- Notify the system administrator via email
- Execute one or more commands, such as a restore program
- Issue a JP1 event in order to link with other JP1 products
- Send an SNMP trap

By linking an alarm table to a monitoring agent, you can detect when any thresholds are exceeded. The act of linking an alarm table to a monitoring agent is called *binding*.

In addition, each monitoring agent can have multiple alarm tables bound to it.

6.2 Process of setting up and operating alarms

The section explains how to set up and operate alarms, and provides a flow chart for the process of creating and operating alarms.

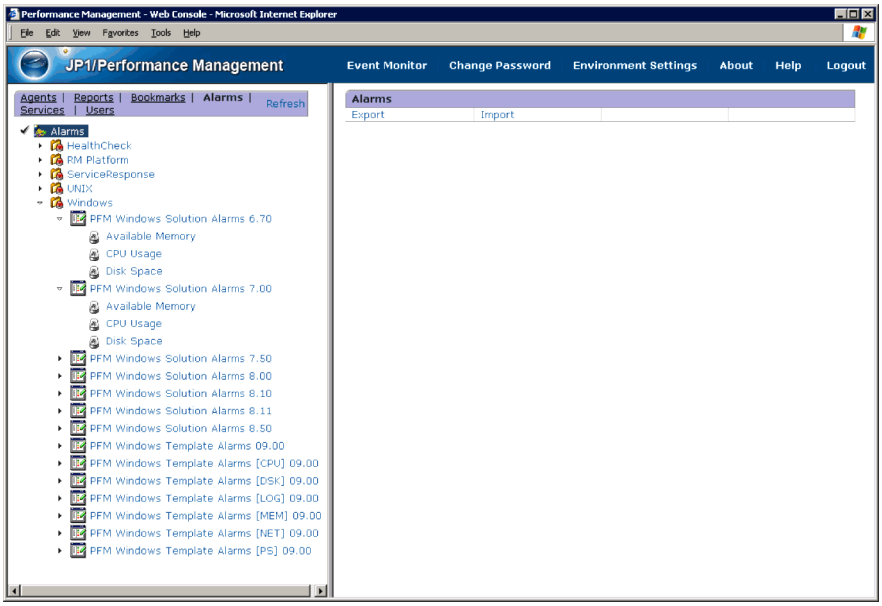
In addition, you can use the Quick Guide to set simplified alarms. For details on the Quick Guide, see *6.5 Setting alarms by using the Quick Guide*.

(1) How to set up and operate alarms

Alarms are set up and operated by using the Alarms window in PFM - Web Console or by using a command.

The following figure is an example of the Alarms window in PFM - Web Console.

Figure 6-1: Example of the Alarms window



You can set up alarms in the following ways:

- Define a new alarm table or individual alarms.

  Create a new alarm table for your system environment, and then define the alarms. You can add new alarms to that alarm table at a later time.

  In addition, you can use the Quick Guide to set simplified alarms. Alarms set using the Quick Guide can be bound to an agent.

- Use an existing alarm table or alarms.

You can use the following methods:

- Use the monitoring template.

  The monitoring template is a set of alarms, which necessary information has been preset, included with each PFM - Agent or PFM - RM. When you use the monitoring template, any active alarms in the monitoring template are enabled when PFM- Agent or PFM - RM is started.

- Customize the monitoring template.

  You can copy the monitoring template and customize it to match your monitoring objectives.

- Use an existing alarm table or alarms.

  You can make a copy of, and then customize one of the already user-defined alarm tables or alarms.

To use alarms, associate (or bind) the alarm table defined above with a monitoring agent.

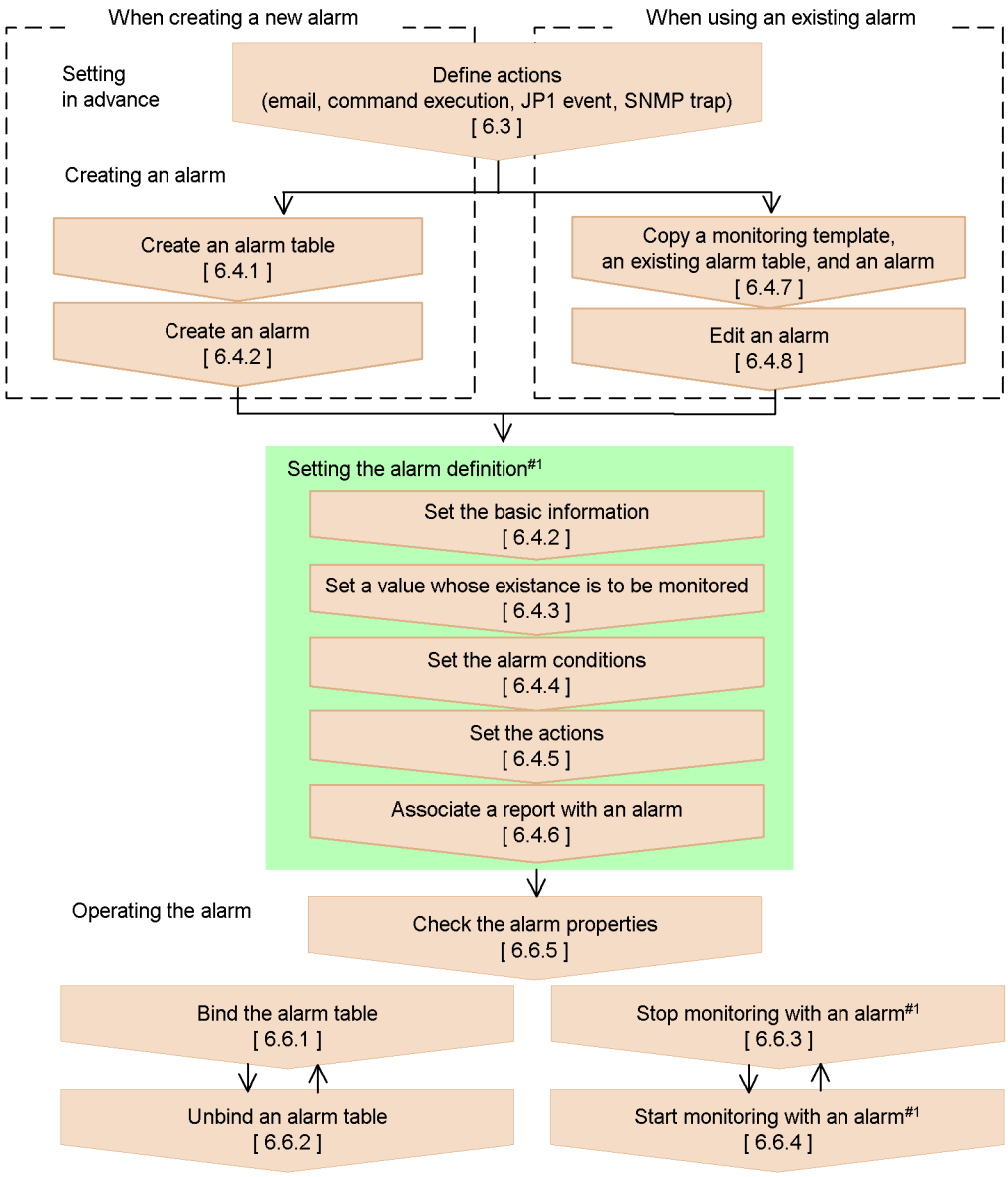
Reference note:

> By using the `jpctool alarm` command to create an alarm definition file, you can create up to 50 alarms at once. This is a useful technique when setting up multiple alarms at the same time to run on multiple servers in a large-scale system.

(2) Flow chart for setting up and operating alarms

The figure below is a flow chart for setting up and operating alarms. When you use the Quick Guide to set and operate alarms, perform the procedures in *6.3 Procedures before setting alarms* and *6.5 Setting alarms by using the Quick Guide*.

Figure 6-2: Flow chart for setting up and operating alarms



Legend: [ ] : See the indicated step.

#1 Perform as needed.

#2 Edit as needed when using an existing alarm.

6.3 Procedures before setting alarms

This section describes the setting procedures to follow before setting alarms.

(1) Configuring the email sender

If you want an email to be sent out when an alarm event occurs in PFM - Agent or PFM - RM, you need to configure the email sender.

To configure the email sender:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

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

   The Services window appears.

3. In the navigation frame, click the **Machines** folder.

   This folder contains folders for the hosts where a Performance Management program is installed.

4. Select the Action Handler service on the host that will send the email.

   The name of the icon indicating the Action Handler service begins with **PH** or is the same as *host-name*`<Action Handler>`.

5. In the method frame, select **Properties**.

   The Properties window appears.

   Set the properties to the following:

   Email in **Capabilities**: `Yes`

   SMTP Host in **Mail**: the host name or IP address of the SMTP server that will send out emails

   SMTP Sender in **Mail**: the email address of the sender

   Mail Subject in **Mail**: the subject of the emails

6. Click the **OK** button.

   The values set in step 5 are saved. For details on the settings for each alarm, see *6.4.5(a) Sending emails*.

(2) Configuring the host to automatically execute commands

If you want commands to be automatically executed when an alarm event occurs in

PFM - Agent or PFM - RM, in the Properties window of the Services tree window in PFM - Web Console, you must set the appropriate Action Handler property on the host where the commands will be executed as follows:

- **Script** in **Capabilities**: `Yes`

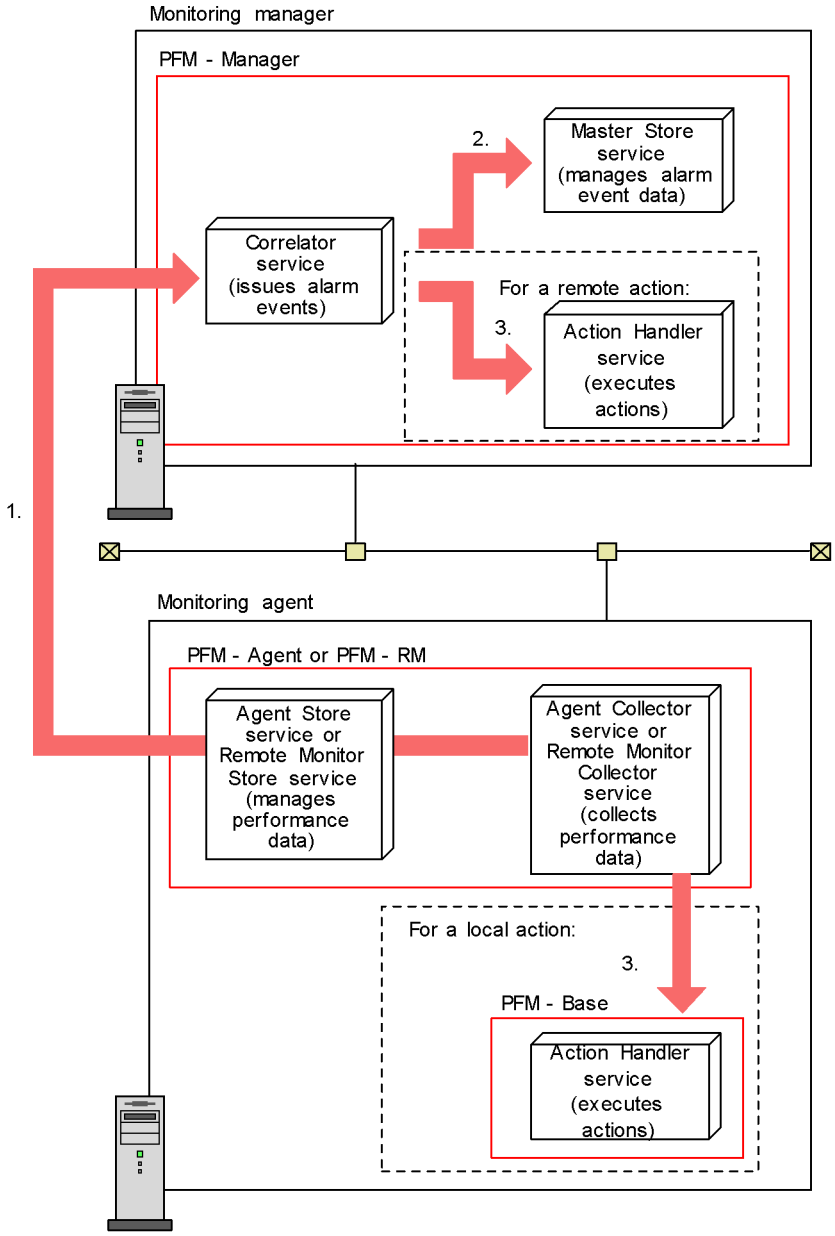
  The action handler you select in the **Action handler** of the **Command** field in the New Alarm > Action Definitions window is used when executing the commands. By default, the Action Handler that is used is the one that resides on the same host as the agent bound to this alarm event (indicated as **LOCAL** in the **Command** tab).

  For details on the settings for each alarm, see *6.4.5(b) Executing commands*.

  The actions in which a command is executed by the Action Handler on the same host as a monitoring agent bound to alarm tables are called *local actions*. The actions in which a command is executed by the Action Handler on the different host from a monitoring agent bound to alarm tables are called *remote actions*.

  The following figure shows an overview of local actions and remote actions.

Figure 6-3: Overview of local actions and remote actions



The following procedure describes the processing flow by using the numbers

displayed in the above figure:

1. If the Agent Collector or Remote Monitor Collector service detects an alarm status change, an alarm event is issued to the Correlator service via the Agent Store or Remote Monitor Store service.
2. The alarm event information is stored in the Master Store service.
3. The Action Handler service receives an alarm event.

   When an alarm event is received, the Action Handler service executes the specified command.

   When a local action is required, the Action Handler service executes the command on the same host as the monitoring agent.

   When a remote action is required, an Action Handler service (a monitoring manager or a monitoring agent) on a different host from that of the monitoring agent executes the command.

(3) Configuration for issuing JP1 events

If you want to issue JP1 events when the alarm event occurs in PFM - Agent or PFM - RM, in the Properties window of the Services tree window in PFM - Web Console, you must set the appropriate Action Handler property on the host where the JP1 event-issuing command will be executed as follows:

- **Script** in **Capabilities**: `Yes`

  The action handler you select in the **Action handler** of the **Command** field in the New Alarm > Action Definitions window is used when executing the commands. By default, the Action Handler that is used is the one that resides on the same host as the agent bound to this alarm event (indicated as **LOCAL** in the **Command** tab).

To issue JP1 events, you must configure the Action Handler to link with JP1/IM. For details on how to do this, see *10.3.2 Setup*.

(4) Configuration for sending SNMP traps

If you want SNMP traps to be sent when an alarm event occurs in PFM - Agent or PFM - RM, in the Properties window of the Services tree window in PFM - Web Console, you must set the appropriate Trap Generator property to issue the SNMP trap as follows:

- **ADD A DESTINATION** in **ADD OR DELETE A TRAP DESTINATION**: The host name or IP address of where the SNMP will be sent

  Note that if you want to delete the location where the SNMP is sent to, select the host name or IP address in **DELETE A DESTINATION**, from the Trap Generator properties.

For details on the settings for each alarm, see *6.4.5(d) Sending an SNMP trap when an alarm occurs*.

6.4 Setting alarms by using the browser

6.4.1 Creating an alarm table

To create a new alarm table:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

2. In the navigation frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the folder of the monitoring agent to create an alarm table.

   The selected folder is marked with a checkmark.

   Alarm tables cannot be created under the **Alarms** folder that is on the first level of the Alarms tree. Alarm tables are created under the **Agent** folder that is on the second level of the Agent tree.

4. In the method frame, select the **New Alarm Table**.

   In the information frame, the New Alarm Table > Main Information window appears.

5. In the **General Settings** area, select a product (data model), and enter the alarm table name.

   In this step, you can create a new alarm in the newly created alarm table by setting the basic information such as the alarm name. For details on how to create alarms, see *6.4.2 Creating an alarm (setting the basic information)*.

   Alarm table name

   You can use up to 64 bytes of alphanumeric characters, spaces, and the following symbols: % - ( ) _ . / @ []

   For example, in PFM - Agent for Platform (Windows) for the inventory management system, when you want to create an alarm table with the data model version 6.0, you can specify the following settings:

   Product: `Windows(6.0)`

   Alarm table name: `Inventory Control System(Win)`

Note: Version of the data model to select in **Product**

Select the appropriate data model version corresponding to the agent to which you want to bind the alarm table. If two or more agents of the same type exist and each uses a different data model version, we recommend that you select the earliest data model version.

To check the data model version of an agent:

1. From the **Agents** tree in the navigation frame, click the agent whose report you want to display.
2. In the method frame, click **Properties**. The Service Properties window appears.
3. In the Service Properties window, click the agent. The data model version appears at the bottom of the information frame.

6.4.2 Creating an alarm (setting the basic information)

To create a new alarm in the alarm table:

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

   The main window appears.

   You must log on as a user with administrator user permissions.
2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.
3. In the navigation frame, select the folder of the PFM - Agent product to create an alarm table.

   The selected folder is marked with a checkmark.
4. In the navigation frame, select the folder of the PFM - Agent or PFM - RM product for which you want to create an alarm table.

   The selected alarm table is marked with a checkmark.
5. In the method frame, select **New Alarm**.

   In the information frame, the New Alarm > Main Information window appears.
6. In the **General Settings** area of the Alarm > Main Information window, set the basic information for the alarm.

   Alarm name

   You can use up to 20 bytes of alphanumeric characters, spaces, and the following symbols: % - ( ) _ . / @ [].

   Alarm Message

   You can enter up to 255 bytes of characters. This item can be omitted.

Product displays the product (data model) that you have selected in the navigation frame. **Alarm table name** displays the name of the alarm table that you have selected in the navigation frame.

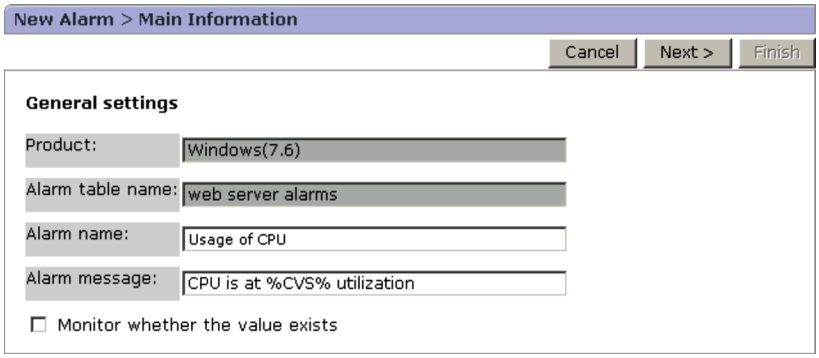
For example, when you want to define an alarm to monitor the busy state of the processor, you can specify the following settings:

Alarm name: `Usage of CPU`

Alarm message: `CPU is at %CVS% utilization`

The following figure shows an example of these settings.

Figure 6-4: New Alarm > Main Information window



Reference note:

You can use variables such as *%SCT* and *%HNS* for the **Alarm message** setting. For further details on the variables, see the chapter that describes the window in the manual *Job Management Partner 1/Performance Management Reference*.

Note 1

If you have selected **Monitor whether the value exists**, the value specified in the conditional expression does not exist when the alarm is reported. In that case, a variable `%CVS` specified in the Message or the Mail Subject is replaced with an empty string.

Note 2

If the message text contains a multi-byte character that follows `%CVS`, the text might be corrupted after variable expansion. Make sure that there are no multi-byte characters following the `%CVS` variable.

7. In the **Advanced settings** area of the New Alarm > Main Information window, set a monitoring time and damping for the alarm.

For example, if the alarm table is defined to monitor the busy state of the processor, and you want to monitor the target 24 hours a day and be notified when the threshold has been exceeded two times over three monitoring intervals, you can specify the following settings:

Enable alarm: selected

Always monitor: selected

Report alarm when the following damping condition is reached . : Selected

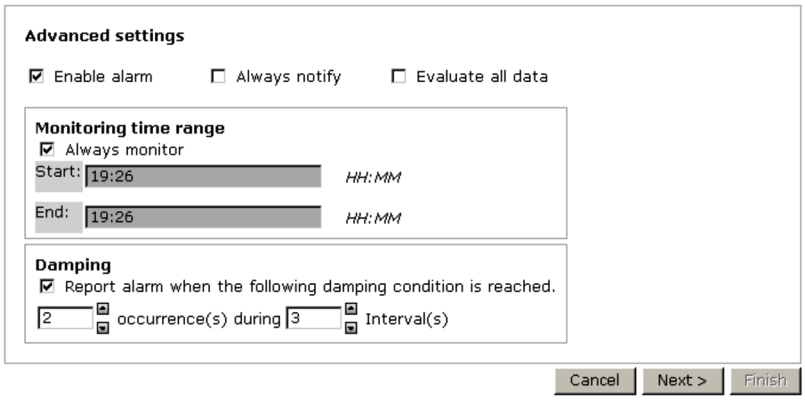
`2` **occurrence(s) during** `3` **Interval(s)**

Note:

The damping setting is still valid when you set the monitoring time range. For example, if you set the alarm to be issued when the threshold is exceeded two times over three intervals within the monitoring time range of 09:00 to 21:00. However, the alarm changes to the normal status when the threshold is exceeded two times outside the monitoring time range in that day.

However, because the alarm status continues even when the date is changed, if the threshold is exceeded only once at or after 9:00 the next day, the condition that the threshold was exceeded twice over three intervals is met, so an alarm occurs.

The following figure shows an example of these settings.



8. Click the **Next >** button.

   The following window and the available alarm conditions depend on whether you select **Monitor whether the value exists** or not.

   - When **Monitor whether the value exists** has been selected:

     You are guided to the **Alarm Conditions** window. Go to *6.4.3 Setting a value whose existence is to be monitored* to set the conditional expression for

monitoring to check all of the fields for the value.

- When **Monitor whether the value exists** has not been selected:

  You are directed to the Alarm Conditions window. Go to *6.4.4 Setting the alarm conditions* to set the alarm conditions.

6.4.3 Setting a value whose existence is to be monitored

To set a value whose existence you want to monitor:

1. Set the value whose existence is to be monitored.

   For example, if you want to monitor whether a particular process is running for PFM - Agent for Platform (Windows), you can specify the following settings:

   Record: `Process Detail (PD)`

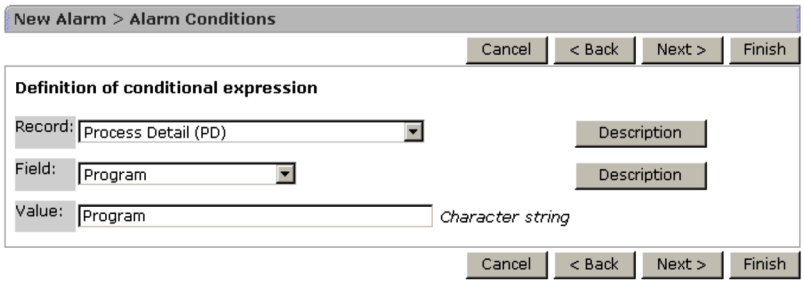
   Field: `Program`

   Value: *name-of-the-program-to-be-monitored*#

   # You can specify alphabetical characters (upper-case and lower-case). The system distinguishes between upper and lower-case characters. The specified program name does not need an extension. You can also use the wildcard character (`*`). For example, by specifying `*AAA*`, you can monitor any string that contains the substring `AAA`. To specify a backslash sign (\) immediately in front of a wildcard character in **Value**, you must specify `\\`.

   The following figure shows an example of these settings.

   Figure 6-5: New Alarm > Alarm Conditions window



2. Click the **Next >** button.

   You are directed to the New Alarm Table > Action window.

Note:

The fields of data type *time_t*, *timeval*, and *utime* are not displayed in a **Field** because they cannot be used in the conditional expressions of the alarm.

To specify a backslash sign (\) immediately in front of a wildcard character in **Value**, you must specify \\.

6.4.4 Setting the alarm conditions

To set the alarm conditions:

1. Set the alarm conditions.

   For example, if you want to monitor the busy state of a processor for the PFM - Agent for Platform (Windows), issue a Warning alarm when the usage of the processor exceeds 80% and issue an Abnormal alarm when it exceeds 90%, you can specify the following settings:

   Record: `System Overview (PI)`

   Field: `CPU%`

   Condition: `>`

   Abnormal value: `90`

   Warning value: `80`

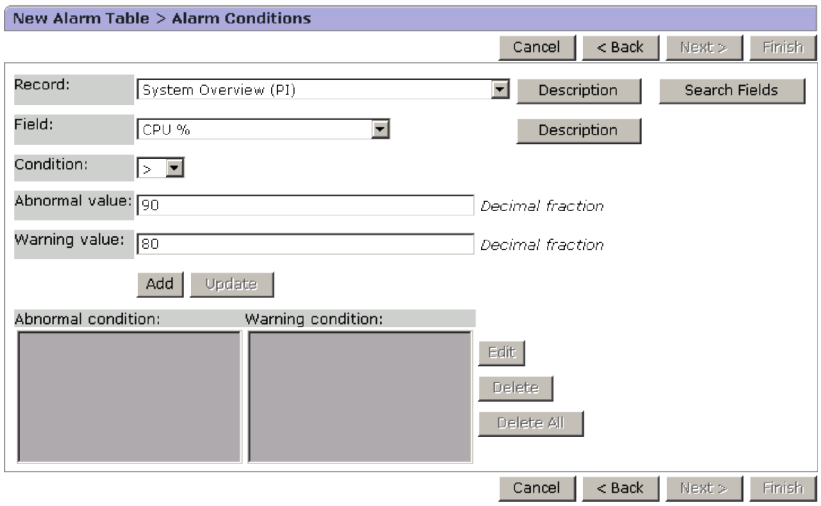
   You can search fields for a character string by clicking the **Search Fields** button. For details on searching for fields, see *(1) Searching for fields*.

   Note

   The evaluation of whether an alarm is in an abnormal condition is performed only after Warning conditions are met.

   Therefore, you must specify conditions for the Abnormal condition that will also be met for the Warning condition.

Figure 6-6: New Alarm > Alarm Conditions window



2. Click the **Add** button.

   The conditional expressions are added to both **Abnormal condition** and **Warning condition**.

   You can set multiple conditional expressions. Multiple conditional expressions are combined with Boolean AND operators. The alarm is issued only when all of the expressions are met.

   Note that when you select a conditional expression already added to **Abnormal condition** or **Warning condition**, and then set an alarm condition, clicking the **Update** button overwrites the selected conditional expression.

   Reference note:

   > You can use alphabetical characters (upper-case and lower-case) when you specify a string for the **Abnormal value** or **Warning value** in the conditional expression. The system distinguishes between upper and lower-case characters. You can also use the wildcard character (`*`). For example, by specifying `item name=*AAA*`, you can monitor any string that contains the substring `AAA`. Note that if you want to specify a backslash sign (`\`) just before the wildcard character, you must specify `\\`.

3. Click the **Next >** button.

   You are directed to the New Alarm > Action window. Go to *6.4.5 Setting the actions*.

(1) Searching for fields

This section describes how to use the New Alarm > Alarm Conditions window to

search for fields. You can include search results from the **Field** pull-down menu in the New Alarm > Alarm Conditions window.

To search for fields using the New Alarm > Alarm Conditions window:

1. Click the **Search fields** button in the New Alarm > Alarm Conditions window.

   The New Alarm > Alarm Conditions > Search Fields window appears.

2. Select the target records from the **Records to search** pull-down menu.

   The items of the pull-down menu are as follows:

   - **--All records--**

     Select this option to search for all records.

   - A list of record names of the selected agent

     A list of record names of the selected agent is displayed in alphabetical order.

3. Enter a character string for the field search into **Keywords to find** and click the **Search** button.

   The search results appear in the information frame.

   - When **--All records--** is selected as the target record

     The search results are listed for each record in the Search results record(s) window.

     If you click the anchor part of the relevant record, the search results are listed for each field in the New Alarm > Alarm Conditions > Search Fields window.

   - When a record name is selected as the target record

     The searched fields are listed in the New Alarm > Alarm Conditions > Search Fields window.

4. Select the radio button of the field that you want to select, and then click the **OK** button.

   The original New Alarm > Alarm Conditions window appears and the selected fields are included in the **Field** pull-down menu.

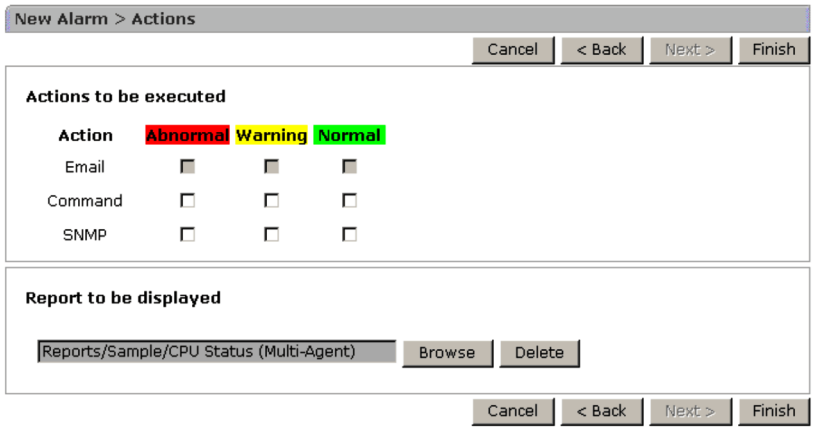
6.4.5 Setting the actions

Set the actions to be performed by the system when the status of the alarm changes. The possible actions are as follows:

- Send emails
- Execute commands

- Issue JP1 events
- Send an SNMP trap

Figure 6-7: New Alarm > Action window



Notes:

- You cannot select **Warning** if you select **Monitor whether the value exists** in the **General Setting** area of the New Alarm > Main Information window.
- You cannot select **Normal** if you select **Always notify** in the **Advanced settings** area of the New Alarm > Main Information window.
- You can combine multiple actions. However, you cannot combine the actions of executing commands with issuing JP1 events.

(a) Sending emails

To send an email when an alarm event occurs:

1. In the New Alarm > Action window, select **Email**.
2. Select a trigger for sending an email among **Abnormal**, **Warning**, or **Normal**.
3. Click the **Next >** button.

   The **Email Settings** area appears.
4. Set the address, the body, and so on of the email.

   For example, suppose you want to send the email under the following conditions:

   - Email address: Send the email to T.Hitachi@Dept01.Hitachi.com
   - Action handler: Send the email through the Action Handler service with the host name `WepAP`

- Email body: Send an email that says "date/time, host name, product name"

In this case, specify the following settings:

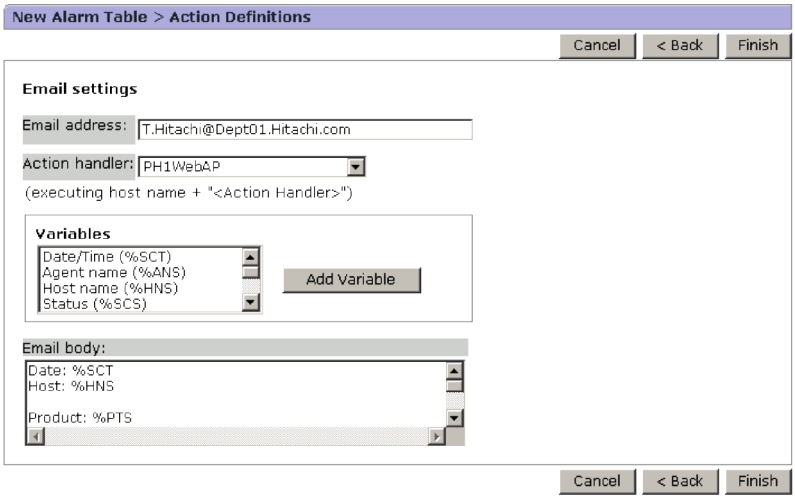
Email address: `T.Hitachi@Dept01.Hitachi.com`

Action handler: `PH1WebAP`

Email body: `Date:%SCT  Host:%HNS  Product:%PTS`

The following figure shows an example of these settings.

Figure 6-8: Edit > Action Definitions window



Reference note:

> You can use variables such as *%SCT* and *%MTS* for the **Email body** setting. For further details on the variable setting window, see the chapter that describes the window in the manual *Job Management Partner 1/ Performance Management Reference*.
>
> If you want to specify multiple email addresses for **Email address**, use a comma to separate them. You can enter a maximum of 127 characters for this setting.

5. Click the **Finish** button.

   The settings are applied.

(b) Executing commands

To execute commands when the alarm event occurs:

1. In the New Alarm > Action window, select **Command**.

2. Select a trigger for executing the command among **Abnormal**, **Warning**, or **Normal**.
3. Click the **Next >** button.

   The **Command Definition** area appears.

   Set the command name, command arguments, and so on.

   For example, suppose you want to execute the command under the following conditions:

   - To execute the `/usr/bin/LogOutput` command that outputs log data
   - To execute the command through the Action Handler of the WebAP host
   - To pass in the date/time, host name, and message text as the command parameters

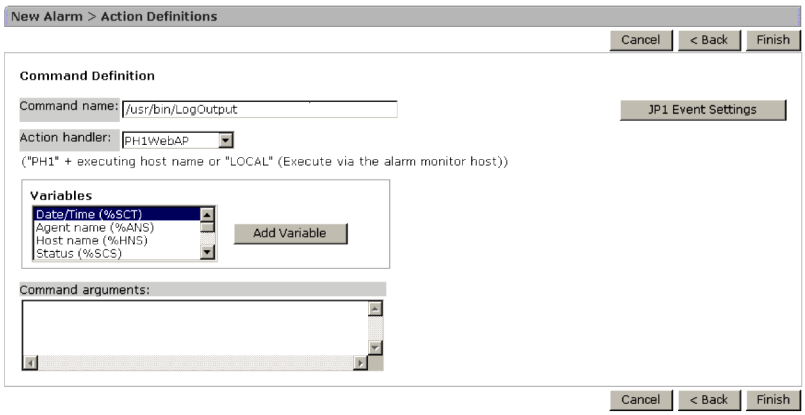
   In this case, specify the following settings:

   Command name: `/usr/bin/LogOutput`

   Action handler: `PH1WebAP`

   Command arguments: `Date:%SCT  Host:%HNS  %MTS`

   The following figure shows an example of these settings.



Note:

- You cannot use the following symbols in a character string that is passed to a command as a parameter:

  < >

  When these symbols are included in a character string, characters that appear before or after these symbols are sometimes truncated.
- You cannot redirect the standard output of a command to a file or other destination.

Reference note:

You can use some variables such as *%SCT* and *%MTS* in the setting of **Command arguments**. For further details on the variables, see the chapter that describes the window in the manual *Job Management Partner 1/ Performance Management Reference*.

4. Click the **Finish** button.

   The settings are applied.

(c) Issuing a JP1 event

For details on how to issue a JP1 event when an alarm event occurs, see *10.3.2(2) Defining alarm events and reports*.

(d) Sending an SNMP trap when an alarm occurs

To send an SNMP trap when an alarm event occurs:

1. In the New Alarm > Action window, select **SNMP**.
2. Select a trigger for sending the SNMP trap among **Abnormal**, **Warning**, or **Normal**.
3. Click the **Finish** button.

   The settings are applied.

(e) Notes on executing actions

The following are cautionary notes on executing actions:

1. Program required to send emails

   A mail server that conforms to SMTP is required for sending emails.

2. Executable files for executing commands

   - In Windows:

     To execute commands, you can run files with the following extensions:

- EXE: Executable files

- COM: Executable (command) files

- BAT: Batch files

If you want to execute internal commands such as DEL or DIR, you must make a batch file and execute such commands in the batch file.

Note that you can only specify program files that are accessible from the system account when the commands are executed. You cannot run files that are located in a network folder.

- In UNIX:

To execute commands, you can run the files listed below. Note that these files must have the execute attributes added to them.

- Executable files

- Shell script files

Note that you can only specify program files that are accessible by users with the root user permission when the commands are executed. To run files that are located in an NFS-mounted directory, those files must be made accessible by users with the root user permission on that host.

3. Account for command execution

- In Windows:

You must use the system account for executing commands (for the Action Handler service, as well).

Therefore, any resources that are viewed or updated from the program must be accessible from the system account.

- In UNIX:

You must use an account with the root user permission for executing commands (note that the account for the Action Handler service has the root user permission).

Therefore, any resources that are viewed or updated from the program must be accessible from an account with the root user permission.

4. The values of the environment variables available when a command is executed

- In Windows:

The environment variables used when a command is executed are the system environment variables that were in effect when the Performance Management program service started.

The profile information is not loaded when a command is executed.

- In UNIX:

  The environment variables used when a command is executed are the environment variables associated with the root user permission when the Performance Management program service started.

  The profile information is not loaded when a command is executed. For details on umask, see *6. Umask for the files generated when a command is executed*.

5. Current directory during the execution of commands

   - In Windows:

     The current folder during the execution of commands is the folder of the Action Handler service (*installation-folder*`\bin\action`).

     For logical hosts, the current folder during executing of commands is *environment-directory*`\jp1pc\bin\action`.

   - In UNIX:

     The current directory during the execution of commands is the directory of the Action Handler service (`/opt/jp1pc/bin/action`).

     For logical hosts, the current directory during executing of commands is *environment-directory*`/jp1pc/bin/action`.

6. Umask for the files generated when a command is executed

   - In Windows:

     Umask is not applicable to the Windows environment.

   - In UNIX:

     When a command is executed, umask is set to `000` (the file permissions become `777`). When you want to modify umask, you must reset umask in the script file you execute or in the program.

7. Other notes on executing commands

   - In Windows:

     - You cannot run a Win16-bit application.

     - You cannot run an application that displays a window or a dialog box.

     However, you can execute the `net send` command to display a dialog box. This is because the dialog box is displayed by the Messenger service of Windows, and not by the `net send` command.

     - You cannot run an application that utilizes the Windows messaging

mechanism, DDE (Dynamic Data Exchange).

- You cannot run an application that requires interactive operations.

- You cannot run a resident program that does not terminate.

- You cannot run a file with an extension that is associated with an application.

- You cannot run programs that are located in a network folder.

- Do not set up a program on a removable disk that is not ready for use.

- Do not allow services to interact with the desktop in the startup settings of the Windows services.

- You cannot retrieve information from the standard output or standard error of the executed program.

- In UNIX:

  - You cannot run an application that requires interactive operations.

  - You cannot run a program that involves a `stty`, `tty`, `tset`, or `script` command and requires an interactive operation environment.

  - You cannot run a resident program, which does not terminate.

  - You cannot run a program that does not have the execute attributes added to it.

  - Do not set up a program on a removable disk that is not ready for use.

  - You cannot retrieve the information from the standard output or standard error of the executed program.

8. Notes on Action Handler labels

   If you set an action for an alarm and select something other than **LOCAL** for **Action handler** in the **Command** field on the New Alarm > Action Definitions window of the PFM - Web Console's browser, the load on PFM - Manager might increase severely. When an alarm triggers an action in a large system, select **LOCAL** for **Action handler** in the **Command** field on the New Alarm > Action Definitions window to prevent the load from centralizing on the PFM - Manager host.

6.4.6 Associating a report with an alarm

To display a report when a defined alarm occurs, associate the report with the alarm in the New Alarm > Action window.

Settings prior to setting associated reports

You need to create the desired report in the Reports window prior to setting it up

as an associated report. For details on how to create reports, see *5. Creation of Reports for Operation Analysis*.

To associate a report with an alarm:

1. In the **Report to be displayed** area of the New Alarm > Action window, click the **Browse** button.

   The New Alarm > Action > Select a report window appears.

2. From the Reports, select a report to be associated with the alarm.

   The selected report is marked with a checkmark.

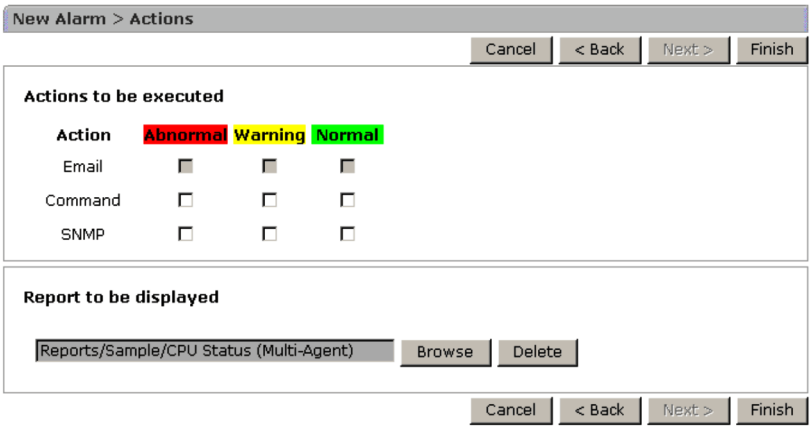
   Only reports that are for the same product and for the same or lesser version of the data model as the alarm you are creating are displayed.

3. Click the **OK** button.

   The report is associated with the alarm.

   The following figure shows an example of the settings in the New Alarm > Action window.

   Figure 6-9: New Alarm > Action window



4. Click the **Finish** button.

For details on how to display a report associated with an alarm, see *5.7.1(2) Displaying a report associated with an alarm*.

6.4.7 Copying an alarm table or alarm

The sections describe how to copy an alarm table or alarm.

(1) Copying an alarm table

To copy a monitoring template or alarm table:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm table to copy.

   The selected report is marked with a checkmark.

4. In the method frame, select **Copy**.

   In the information frame, the Copy > Input Name (Alarm Table) window appears.

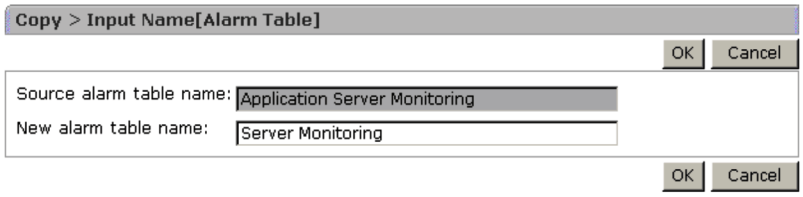
5. Enter the new alarm table name.

   New alarm table name

   You can use up to 64 bytes of alphanumeric characters, spaces, and the following symbols: % - ( ) _ . / @ []. Note that you cannot specify an alarm table name that begins with `PFM`.

   The following figure shows an example of this setting.

   Figure 6-10: Copy > Input Name [Alarm Table] window



6. Click the **OK** button.

   The alarm table selected in step 3 is copied into the same location as the original alarm table.

Supplemental information:

The alarm table cannot be copied into a folder different from the folder of the original alarm table.

(2) Copying an alarm

When you want to add an alarm to the alarm table, you can copy an existing alarm.

To copy an alarm:

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

The main window appears.

You must log on as a user with administrator user permissions.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm to copy.

   The selected alarm is marked with a checkmark.

4. In the method frame, select **Copy**.

   In the information frame, the Copy > Input Name (Alarm) window appears.

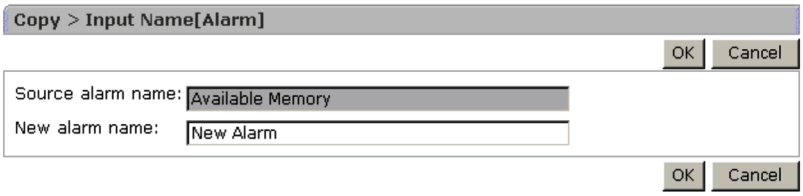
5. Enter the new alarm name.

   New alarm name

   You can use up to 20 bytes of alphanumeric characters, spaces, and the following symbols: % - ( ) _ . / @ [].

   The following figure shows an example of this setting.

   Figure 6-11: Copy > Input Name [Alarm] window



6. Click the **OK** button.

   The alarm selected in step 3 is added.

   Supplemental information:

   The alarm can only be copied into the alarm table where the original alarm is.

6.4.8 Editing an alarm

To edit an alarm:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm to edit.

   The selected alarm is marked with a checkmark.

4. In the method frame, select **Edit**.

   In the information frame, the Edit > Main Information window appears.

5. Edit the definition of the alarm.

   The subsequent steps are similar to those when creating a new alarm. For details on those procedures, see the sections from *6.4.2 Creating an alarm (setting the basic information)* to *6.4.5 Setting the actions*.

   Supplemental information:

   When you edit an existing alarm, you cannot modify **Product**, **Alarm table name**, or **Alarm name**.

6.4.9 Deleting an alarm table or alarm

You can delete alarm tables or alarms that are no longer needed. The following sections describe how to do this.

(1) Deleting an alarm table

To delete an alarm table:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm table to delete from the folder of the monitoring agent.

   The selected alarm table is marked with a checkmark.

4. In the method frame, select **Delete**.

   A message box to confirm your deletion appears.

5. Click **OK** in the message box.

   The alarm table selected in step 3 is deleted.

Supplemental information:

You can delete alarm tables even when they are active (bound to the monitoring agent).

Note that you cannot delete any alarm tables that begin with PFM.

(2) Deleting an alarm

To delete an alarm:

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

   The main window appears.

   You must log on as a user with administrator user permissions.
2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.
3. In the navigation frame, select the alarm to delete from the folder of the monitoring agent.

   The selected alarm is marked with a checkmark.
4. In the method frame, select **Delete**.

   A message box to confirm your deletion appears.
5. Click **OK** in the message box.

   The alarm selected in step 3 is deleted.

Supplemental information:

You can delete alarm tables even when they are active (bound to the monitoring agent). When you delete all of the alarms in an alarm table, the alarm table itself is also deleted.

6.4.10 Exporting alarm tables

To export one or more alarm tables:

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

   The main window appears.

   You must log on as a user with administrator user permissions.
2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.
3. In the alarms of the navigation frame, select targets to be exported.

   The report is exported according to the selected target as follows:

   - When the root **Alarms** is selected:

     All the folders and alarm tables under **Alarms** are exported.

- When a folder is selected:

  The selected folder and alarm tables under it are exported.

- When an alarm table is selected:

  The selected alarm table is exported.

4. In the method frame, select **Export**.

   The Download File window appears.

5. Click the **Save** button.

   The Save As window appears.

6. Specify the export destination and the file name.

   The target selected in step 3 is output to the file specified here.

7. Click the **Save** button.

   The target selected in step 3 is exported.

Note

You can export alarm definition files from the PFM - Web Console window in binary format.

6.4.11 Importing alarm tables

To import the alarm table:

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

   The main window appears.

2. In the tab frame of the main window, select the **Alarms** tab.

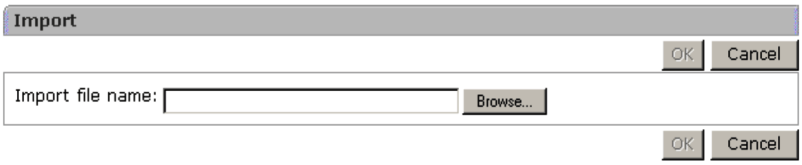
   The Alarms window appears.

3. In the method frame, select **Import**.

   The Import window appears.

   The following figure shows an example of the Import window.

   Figure 6-12: Import window



4. Click the **Browse** button of **Import file name**.

The **Select File** window appears.

5. Select the definition file of the alarm to be imported.

   The root, folders, and alarm tables described in the definition file to be selected here are imported.

6. Click the **OK** button.

   A message box to confirm your replacement appears.

7. If you want to replace the definition file of the alarm table, click the **OK** button in the message box.

   The alarm tables are imported.

Note:

If importing an alarm table causes one of the already bound alarm tables to be overwritten, the alarm table is unbound. You must rebind the alarm table, if necessary.

6.5 Setting alarms by using the Quick Guide

You can use the Quick Guide to create simplified alarm definitions by setting the minimum items. For details on the default values of an alarm that was created by using the Quick Guide, see *6.5.2 The default values of an alarm created by using the Quick Guide*.

6.5.1 Procedure for creating alarms by using the Quick Guide

The procedure for creating an alarm by using the Quick Guide is shown below. For details on how to create a report, see *5.4 Creating reports by using the Quick Guide*.

To create an alarm by using the Quick Guide:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. From the **Display format** pull-down menu in the navigation frame, select the display format for the Agents tree.

   The Agents tree appears in the selected display format.

   - When **User Agents** is selected:

     The Agents tree that has **User Agents** (*logged-on-user-name*) as the root appears.

   - When **Products** is selected:

     The Agents tree that has **Products** as the root appears.

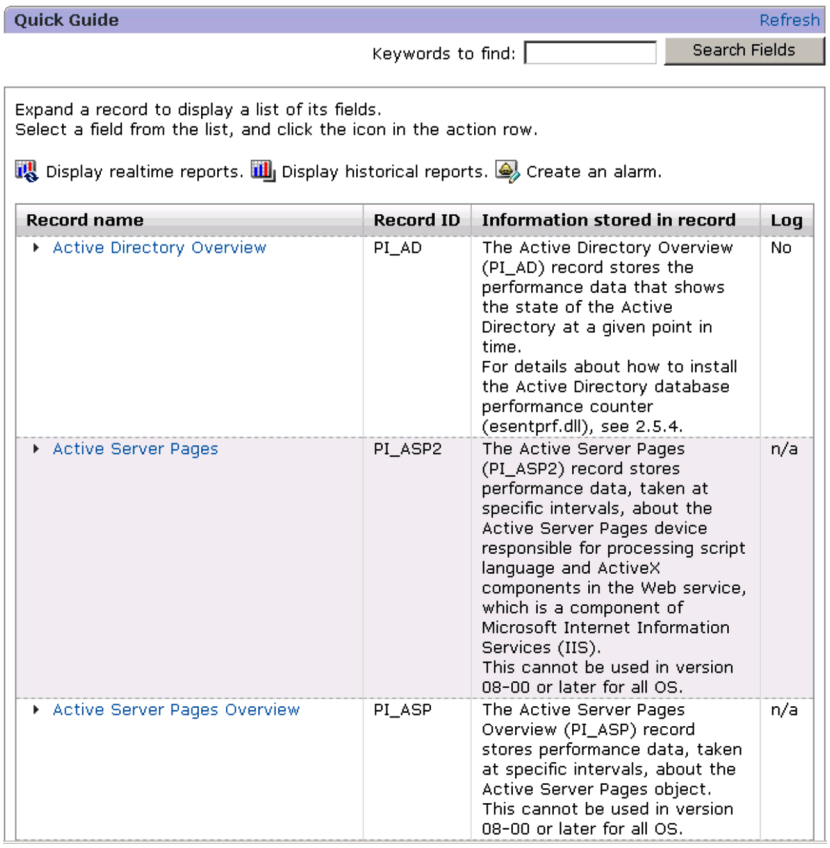
4. From the **Agents** tree in the navigation frame, select the agent for which you want to create an alarm.

   The selected agent is marked with a checkmark.

5. Choose the **Quick Guide** button in the method frame.

   The Quick Guide window appears.

Figure 6-13: Quick Guide window



6. Display a field for which you want to create an alarm.

   You can use one of the following ways to display a field:

   - Click and expand the appropriate record name anchor and select fields from the displayed list.
   - Search fields for a specific character string and select fields from the search results.

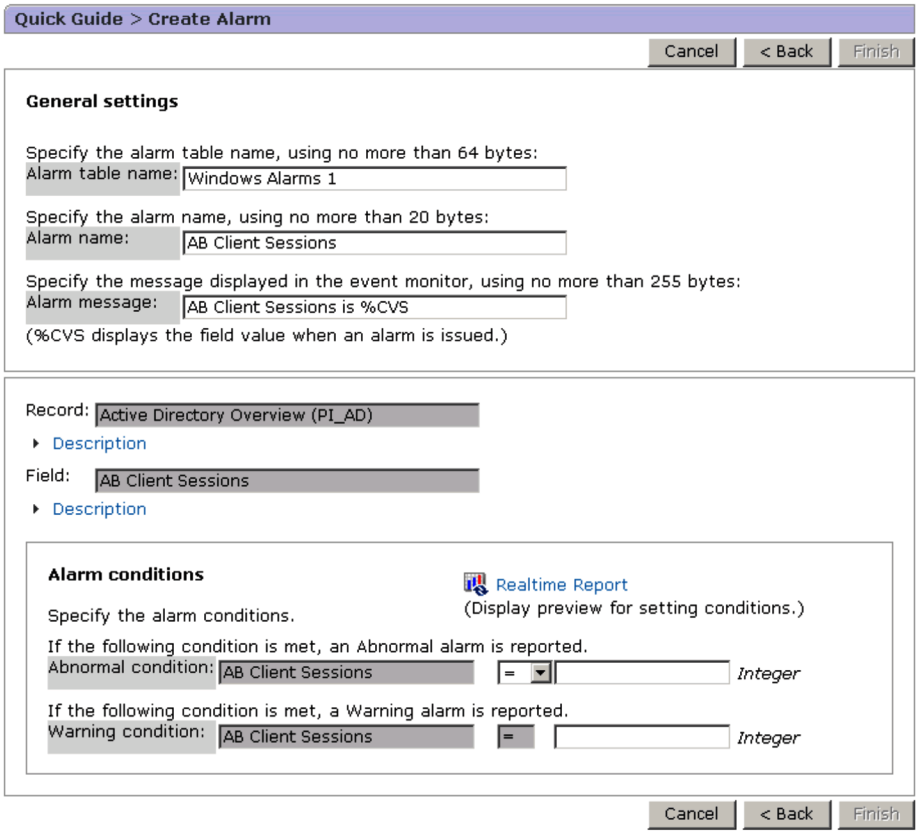
     You can search fields by entering a search string into **Keyword** and clicking the **Search Fields** button. For details on searching for fields, see *5.4.2 Searching fields*.

7. Click an alarm icon that is displayed in the field.

   If you click an alarm icon, the Quick Guide > Create Alarm window appears.

- Alarm icon: 

Figure 6-14: Quick Guide > Create Alarm window (Quick Guide)



8. Enter a value for **Abnormal condition** and **Warning condition** of conditional expressions.
9. If necessary, enter a value for **Alarm table name**, **Alarm name**, and **Alarm message**.

   The default alarm table name, alarm name and alarm message are preset. You can change these items as required.
10. Click the **Finish** button.

    The KAVJJ8554-Q message appears.
11. Choose **Yes** or **No**.

    The alarm will be created. If you choose **Yes**, the created alarm table is bound to

the agent selected in step 4. If you choose **No**, the alarm table is not bound to an agent.

6.5.2 The default values of an alarm created by using the Quick Guide

The following table shows the default values of an alarm that is created by using the Quick Guide.

Table 6-1: Default values of an alarm created by using the Quick Guide

Item			Default value	Edit
Main Information	General	Product	The earliest version of the data models used by the agent products or agents selected by the user	--
		Alarm table name	The value entered in the alarm creation window	Y
		Alarm name	The value entered in the alarm creation window	Y
		Alarm message	The value entered in the alarm creation window	Y
		Monitor whether the value exists	Off	--[#1]
	Advanced settings	Enable alarm	On	--
		Always notify	Off	
		Evaluate all data	Off	
		Monitoring time range	Always monitor: On	
		Damping	**Report alarm when the following damping condition is met**: Off	
Alarm Conditions		Record	The record containing the field selected in the window for selecting fields	Y[#2]
		Field	The field selected in the window for selecting fields	
		Abnormal condition	The value entered in the alarm creation window	Y[#3]

Item		Default value	Edit
	Warning condition	The value entered in the alarm creation window	
Actions	Actions	All off	--
	Report to be displayed	None	--#4

Legend:

Y: You can edit the setting.

--: You cannot edit the setting.

#1

You cannot create an alarm that monitors whether a value exists.

#2

You cannot edit the settings in the Quick Guide > Create Alarm window. Select them in the window for selecting fields.

#3

You can only specify one condition for the alarm condition.

#4

You cannot associate a report to be displayed with an alarm. However, you can display a report of an alarm for which a report is not associated.

6.6 Operating alarms by using the browser

This section explains how to operate alarms from the PFM - Web Console window.

6.6.1 Changing the association between an alarm table and a monitoring agent

An alarm table is a collection of several alarms. For Performance Management to monitor with alarms, you must associate one or more alarm tables with a monitoring agent. This association is known as *binding*. Canceling a bound alarm table is called *unbinding*. You can bind an alarm table to multiple monitoring agents, or bind one or more alarm tables to a monitoring agent. To bind more than one alarm table to a single monitoring agent, you must enable the functionality for binding multiple alarm tables using PFM - Manager, beforehand. For details on how to set this functionality, see the chapter that describes installation and setup in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

The following describes the procedures for changing the association of an alarm table:

(1) When the functionality for binding multiple alarm tables is enabled

If the functionality for binding multiple alarm tables is enabled, you can both bind and unbind alarm tables in a single window.

To change the association of an alarm table when the functionality for binding multiple alarm tables is enabled:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

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

   The Agents window appears.

3. In the **Display format** pull-down menu in the navigation frame, select **Products**.

   The agent tree organized by products appears.

4. In the navigation frame, select the monitoring agent to bind to the alarm table.

   The selected agent is marked with a checkmark.

   If you select **Multiselect**, you can select multiple agents.

Hint:

To bind an agent monitored by PFM - RM, select the appropriate remote or group agent as the monitored agent.

5. In the method frame, select the **Alarm Table Bind Settings** method.

   In the information frame, the Alarm Table Bind Settings [Select Alarm Tables] window appears.

   For binding:

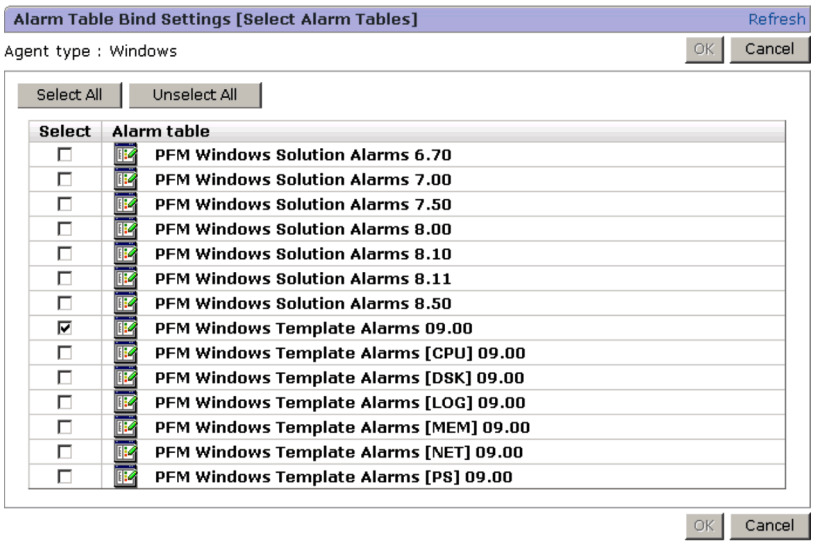
   Select one or more alarm tables to bind. After you select alarm tables, the selected alarm tables are marked with a checkmark. You can select no more than 50 alarm tables.

   For unbinding:

   Clear the selection for the alarm table to unbind it.

   The following figure shows an example of the Alarm Table Bind Settings [Select Alarm Tables] window.

   Figure 6-15: Alarm Table Bind Settings [Select Alarm Tables] window



   Reference note:

   You can only bind or unbind alarms on an alarm table basis. Therefore, you cannot bind or unbind individual alarms separately.

6. Click the **OK** button.

The alarm table selected in step 5 is bound to or unbound from the agent selected in step 4.

Reference note:

When an alarm table is bound or unbound, all the alarms bound to the monitoring agent are reset to **Normal Status**. If an alarm table is bound to a monitoring agent that has one or more alarm tables already bound to it, all the alarms in the alarm tables including the existing alarm tables are reset to **Normal**. These alarms are then set to their actual state the next time they are evaluated.

(2) When the functionality for binding multiple alarm tables is disabled

(a) Associating an alarm table with a monitoring agent

Note

Each agent can only have one alarm table bound to it. If you bind an alarm table to an agent already bound to another alarm table, the existing alarm table is unbound automatically and the new alarm table is bound.

When the functionality for binding multiple alarm tables is disabled, you can only bind one alarm table to an agent. Alternately, you can use the Quick Guide to set simplified alarms. For details on the Quick Guide, see *6.5 Setting alarms by using the Quick Guide*.

To bind an alarm table when the functionality for binding multiple alarm tables is disabled:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

   You must log on as a user with administrator user permissions.

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

   The Agents window is displayed.

3. In the **Display format** pull-down menu in the navigation frame, select **Products**.

   The **Agents** tree organized by products appears.

4. In the navigation frame, select the monitoring agent to bind to the alarm table

   The selected agent is marked with a checkmark.

   If you select **Multiselect**, you can select multiple agents.

Hint:

To bind an agent monitored by PFM - RM, select the appropriate remote or group agent as the monitored agent.

5. In the method frame, select the **Bind Alarm Table**.

   In the information frame, the Bind Alarm Table to Agents (Select Alarm Table) window appears.

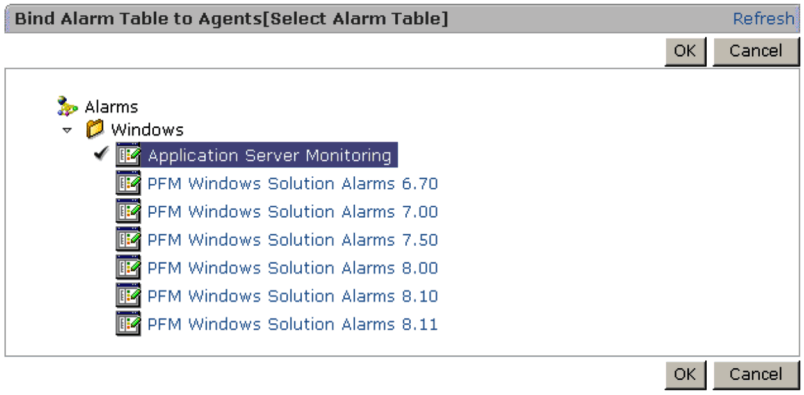
6. Select the alarm table to bind.

   The selected alarm table is marked with a checkmark.

   You cannot select multiple alarm tables.

   The following figure shows an example of the Bind Alarm Table to Agents (Select Alarm Table) window.

   Figure 6-16: Bind Alarm Table to Agents [Select Alarm Table] window



   Reference note:

   You can bind alarms only on an alarm table basis. You cannot bind individual alarms separately.

7. Click the **OK** button.

   The alarm table selected in step 6 is bound to the agent selected in step 4.

(b) Unbinding an alarm table bound to a monitoring agent

To unbind an alarm table when the functionality for binding multiple alarm tables is disabled:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

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

   The Agents window appears.

3. In the **Display format** pull-down menu in the navigation frame, select **Products**.

   The agent tree by products appears.

4. In the navigation frame, select the monitoring agent to unbind the alarm table from.

   The selected agent is marked with a checkmark. If you select **Multiselect**, you can select multiple agents.

Hint:

To unbind an agent monitored by PFM - RM, select the appropriate remote or group agent as the monitored agent.

5. In the method frame, select the **UnBind Alarm Table**.

   The message box to confirm the unbinding of the alarm table appears.

6. If you want to unbind, click the **OK** button in the message box.

   The alarm table is unbound from the monitoring agent selected in step 4.

(3) Notes on the limit on the number of alarms and alarm tables

You can create up to 50 alarms in one alarm table. In addition, you can bind up to 50 alarm tables to one agent.

Binding a large number of alarms to PFM - Agent or PFM - RM in the Performance Management system might delay the processing of PFM - Manager, PFM - Agent, or PFM - RM. We recommend that you limit the number of bound alarms to the following:

- 250 alarms per agent.
- 10,000 alarms across the entire Performance Management system.

6.6.2 Displaying the monitoring agents bound to an alarm table

You can check which monitoring agents are bound to an alarm table.

To display the monitoring agents bound to an alarm table:

1. In the navigation frame of the Alarms window, select the alarm table for which you want to display bound monitoring agents.
2. In the method frame, select the **Show Bound Agents** method.

   A list of the agents bound to the selected alarm table appears in the information frame.

6.6.3 Stopping monitoring with an alarm

You can temporarily stop and then start monitoring with an alarm without unbinding the alarm from the monitoring agent.

If you want to not only stop monitoring but also unbind the alarm definition from the monitoring agent, see *6.6.1(2)(b) Unbinding an alarm table bound to a monitoring agent*.

To stop monitoring:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm tables to stop monitoring from the folder of the monitoring agent.

   The selected alarm table is marked with a checkmark.

4. In the method frame, select **Activate**.

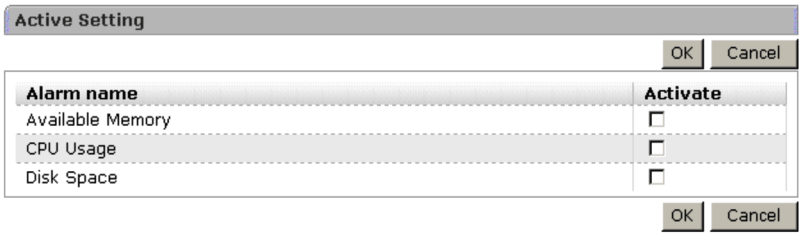
   The Activate window appears.

5. Change the setting of **Activate**.

   Deselect **Activate** for the alarm for which monitoring is to stop.

   The following figure shows an example of this setting.

   Figure 6-17: Active Setting window 1



6. Click the **OK** button.

   The monitoring with the alarm stops.

6.6.4 Starting monitoring with an alarm

You can temporarily stop, and then start monitoring with an alarm without unbinding the alarm from the monitoring agent.

To start monitoring:

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

   The main window appears.

   You must log on as a user with administrator user permissions.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm tables to start monitoring from the folder of the monitoring agent.

   The selected alarm table is marked with a checkmark.

4. In the method frame, select **Activate**.

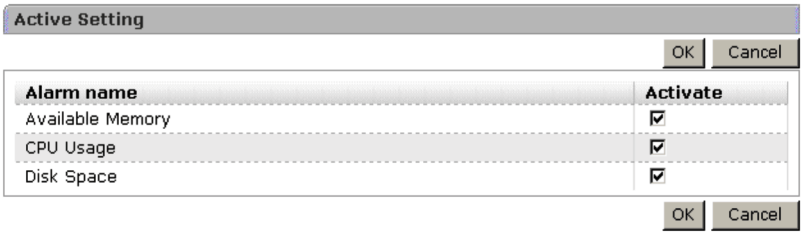
   The Activate window appears.

5. Change the setting of **Activate**.

   Check **Activate** for the alarm for which monitoring is to start.

   The following figure shows an example of this setting.

   Figure 6-18: Active Setting window 2



6. Click the **OK** button.

   The monitoring with the alarm starts.

6.6.5 Displaying alarm properties (definitions)

This section explains how to check alarm properties. You can check alarm properties from one of the following windows:

- The Alarms window

  Here you can check the properties of all the alarms.

- The Agents window

  Here you can check the properties of the alarms contained in the alarm table bound to an agent.

- The Event Monitor window

  Here you can check the properties of the alarms that have issued alarm events.

Only management users can display alarm properties from the Alarms window.

(1) Checking from the Alarms window

To display alarm properties from the Alarms window:

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

   The main window appears.

2. In the tab frame of the main window, select the **Alarms** tab.

   The Alarms window appears.

3. In the navigation frame, select the alarm to display the properties for from the folder of the monitoring agent.

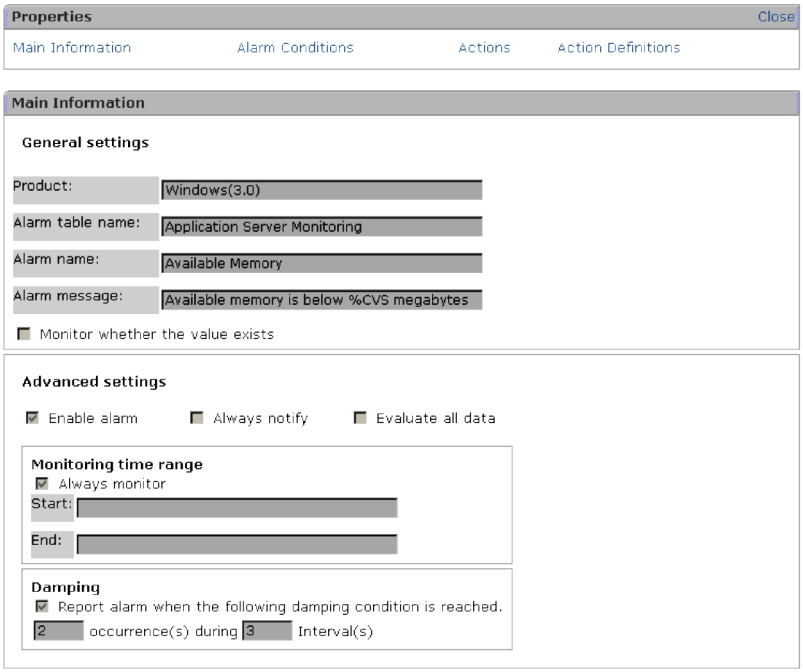
4. In the method frame, select **Properties**.

   The Properties window appears.

   Click **Main Information**, **Alarm Conditions**, **Action**, and **Action Definitions** on the menu-bar to jump to the corresponding information.

   The following figure shows an example of the Properties window.

Figure 6-19: Properties window



(2) Checking from the Agents window

To display the properties of the alarms from the Agents window:

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

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame, select the agent whose alarm properties you want to check from the agent tree.

4. In the method frame, select the **Display Alarm Status** method.

   The Display Alarm Status window appears.

(3) Checking from the Event Monitor window

To display the properties of the alarms from the Event Monitor window:

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

   The main window appears.

2. In the toolbar frame of the main window, select the **Event Monitor** menu.
   The Event Monitor window appears as a separate window.
3. From the **View** pull-down menu, select **Alarm events**.
   The alarm events are listed.
4. Select the icon of the alarm whose properties you want to display.
   The Alarm Properties window appears as a separate window.

6.7 Setting alarms by using commands

This section explains how to set up alarms by using commands.

6.7.1 Creating an alarm definition file

(1) Outputting the template file for the alarm definition file

To create an alarm definition file, first output the template file that includes all of the labels that need to be defined in the alarm definition file.

For example, we will output the template file called `/tmp/alarmtmp01.cfg`.

To output the template file for the alarm definition file:

1. Output the template file.

   To output the template file, you can use the `jpctool alarm export` command. Execute the command with the `-template` option, as follows:

   ```
   jpctool alarm export -f /tmp/alarmtmp01.cfg -template
   ```

   The output is shown below.

   ```
   #Alarm Definition File Version=0001
   #Alarm Definition File Code=

   #[Alarm Data]
   #[[General]]
   #Product=
   #Alarm Table Name=
   #Alarm Name=
   #Message Text=
   #Check Value Exist=N

   #[[Advanced Setting]]
   #Active Alarm=Y
   #Regularly Alarm=Y
   #Evaluate All Data=N
   #Monitoring Regularly=N
   #Monitoring Time=
   #Damping=N
   #Damping Count=

   #[[Check Value Exist]]
   #Record=
   #Field=
   ```

```
#Value=

#[[Alarm Condition Expressions]]
#Condition=

#[[Actions]]
#Report=
#E-mail=Abnormal,Warning,Normal
#Command=Abnormal,Warning,Normal
#SNMP=Abnormal,Warning,Normal
#JP1 Event=N

#[[Action Definition E-mail]]
#E-mail Address=
#Action Handler=

#[[[Message Text]]]
#Date: %SCT
#Host: %HNS
#
#Product: %PTS
#Agent: %ANS
#
#Alarm: %AIS (%ATS)
#State: %SCS
#
#Message: %MTS

#[[Action Definition Command]]
#Command Name=
#Action Handler=

#[[[Message Text]]]
#
#[[Action Definition JP1 Event]]
#Event ID=
#Message=%MTS
#Switch Alarm Level=Y
#Action Handler=
#Exec Logical Host=
```

Note that each line in the template file begins with a sharp (#). Lines that begin with a sharp are comment lines.

For details on the `jpctool alarm export` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

(2) Creating the alarm definition file

Edit the output template file `/tmp/alarmtmp01.cfg` into an alarm definition file.

To create the alarm definition file:

1. Open the `/tmp/alarmtmp01.cfg` file with a text editor or other tool.
2. Define the header part of the alarm definition file.

   Define the header part. In the header part, define the syntax version of the alarm definition file and the character set to use to write the file. These values are defined in the following portion:

   ```
   #Alarm Definition File Version=0001
   #Alarm Definition File Code=
      :
   ```

   Delete the sharps (`#`) at the beginning of these lines, and edit the lines as follows:

   ```
   Alarm Definition File Version=0001
   Alarm Definition File Code=C
      :
   ```

   - `Alarm Definition File Version` label

     This is the syntax version of the alarm definition file.

     For PFM - Manager 08-00 or later, this must be `0001`, which is set in the template file by default.

     You cannot omit this item.

   - `Alarm Definition File Code` label

     This is the character code used to create the alarm definition file. Specify `C` or `UTF-8`.

     You cannot omit this item.
3. Define the PFM - Agent or PFM - RM type, the version of the data model, the alarm table name, and the alarm name.

   Define individual alarms. The definition of an alarm is coded in the `Alarm Data` section. For each alarm definition, you must create an `Alarm Data` section.

   Each `Alarm Data` section consists of different subsections.

   The following values are defined in the `General` subsection.

   - PFM - Agent or PFM - RM type

- Version of the data model
- Alarm table name
- Alarm name

These values are defined in the following portion:

```
   :
#[Alarm Data]
#[[General]]
#Product=
#Alarm Table Name=
#Alarm Name=
#Message Text=
#Check Value Exist=N
```

In this example, we define the alarm Free Space (hda3) that monitors the free space of the disk `/dev/hda3`.

Delete the sharps (`#`) at the beginning of these lines, and edit the lines as follows:

```
[Alarm Data]
[[General]]
Product=U4.0
Alarm Table Name=Disk Monitoring
Alarm Name=Free Space (hda3)
Message Text=Free Space (%CVS%)
Check Value Exist=N
   :
```

If the content of `Alarm Table Name`, `Alarm Name`, or `Message Text` includes space(s), you must enclose the item in double quotation marks (`"`).

For the `Alarm Table Name` label, you cannot specify a name that begins with `PFM`.

- `Product` label

  Defines the PFM - Agent or PFM - RM type and the data model version. With this label, both the product ID of PFM - Agent or PFM - RM and the version of the data model are defined.

  You cannot omit this item.

- `Alarm Table Name` label

  Defines the alarm table name in 1 to 64 bytes.

  You cannot omit this item.

- `Alarm Name` label

Defines the alarm name in 1 to 20 bytes.

You cannot omit this item.

- `Message Text` label

  Defines (in 0 to 255) bytes the content of the variable *%MTS*, which is used in the message text sent by the email or the JP1 event.

  An empty string is used by default.

- `Check Value Exist` label

  Defines whether the alarm monitors whether a value exists.

  - To define the alarm as monitoring whether a value exists: `Y`

    In this case, you must define the record and the value to be monitored in the `Check Value Exist` subsection.

    Note that you cannot specify `Warning` for the `E-mail`, `Command`, or `SNMP` label in the `Actions` subsection.

  - To define an ordinary alarm: `N`

    In this case, you must define the alarm conditions in the `Alarm Condition Expressions` subsection.

  `N` is the default value.

4. Define the conditions for the alarm.

Note:

The evaluation of whether an alarm is in an abnormal condition is performed only after Warning conditions are met.

Therefore, you must specify conditions for the Abnormal condition that will also be met for the Warning condition.

When defining an ordinary alarm (when you specify `Check Value Exist=N` in the `General` subsection), define the conditions for the alarm.

You can define the conditions for the alarm in the `Alarm Condition Expressions` subsection.

If you define an ordinary alarm, you cannot omit this subsection.

The conditions for the alarm are defined in the following portion:

```
   :
#[[Alarm Condition Expressions]]
#Condition=
   :
```

For the Condition label, code the conditional expressions for the alarm using the record name and the field name to be monitored.

In this example, we will monitor two items, the disk name and the free space, so we need to define two conditional expressions.

- The conditional expression to determine the disk to be monitored

  The disk name is stored in the File System (FILESYSTEM_NAME) field of the File System Detail - Local (PD_FSL) record. The value of this field is used for the judgment condition.

  ```
  PD_FSL_FILESYSTEM_NAME="/dev/hda3","/dev/hda3"
  ```

The left side of the conditional expression specifies the field name of the record to be used for the judgment in the form of the PFM - Manager name.

The right side of the conditional expression specifies the judgment conditions for Abnormal and Warning, separated by a comma.

In this example, we specify the same values to monitor the same disk for both Abnormal and Warning.

- The conditional expression to judge the free space ratio

  The free space is stored in the Mbytes Free % (TOTAL_MBYTES_FREE_PERCENT) field of the File System Detail - Local (PD_FSL) record. The value of this field is used for the judgment condition.

  ```
  PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20
  ```

  In this example, we will define a free space ratio lower than 10% as Abnormal and one lower than 20% as Warning.

Delete the sharps (#) at the beginning of the appropriate lines, and code these conditional expressions combined with an AND operator in the alarm definition file.

```
   :
[[Alarm Condition Expressions]]
Condition=PD_FSL_FILESYSTEM_NAME="/dev/hda3","/dev/hda3"
AND PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20
   :
```

If you specify strings on the right side of the conditional expression (the Abnormal and Warning values), you must enclose them in double quotation marks (").

To specify a hash mark (#) to the right of a conditional expression, you must specify \#.

The right side of a conditional expression must not contain (,), [,], <, >, =, or ".

To use these characters, use the wildcard character (*) to specify a conditional expression. To specify a backslash sign (\) immediately before the wildcard character to the right of a conditional expression, you must specify \\.

5. Define the actions to be taken when the alarm occurs.

   You can define the actions to be taken when the alarm occurs in the Actions subsection. The actions to be taken when the alarm occurs are defined in the following portion:

```
    :
#[[Actions]]
#Report=
#E-mail=Abnormal,Warning,Normal
#Command=Abnormal,Warning,Normal
#SNMP=Abnormal,Warning,Normal
#JP1 Event=N
    :
```

   Code the following to have an email sent when the Abnormal alarm status is reached and a JP1 event issued when the Abnormal or Warning status is reached:

```
    :
[[Actions]]
#Report=
E-mail=Abnormal
Command=Abnormal,Warning
#SNMP=Abnormal,Warning,Normal
JP1 Event=Y
    :
```

   - E-mail label

     Defines the alarm status that triggers an email to be sent.

     - To have emails sent in the Abnormal status: Abnormal

     - To have emails sent in the Warning status: Warning

     - To have emails sent in the Normal status: Normal

     If you want to specify multiple statuses for the action, separate them with commas.

     If you specify a status here, you must define the details of the emails in the Action Definition E-mail subsection.

     You can omit this item.

   - Command label

     Defines the alarm status for which actions are to be performed, when the

action is to issue a JP1 event or to execute a command.

- To perform the action when the status is Abnormal: `Abnormal`

- To perform the action when the status is Warning: `Warning`

- To perform the action when the status is Normal: `Normal`

If you want to specify multiple statuses for the actions, separate them with commas.

You can omit this item.

- `JP1 Event` label

  Defines whether to issue JP1 events or to execute commands as the actions defined for the `Command` label.

  - To issue JP1 events: `Y`

    In this case, you must define the details for issuing JP1 events in the Action `Definition JP1 Event` subsection.

  - To execute commands: `N`

    In this case, you must define the details for executing commands in the `Action Definition Command` subsection.

  `N` is the default value.

6. Define the destination and message text of the email.

   Define the destination and message text of the email to be sent.

   You can define the destination and message text of the email in the `Action Definition E-mail` subsection.

   If you define the action of sending an email, you cannot omit this subsection.

   The destination and message text of the email are defined in the following portion:

```
   :
#[[Action Definition E-mail]]
#E-mail Address=
#Action Handler=

#[[[Message Text]]]
#Date: %SCT
#Host: %HNS
#
#Product: %PTS
#Agent: %ANS
#
#Alarm: %AIS (%ATS)
```

```
#State: %SCS
#
#Message: %MTS
   :
```

For the following example, suppose we want to specify the email destination as `operatorA@aaa.com` and the message text with some variables. Delete the sharps (#) at the beginning of the appropriate lines, and edit those lines as follows:

```
   :
[[Action Definition E-mail]]
E-mail Address=operatorA@aaa.com
Action Handler=PH1host01
   :
[[[Message Text]]]
Date: %SCT
Host: %HNS

Product: %PTS
Agent: %ANS

Alarm: %AIS (%ATS)
State: %SCS

Message: %MTS
   :
```

- `E-mail Address` label

  Defines the destination of the email in 1 to 127 bytes of characters. If you want to specify multiple destinations, separate them with commas.

  You cannot omit this item.

- `Action Handler` label

  Defines the service ID of the Action Handler service to send the email from.

  You cannot omit this item.

- `Message Text` sub-subsection

  Defines the message text in 0 to 1,000 bytes.

  All characters including any linefeeds that appear before the line where the next section or subsection begins, or just before the end of the file, are considered valid text strings. As an exception, any comment lines in this sub-subsection are excluded. Also, the linefeed character in the last line is excluded.

  If this value is omitted, an empty string is assumed.

The variables used in the example above are defined as:

- Date and time when the alarm occurred

- Host name of the agent where the alarm occurred

- Agent type and version of the data model

- Name of the agent where the alarm occurred

- Alarm name

- Alarm table name

- Status of the alarm

- Free space (the value defined for the `Message Text` label in the `General` subsection)

For details on variables used in the definitions for the `Message Text` subsection, and their meanings, see the chapter explaining the Alarms window of PFM - Web Console in the manual *Job Management Partner 1/Performance Management Reference*.

7. Define the details for issuing the JP1 events.

   You can define the details for issuing the JP1 events in the `Action Definition JP1 Event` subsection.

   If you define the actions to issue JP1 events, you cannot omit this subsection.

   The details for issuing the JP1 events are defined in the following portion:

```
   :
#[[Action Definition JP1 Event]]
#Event ID=
#Message=%MTS
#Switch Alarm Level=Y
#Action Handler=
#Exec Logical Host=
   :
```

   Delete the sharps (#) at the beginning of the appropriate lines, and edit those lines as follows:

```
   :
[[Action Definition JP1 Event]]
Event ID=1234
Message=%MTS
Switch Alarm Level=Y
Action Handler=PH1host01
#Exec Logical Host=
   :
```

- `Event ID` label

  Defines the event ID of the JP1 event in hexadecimal. For a JP1 system event, the information set for this option is identified as an event ID (JPC_USER_EVENTID) with an extended JP1 event attribute when output. For a JP1 user event, it is identified as an event ID (JPC_USER_EVENTID) with a basic JP1 event attribute when output. For details on the JP1 event types, see *10.2 Considerations for linking with JP1/IM*.

  You cannot omit this item.

- `Message` label

  Defines the message to send with the JP1 event in 0 to 128 bytes.

  If a label contains a space, you must enclose the value with double quotation marks (").

  An empty string is used by default.

- `Switch Alarm Level` label

  Defines whether to convert the alarm level to the severity level.

  - To convert the alarm level to the severity level: `Y`

  - To not convert the alarm level to the severity level: `N`

  `Y` is the default.

- `Action Handler` label

  Defines the service ID of the Action Handler service to issue the JP1 event from.

  You cannot omit this item.

8. Define the alarm `Free Space (hda4)` in the same way.

   By following steps 3-7, define the alarm `Free Space (hda4)` that monitors the free space of the disk `/dev/hda4`.

   The completed alarm definition file is shown below:

```
Alarm Definition File Version=0001
Alarm Definition File Code=C

[Alarm Data]
[[General]]
Product=U4.0
Alarm Table Name=Disk Monitoring
Alarm Name=Free Space (hda3)
Message Text=Free Space (%CVS%)
Check Value Exist=N
```

```
#[[Advanced Setting]]
#Active Alarm=Y
#Regularly Alarm=Y
#Evaluate All Data=N
#Monitoring Regularly=N
#Monitoring Time=
#Damping=N
#Damping Count=

#[[Check Value Exist]]
#Record=
#Field=
#Value=

[[Alarm Condition Expressions]]
Condition=PD_FSL_FILESYSTEM_NAME="/dev/hda3","/dev/hda3"
AND PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20

[[Actions]]
#Report=
E-mail=Abnormal
Command=Abnormal,Warning
#SNMP=Abnormal,Warning,Normal
JP1 Event=Y

[[Action Definition E-mail]]
E-mail Address=operatorA@aaa.com
Action Handler=PH1host01

[[[Message Text]]]
Date: %SCT
Host: %HNS

Product: %PTS
Agent: %ANS

Alarm: %AIS (%ATS)
State: %SCS

Message: %MTS

#[[Action Definition Command]]
#Command Name=
#Action Handler=

#[[[Message Text]]]
#
```

```
[[Action Definition JP1 Event]]
Event ID=1234
Message=%MTS
Switch Alarm Level=Y
Action Handler=PH1host01
#Exec Logical Host=

[Alarm Data]
[[General]]
Product=U4.0
Alarm Table Name=Disk Monitoring
Alarm Name=Free Space (hda4)
Message Text=Free Space (%CVS%)
Check Value Exist=N

#[[Advanced Setting]]
#Active Alarm=Y
#Regularly Alarm=Y
#Evaluate All Data=N
#Monitoring Regularly=N
#Monitoring Time=
#Damping=N
#Damping Count=

#[[Check Value Exist]]
#Record=
#Field=
#Value=

[[Alarm Condition Expressions]]
Condition=PD_FSL_FILESYSTEM_NAME="/dev/hda4","/dev/hda4"
AND PD_FSL_TOTAL_MBYTES_FREE_PERCENT<10,20

[[Actions]]
#Report=
E-mail=Abnormal
Command=Abnormal,Warning
#SNMP=Abnormal,Warning,Normal
JP1 Event=Y

[[Action Definition E-mail]]
E-mail Address=operatorA@aaa.com
Action Handler=PH1host01

[[[Message Text]]]
Date: %SCT
Host: %HNS
```

```
Product: %PTS
Agent: %ANS

Alarm: %AIS (%ATS)
State: %SCS

Message: %MTS

#[[Action Definition Command]]
#Command Name=
#Action Handler=

#[[[Message Text]]]
#
[[Action Definition JP1 Event]]
Event ID=1234
Message=%MTS
Switch Alarm Level=Y
Action Handler=PH1host01
#Exec Logical Host=
```

9. When you have finished making the necessary changes, save the `/tmp/alarmtmp01.cfg` file.

For details on the items that are not specified in above example, see the description of the `jpctool alarm import` command in the manual *Job Management Partner 1/ Performance Management Reference*.

6.7.2 Checking the alarm definition file

Check the contents of the alarm definition file you created. You can use the `jpctool alarm check` command to check the alarm definition file.

In the following example, we check not only the syntax of the alarm definition file but also the details of the definition, such as whether PFM - Agent or PFM - RM defined in the file is set up, whether the record and field are supported, and so on.

To check the alarm definition file:

1. Verify that the Name Server, Master Manager, and View Server services are running.

   You can use the `jpctool service list` command to verify that the services of the Performance Management programs are running.

   For example, execute the following command when you want to list the services running on the host `host01`:

   ```
   jpctool service list -id "*" -host host01
   ```

When PFM - Manager is running on the host01, the output is as follows:

```
Host Name  ServiceID  Service Name    PID   Port  Status
---------  ---------  --------------  ----  ----  ------
host01     PC1host01  Trap Generator  1468  1134  Active
host01     PE1001     Correlator      1420  1114  Active
host01     PH1host01  Action Handler  872   1116  Active
host01     PM1001     Master Manager  1388  1104  Active
host01     PP1host01  View Server     1504  1155  Active
host01     PS1001     Master Store    632   1109  Active
host01     PN1001     Name Server     484   8204  Active
```

In this example, the Name Server, Master Manager, and View Server services are all running.

For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

2. Execute the `jpctool alarm check` command.

   Execute the command as follows:

   ```
   jpctool alarm check -f /tmp/alarmtmp01.cfg
   ```

   If any errors are found in the alarm definition file, an error message is generated for each error, indicating the detail of the error and the line number in the file.

   You must check the messages, and then resolve the errors.

   For further details on the `jpctool alarm check` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.7.3 Modifying an alarm definition

You can modify an alarm definition by exporting the alarm definition information to a file, editing the file, and then importing the file again.

In this procedure, use the following commands:

- To export the alarm definition:

  `jpctool alarm export` command

- To import the alarm definition:

  `jpctool alarm import` command

Note:

You cannot modify alarms that are defined in a monitoring template (the alarm tables that begin with PFM). If you want to edit them, you must first export the monitoring template, rename the alarm tables in the alarm definition file, and then import them.

To modify an existing alarm definition:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table whose definition you want to edit.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

   ```
   Product ID:U
   Alarm Table Name:
     alarmtable1
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

3. Execute the `jpctool alarm list` command to view the name of the alarm to edit the definition for.

   For example, execute the following command when you want to view the alarm names defined in the alarm table named `alarmtable1` of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX -table alarmtable1
   ```

   The output is shown below.

   ```
   Product ID:U
   DataModelVersion:4.0
   Alarm Table Name:alarmtable1
   Alarm Name:
     Kernel CPU 01       [active]
     Kernel CPU 02       [active]
     User CPU 01         [active]
   ```

```
The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

4. Execute the `jpctool alarm export` command.

   For example, execute the following command when you want to export the definition information for all alarms defined in the alarm table `alarmtable1` of PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm export -f /tmp/alarmtable1.cfg -key UNIX
   -table alarmtable1
   ```

   For further details on the `jpctool alarm export` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

5. Open the `/tmp/alarmtable1.cfg` file with a text editor or other tool.

6. Edit the `/tmp/alarmtable1.cfg` file.

   For details on how to edit individual definitions in the alarm definition file, see *6.7.1 Creating an alarm definition file*.

7. Save the `/tmp/alarmtable1.cfg` file.

8. Execute the `jpctool alarm import` command.

   For example, execute the following command when you want to import the definition information from the alarm definition file `/tmp/alarmtable1.cfg`:

   ```
   jpctool alarm import -f /tmp/alarmtable1.cfg
   ```

   For further details on the `jpctool alarm import` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

6.7.4 Copying an alarm table

To copy an alarm table, you can use the `jpctool alarm copy` command.

Notes:

- When you make a copy of an alarm table, the copy belongs to the same PFM - Agent or PFM - RM as the original. You cannot make a copy of an alarm table as an alarm table belonging to another PFM - Agent or PFM - RM.
- For the destination alarm table name, you cannot specify a name that begins with `PFM`.

To copy an alarm table:

1. Log on to a host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to copy.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that only the monitoring template is defined.

   ```
   Product ID:U
   Alarm Table Name:
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
3. Execute the `jpctool alarm copy` command.

   For example, execute the following command when you want to copy the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) as the alarm table named `alarmtable1`:

   ```
   jpctool alarm copy -key UNIX -table "PFM UNIX Solution Alarms
   7.00" -name alarmtable1
   ```

   For details on the `jpctool alarm copy` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
4. Execute the `jpctool alarm list` command to make sure that the alarm table has been copied.

Like in step 2, execute the command as follows:

```
jpctool alarm list -key UNIX
```

The output is shown below. In this example, you can see that the alarm table `alarmtable1` is newly created.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.7.5 Deleting an alarm table

To delete an alarm table, you can use the `jpctool alarm delete` command.

To delete an alarm table:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to delete.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

   ```
   Product ID:U
   Alarm Table Name:
     alarmtable1
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

3. Execute the `jpctool alarm delete` command.

   For example, execute the following command when you want to delete the alarm table `alarmtable1` of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm delete -key UNIX -table alarmtable1
   ```

   For further details on the `jpctool alarm delete` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm table has been deleted.

   Like in step 2, execute the command as follows:

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that the alarm table `alarmtable1` has been deleted.

   ```
   Product ID:U
   Alarm Table Name:
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.7.6 Deleting an alarm

To delete an individual alarm, you can use the `jpctool alarm delete` command.

To delete an individual alarm:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table containing the definition you want to delete.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

```
Product ID:U
Alarm Table Name:
  alarmtable1
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

3. Execute the `jpctool alarm list` command to view the name of the alarm to delete.

   For example, execute the following command when you want to view the alarm names defined in the alarm table named `alarmtable1` of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX -table alarmtable1
   ```

   The output is shown below. In this example, you can see that the alarms `Kernel CPU 01`, `Kernel CPU 02`, and `User CPU 01` are defined in the alarm table `alarmtable1`.

   ```
   Product ID:U
   DataModelVersion:4.0
   Alarm Table Name:alarmtable1
   Alarm Name:
     Kernel CPU 01        [active]
     Kernel CPU 02        [active]
     User CPU 01          [active]

   The Bound Agent:
     UA1hostA
     UA1hostB
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

4. Execute the `jpctool alarm delete` command.

   For example, execute the following command when you want to delete the alarm `Kernel CPU 02` in the alarm table `alarmtable1` of the PFM - Agent for

Platform (UNIX):

```
jpctool alarm delete -key UNIX -table alarmtable1 -alarm
"Kernel CPU 02"
```

For further details on the `jpctool alarm delete` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

5. Execute the `jpctool alarm list` command to make sure that the alarm has been deleted.

   Like in step 2, execute the command as follows:

   ```
   jpctool alarm list -key UNIX -table alarmtable1
   ```

   The output is shown below. In this example, you can see that the alarm table `Kernel CPU 02` has been deleted.

   ```
   Product ID:U
   DataModelVersion:4.0
   Alarm Table Name:alarmtable1
   Alarm Name:
     Kernel CPU 01       [active]
     User CPU 01         [active]

   The Bound Agent:
     UA1hostA
     UA1hostB
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.8 Operating alarms by using commands

This section explains how to operate alarms by using commands. Alternately, you can use the Quick Guide to set simplified alarms. For details on the Quick Guide, see *6.5 Setting alarms by using the Quick Guide*.

6.8.1 Associating an alarm table with a monitoring agent

To bind the alarm table to the monitoring agent, use the `jpctool alarm bind` command.

(1) When the functionality for binding multiple alarm tables is enabled

To bind multiple alarm tables when the functionality for binding multiple alarm tables is enabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to bind.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can confirm that a monitoring template and UNIX Alarm CPU are defined.

   ```
   Product ID:U
   Alarm Table Name:
     UNIX Alarm CPU
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
3. Execute the `jpctool alarm bind` command.

   For example, execute the following command when you want to bind the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) to the agent on `host01`:

   ```
   jpctool alarm bind -key UNIX -table "PFM UNIX Solution Alarms
   ```

```
7.00" -id UA1host01
```

Hint:

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the monitored object as the service ID.

4. Execute the `jpctool alarm bind` command with the `-add` option specified.

   For example, to add UNIX Alarm CPU to an agent on `host01`, execute the following command:

   ```
   jpctool alarm bind -key UNIX -table "UNIX Alarm CPU" -id
   UA1host01 -add
   ```

   You can bind up to 50 alarm tables at the same time.

   For further details on the `jpctool alarm bind` command, see the chapter that describes the commands in the *Job Management Partner 1/Performance Management Reference*.

5. Execute the `jpctool alarm list` command to make sure that the alarm table has been bound.

   Specify and execute the command as follows:

   ```
   jpctool alarm list -id UA1host01
   ```

   The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 and UNIX Alarm CPU are bound to an agent UA1host01.

   ```
   Service ID:UA1host01
   Bound Alarm Table Name:
     UNIX Alarm CPU
     PFM UNIX Solution Alarms 7.00
   ```

   For details of the `jpctool alarm list` command, see the chapter about commands in the *Job Management Partner 1/Performance Management Reference*.

(2) When the functionality for binding multiple alarm tables is disabled

Note

Each agent can only have one alarm table bound to it. If you bind an alarm table

to an agent already bound to another alarm table, the existing alarm table is unbound automatically and the new alarm table is bound.

To bind an alarm table when the functionality for binding multiple alarm tables is disabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to bind.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that only the monitoring template is defined.

   ```
   Product ID:U
   Alarm Table Name:
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   For details on the `jpctool alarm list` command, see the chapter that describes the commands in the manual *Job Management Partner 1/Performance Management Reference*.
3. Execute the `jpctool alarm list` command to determine which agent the alarm table to bind is bound to.

   For example, execute the following command when you want to determine which agent the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) is bound to:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

Hint:

To view a report on an object monitored by PFM - RM, select the appropriate remote or group agent for the monitored object as the service ID.

The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to the hosts `hostA` and `hostB`.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time    [active]
  I/O Wait Time        [active]
  Kernel CPU           [active]
  Pagescans            [active]
  Run Queue            [active]
  Swap Outs            [active]
  User CPU             [active]

The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

4. Execute the `jpctool alarm bind` command.

   For example, execute the following command when you want to bind the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) to the agent on `host01`:

   ```
   jpctool alarm bind -key UNIX -table "PFM UNIX Solution Alarms
   7.00" -id UA1host01
   ```

   For further details on the `jpctool alarm bind` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

5. Execute the `jpctool alarm list` command to make sure that the alarm table has been bound.

   Like in step 3, execute the command as follows:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to the hosts `host01`, `hostA`, and `hostB`.

```
Product ID:U
DataModelVersion:3.0
Alarm Table Name:PFM UNIX Solution Alarms 7.00
Alarm Name:
  Disk Service Time   [active]
  I/O Wait Time       [active]
  Kernel CPU          [active]
  Pagescans           [active]
  Run Queue           [active]
  Swap Outs           [active]
  User CPU            [active]

The Bound Agent:
  UA1host01
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.8.2 Unbinding an alarm table bound to a monitoring agent

To unbind an alarm table, use the `jpctool alarm unbind` command.

(1) When the functionality for binding multiple alarm tables is enabled

To unbind an alarm table when the functionality for binding multiple alarm tables is enabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to make sure that the alarm table has been bound.

   Specify and execute the command as follows:

   ```
   jpctool alarm list -id UA1host01
   ```

   The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 and UNIX Alarm CPU are bound to an agent UA1host01.

   ```
   Service ID:UA1host01
   Bound Alarm Table Name:
     UNIX Alarm CPU
     PFM UNIX Solution Alarms 7.00
   ```

For details of the `jpctool alarm list` command, see the chapter that describes the commands in the *Job Management Partner 1/Performance Management Reference*.

3. Execute the `jpctool alarm unbind` command.

   For example, to unbind all the alarm tables bound to the agent UA1host01, execute the following command:

   ```
   jpctool alarm unbind -key UNIX -all -id UA1host01
   ```

   For details of the `jpctool alarm unbind` command, see the chapter that describes the commands in the manual *Job Management Partner 1/Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm table has been unbound.

   Like in step 2, execute the command as follows:

   ```
   jpctool alarm list -id UA1host01
   ```

   The output is shown below. In this example, you can confirm that no alarm table is bound to the agent UA1host01.

   ```
   Service ID:UA1host01
   Bound Alarm Table Name:
   ```

   For details of the `jpctool alarm list` command, see the chapter that describes the commands in the *Job Management Partner 1/Performance Management Reference*.

(2) When the functionality for binding multiple alarm tables is disabled

To unbind an alarm table when the functionality for binding multiple alarm tables is disabled:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table to unbind.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

The output is shown below. In this example, you can see that only the monitoring template is defined.

```
Product ID:U
Alarm Table Name:
  PFM UNIX Solution Alarms 6.70
  PFM UNIX Solution Alarms 7.00
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

3. Execute the `jpctool alarm list` command to determine which agent the alarm table to unbind is bound to.

   For example, execute the following command when you want to determine which agent the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) is bound to:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to the hosts `host01`, `hostA`, and `hostB`.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time    [active]
     I/O Wait Time        [active]
     Kernel CPU           [active]
     Pagescans            [active]
     Run Queue            [active]
     Swap Outs            [active]
     User CPU             [active]

   The Bound Agent:
     UA1host01
     UA1hostA
     UA1hostB
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance*

Management Reference.

4. Execute the `jpctool alarm unbind` command.

   For example, execute the following command when you want to unbind all the hosts whose name begins with `host` in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm unbind -key UNIX -table "PFM UNIX Solution
   Alarms 7.00" -id "UA1host*"
   ```

   For further details on the `jpctool alarm unbind` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

5. Execute the `jpctool alarm list` command to make sure that the alarm table has been unbound.

   Like in step 3, execute the command as follows:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. In this example, you can see that the monitoring template PFM UNIX Solution Alarms 7.00 is bound to no host.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time    [active]
     I/O Wait Time        [active]
     Kernel CPU           [active]
     Pagescans            [active]
     Run Queue            [active]
     Swap Outs            [active]
     User CPU             [active]

   The Bound Agent:
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.8.3 Checking the connection between an alarm table and a monitoring agent

To check whether an alarm table is bound, you can use the `jpctool alarm list` command.

To check whether of an alarm table is bound:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name of the alarm table whose binding you want to check.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that only the monitoring template is defined.

   ```
   Product ID:U
   Alarm Table Name:
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
3. Execute the `jpctool alarm list` command to determine which agent the alarm table is bound to.

   For example, execute the following command when you want to determine which agent the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX) is bound to:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. In this example, you can see that the monitoring template is bound to the agents on the `host01`, `hostA`, and `hostB`.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   ```

```
Alarm Name:
  Disk Service Time    [active]
  I/O Wait Time        [active]
  Kernel CPU           [active]
  Pagescans            [active]
  Run Queue            [active]
  Swap Outs            [active]
  User CPU             [active]

The Bound Agent:
  UA1host01
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.8.4 Starting monitoring with an alarm

You can use the `jpctool alarm active` command to enable an alarm.

To enable an alarm:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command to view the name and the status of the alarm to enable.

   For example, execute the following command when you want to view the status of each alarm in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. The output displays `active` at the right of the alarm name for enabled alarms, and `inactive` for disabled alarms. In this example, you can see that the alarm `Disk Service Time` is disabled.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time    [inactive]
     I/O Wait Time        [active]
     Kernel CPU           [active]
   ```

```
  Pagescans           [active]
  Run Queue           [active]
  Swap Outs           [active]
  User CPU            [active]

The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

3. Execute the `jpctool alarm active` command.

   For example, execute the following command when you want to enable the alarm Disk Service Time in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm active -key UNIX -table "PFM UNIX Solution
   Alarms 7.00" -alarm "Disk Service Time"
   ```

   For further details on the `jpctool alarm active` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm has been enabled.

   Like in step 2, execute the command as follows:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. In this example, you can see that the alarm Disk Service Time is now enabled.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time   [active]
     I/O Wait Time       [active]
     Kernel CPU          [active]
     Pagescans           [active]
     Run Queue           [active]
   ```

```
  Swap Outs            [active]
  User CPU             [active]

The Bound Agent:
  UA1hostA
  UA1hostB
```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.8.5 Stopping monitoring with an alarm

You can use the `jpctool alarm inactive` command to disable an alarm.

To disable an alarm:

1. Log on to the host where PFM - Manager is installed.
2. Execute `jpctool alarm list` command to view the name and the status of the alarm to disable.

   For example, execute the following command when you want to view the status of each alarm in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. Displays `active` at the right of the alarm name for enabled alarms. In this example, you can see that all the alarms are enabled.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time    [active]
     I/O Wait Time        [active]
     Kernel CPU           [active]
     Pagescans            [active]
     Run Queue            [active]
     Swap Outs            [active]
     User CPU             [active]

   The Bound Agent:
     UA1hostA
     UA1hostB
   ```

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

3. Execute the `jpctool alarm inactive` command.

   For example, execute the following command when you want to disable the alarm Disk Service Time in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm inactive -key UNIX -table "PFM UNIX Solution
   Alarms 7.00" -alarm "Disk Service Time"
   ```

   For further details on the `jpctool alarm inactive` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

4. Execute the `jpctool alarm list` command to make sure that the alarm has been disabled.

   Like in step 2, execute the command as follows:

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. Displays `inactive` at the right of the alarm name for disabled alarms. In this example, you can see that the alarm `Disk Service Time` is now disabled.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time    [inactive]
     I/O Wait Time        [active]
     Kernel CPU           [active]
     Pagescans            [active]
     Run Queue            [active]
     Swap Outs            [active]
     User CPU             [active]

   The Bound Agent:
     UA1hostA
     UA1hostB
   ```

   For further details on the `jpctool alarm list` command, see the chapter that

describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.8.6 Checking the properties of an alarm table

You can display a list of the alarm tables defined for a specific PFM - Agent or PFM - RM, or a list of defined alarms and a list of the agents bound for a specific alarm table.

This section explains how to view the definition information of alarm tables.

Note:

You cannot view the definition information of an individual alarm, such as the alarm threshold. To view the definition information of an alarm, you must use `jpctool alarm export` command to export the alarm definition to be checked. For details on how to export alarm definitions, see *6.7.3 Modifying an alarm definition*.

(1) Displaying a list of alarm tables

To list the alarm tables defined for a specific PFM - Agent or PFM - RM, you can use the `jpctool alarm list` command.

To display the list of the alarm tables:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command.

   For example, execute the following command when you want to view the alarm table names defined in the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX
   ```

   The output is shown below. In this example, you can see that the monitoring template and the alarm table `alarmtable1` are defined.

   ```
   Product ID:U
   Alarm Table Name:
     alarmtable1
     PFM UNIX Solution Alarms 6.70
     PFM UNIX Solution Alarms 7.00
   ```

   The following table describes the information displayed by executing the `jpctool alarm list` command with only the `-key` option specified.

Table 6-2: Information displayed by the `jpctool alarm list` command (-key option specified)

Order	Information	Description
1	`Product ID`	The product ID indicating the PFM - Agent or PFM - RM type. For details on the product ID for each PFM - Agent or PFM - RM, see the ID list in an appendix of each PFM - Agent or PFM - RM manual.
2	`Alarm Table Name`	The alarm table name.

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

(2) Viewing the information for the alarms in an alarm table

To list the alarms defined in and the agents bound to a specific alarm table, you can use the `jpctool alarm list` command.

To display the information of an alarm:

1. Log on to the host where PFM - Manager is installed.
2. Execute the `jpctool alarm list` command.

   For example, execute the following command when you want to view the information for the alarms defined in the monitoring template PFM UNIX Solution Alarms 7.00 of the PFM - Agent for Platform (UNIX):

   ```
   jpctool alarm list -key UNIX -table "PFM UNIX Solution Alarms
   7.00"
   ```

   The output is shown below. In this example, you can see that all the alarms in the monitoring template are enabled, and that the monitoring template is bound to the hosts `hostA` and `hostB`.

   ```
   Product ID:U
   DataModelVersion:3.0
   Alarm Table Name:PFM UNIX Solution Alarms 7.00
   Alarm Name:
     Disk Service Time    [active]
     I/O Wait Time        [active]
     Kernel CPU           [active]
     Pagescans            [active]
     Run Queue            [active]
     Swap Outs            [active]
   ```

```
  User CPU              [active]

The Bound Agent:
  UA1hostA
  UA1hostB
```

The following table describes the information displayed by executing the `jpctool alarm list` command with the `-key` and `-table` options specified.

Table 6-3: Information displayed by the `jpctool alarm list` command (-key and -table options specified)

Order	Information	Description
1	`Product ID`	The product ID indicating the PFM - Agent or PFM - RM type. For details on the product ID for each PFM - Agent or PFM - RM, see the ID list in an appendix of each PFM - Agent or PFM - RM manual.
2	`Data Model Version`	The version of the data model.
3	`Alarm Table Name`	The alarm table name.
4	`Alarm Name`	Indicates whether the alarm name is valid and the alarm is enabled. • `active`: the alarm is enabled. • `inactive`: the alarm is disabled.
5	`The Bound Agent`	Indicates the service ID of the agent for the alarm table to be bound to.

For further details on the `jpctool alarm list` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

6.9 Notes on alarms

This section contains cautionary notes on alarms.

6.9.1 Notes on creating alarms

(1) Time for evaluating the alarm

If monitoring conditions of multiple records are set for an alarm and the monitoring intervals and offsets of the records are different, the alarm is only evaluated when their collection schedules match. You must review the collection interval setting if necessary.

(2) Saving of records to be evaluated in the alarm

You do not have to save the records that you selected for the alarm conditions in the Store database.

(3) Limitation on the number of alarms

You can register up to 50 alarms in one alarm table. In addition, you can bind up to 50 alarm tables to one agent.

Binding a large number of alarms to PFM - Agent or PFM - RM in the Performance Management system, might delay the processing of PFM - Manager, PFM - Agent, or PFM - RM.

We recommend that you limit the number of bound alarms to the following:

- 250 alarms per agent.
- 10,000 alarms across the entire Performance Management system.

(4) When you set an alarm to monitor whether a value exists

If you have selected **Monitor whether the value exists**, the value specified in the conditional expression does not exist when the alarm is reported. In such a case, note that any variables specified in message text or in `Mail Subject` are replaced by an empty string.

(5) How the number of alarm occurrences affects the PFM - Agent or PFM - RM connection

In Performance Management, the PFM - Manager receives the alarms issued by PFM - Agent or PFM - RM, and handles them sequentially, for example, by storing them in the Store database (Master Store). When alarms occur more frequently or are issued by many PFM - Agents or PFM - RMs at the same time, the processing of PFM - Manager might be delayed. In such a case, unhandled alarms are accumulated in the memory of the PFM - Manager host, which might cause the memory usage to increase or the system performance to degrade.

We therefore recommend that you consider how frequently an alarm will occur when you define it, to avoid exceeding the maximum number of alarm occurrences that PFM - Manager can handle in a particular unit of time. We also recommend that you determine the number of PFM - Agent or PFM RM instances to be connected to PFM - Manager, beforehand. For details on the relationship between the alarm damping and the number of PFM - Agent or PFM - RM instances to be connected to PFM - Manager, see the sections that describe the system configuration in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(6) How the number of alarm occurrences affects the system resources

If a large number of alarms for which an action is specified are issued at the same time, when the actions are executed, the system might become unstable due to a large consumption of system resources.

6.9.2 Relationship between the alarm damping and alarm event issues

This section describes the relationship between the alarm damping settings and how alarm events are issued, using an example.

Reference note:

The cases in this example assume that a multi-instance record is used to create an alarm. A multi-instance record is a record consisting of multiple instances collected at the same time. For example, assume a multi-instance record that checks the status of disk A and disk B. During alarm evaluation, the status of the disks is evaluated for alarms, and if either (or both) of the disks meets an alarm condition, an alarm is issued for each disk.

- (1)(c) When the alarm damping is n/n (n=n) (**Always** is cleared and **All** is selected)
- (1)(d) When the alarm damping is n/n (n=n) (**Always** is selected and **All** is selected)
- (2)(c) When the alarm damping is n/m (n<m) (**Always** is cleared and **All** is selected)
- (2)(d) When the alarm damping is n/m (n<m) (**Always** is selected and **All** is selected)

(1) When the alarm damping is n/n (n=n)

The following combinations of **Always notify** and **Evaluate all data** check box settings are assumed. These settings can be found in the New Alarm > Main Information window or in **Advanced settings** in the Edit > Main Information window.

Evaluate all data	Always notify	
	Cleared	Selected
Cleared	*(a)*	*(b)*
Selected	*(c)*	*(d)*

In the cases described below, the check box names are referred to as follows:

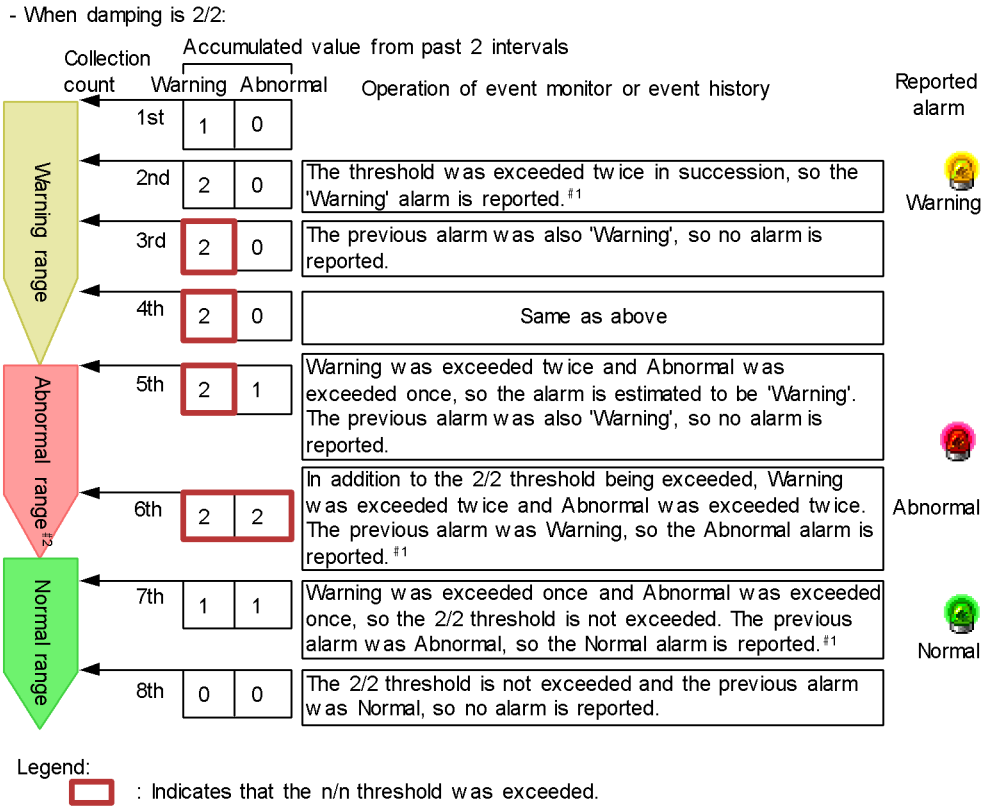
- **Always**: Indicates the **Always notify** check box.
- **All**: Indicates the **Evaluate all data** check box.

(a) When the alarm damping is n/n (n=n) (Always is cleared and All is cleared)

If **Always** is cleared and **All** is cleared, the following occurs:

- This case specifies when a change in the status of the alarm is to be triggered. This is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- Among the instances that were collected at the time of reporting the alarm, the alarm status of the instance that indicates the highest severity is reported.

This functionality is illustrated by the following examples:



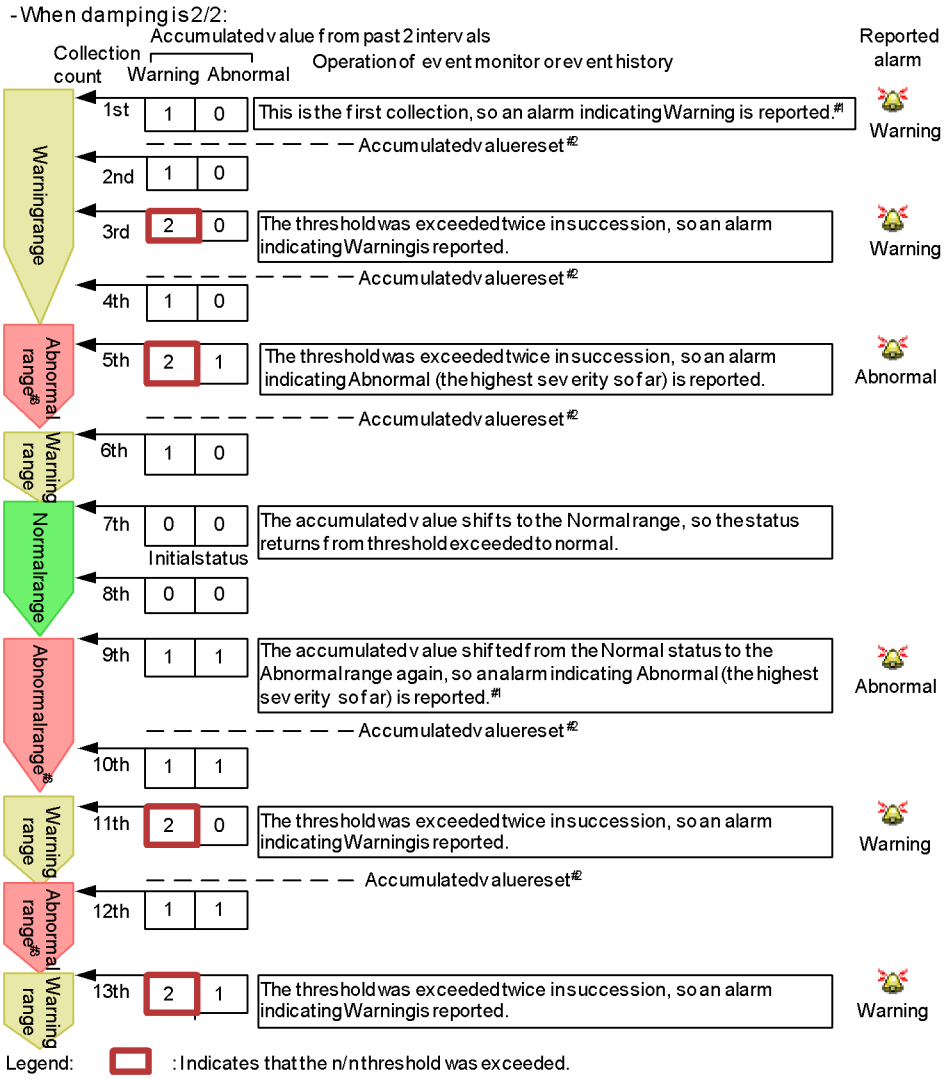
#1: 'Always' was not checked, so the accumulated value is not reset.
#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

(b) When the alarm damping is n/n (n=n) (Always is selected and All is cleared)

If **Always** is selected and **All** is cleared, the following occurs:

- This case specifies when the alarm is to be reported. This is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations. You can use this to control the frequency of the alarm.
- The instance that indicates the highest severity at the time of reporting the alarm is reported.

This functionality is illustrated by the following examples:



Legend: : Indicates that the n/n threshold was exceeded.

#1: If Always was checked and alarm damping is n/n (n = n), an initial alarm is reported when the following conditions are met:

- At the first collection
- When the accumulated value has shifted from Warning or Abnormal to Normal, and then has again shifted to Warning or Abnormal

#2: Always was checked, so the accumulated value is reset when an alarm is reported.

#3: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

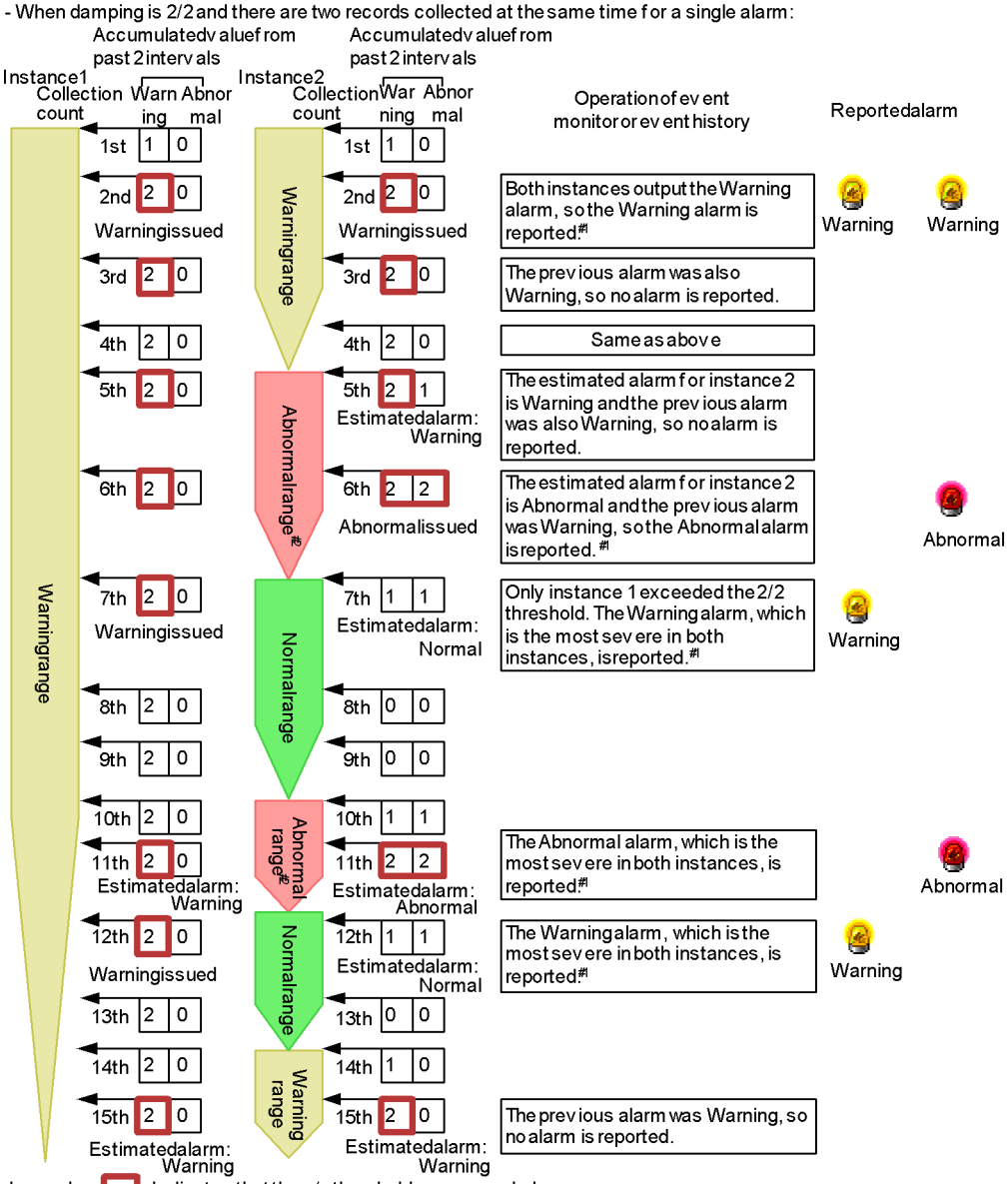
(c) When the alarm damping is n/n (n=n) (Always is cleared and All is selected)

If **Always** is cleared and **All** is selected, the following occurs:

- This case specifies when the status of the alarm changes. The status change is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- If the status is Warning or Abnormal, the alarm statuses of all the instances that meet the status condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:

- When damping is 2/2 and there are two records collected at the same time for a single alarm:



Legend: : Indicates that the n/n threshold was exceeded.

#1: Always was not checked, so the accumulated value is not reset.

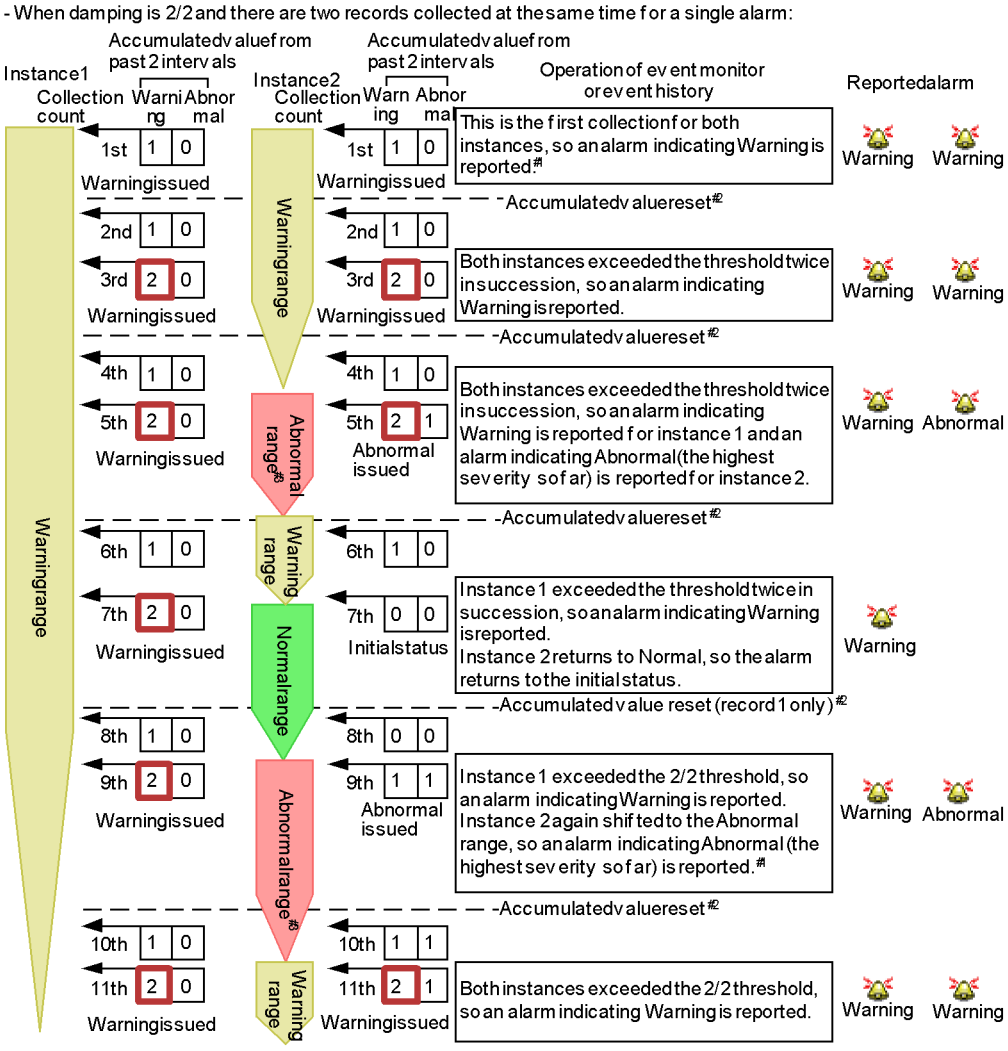
#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

(d) When the alarm damping is n/n (n=n) (Always is selected and All is selected)

If **Always** is selected and **All** is selected, the following occurs:

- This case specifies when the alarm is to be reported. This is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations. You can use this to control the frequency of the alarm.
- All of the instances that meet the Warning or Abnormal condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:



Legend: : Indicates that the n/n threshold was exceeded.

#1: If Always was checked and alarm damping is n/n (n = n), an initial alarm is reported when the following conditions are met:

- At the first collection
- When the accumulated value has shifted from Warning or Abnormal to Normal, and then has again shifted to Warning or Abnormal

#2: Always was checked, so the accumulated value is reset when an alarm is reported.

#3: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

(2) When the alarm damping is n/m (n<m)

The following combinations of **Always notify** and **Evaluate all data** check box

settings are assumed. These settings are available in the New Alarm > Basic Information window or in **Advanced settings** in the Edit > Basic Information window.

Evaluate all data	Always notify	
	Cleared	Selected
Cleared	*(a)*	*(b)*
Selected	*(c)*	*(d)*

In the cases described below, the check box names are referred to as follows:

- **Always**: Indicates the **Always notify** check box.
- **All**: Indicates the **Evaluate all data** check box.

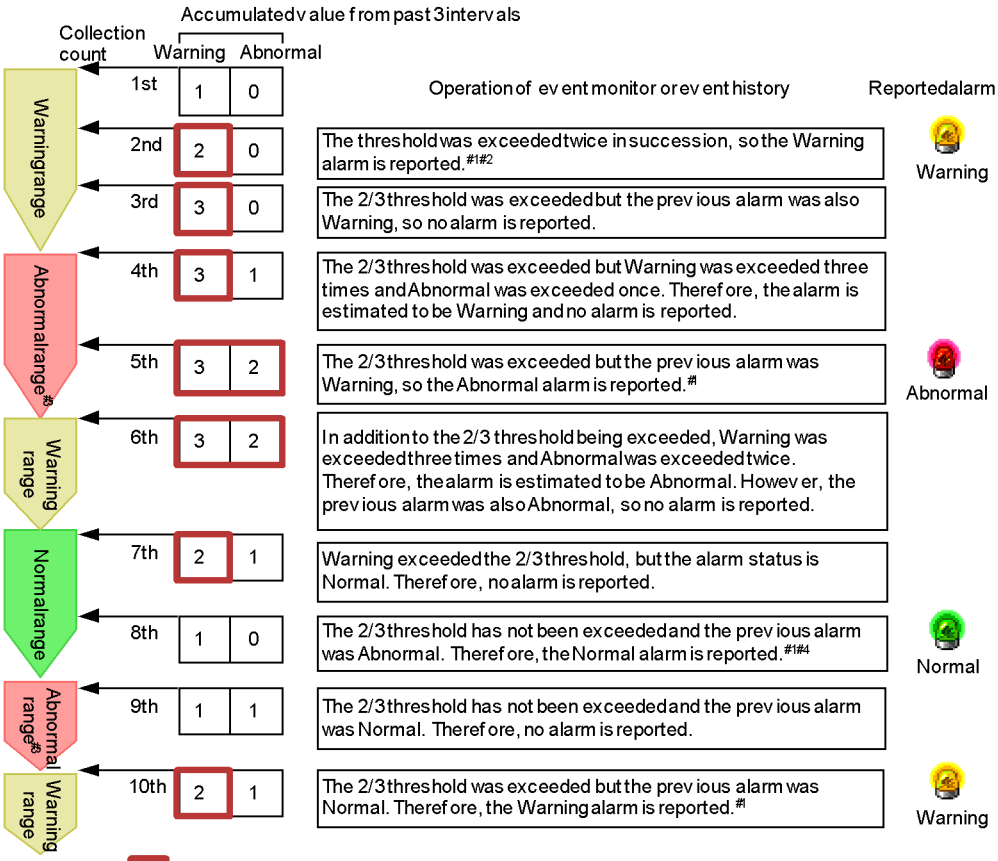
(a) When the alarm damping is n/m (n<m) (Always is cleared and All is cleared)

If **Always** is cleared and **All** is cleared, the following occurs:

- This case specifies when the status of the alarm changes. The status change is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- Among the instances that were collected at the time of reporting the alarm, the alarm status of the instance that indicates the highest severity is reported.

This functionality is illustrated by the following examples:

- When damping is 2/3:



Legend: : Indicates that the n/m threshold was exceeded.

#1: Always was not checked, so the accumulated value is not reset.
#2: Although alarm damping is 2/3, the Warning alarm is reported when the threshold is exceeded twice in succession.
#3: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.
#4: The following explains patterns of operation of the alarm at the 8th collection that differ from the example given above.

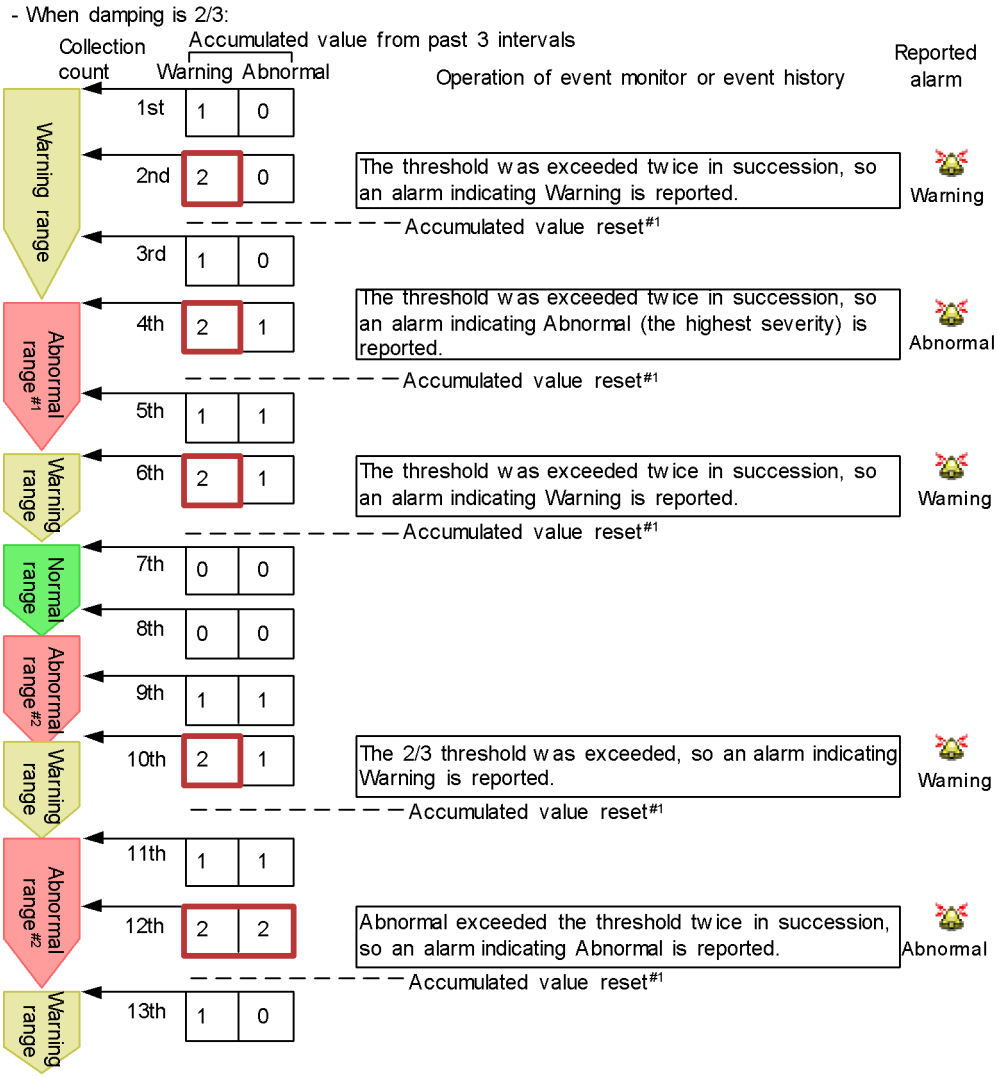
- When the 8th collection is in the Warning range or Abnormal range:
  In the past three intervals, Warning was exceeded twice and Abnormal was not exceeded (or exceeded once for the Abnormal range). Therefore, Warning exceeds the 2/3 threshold.
  Furthermore, the previous alarm was Abnormal, so the Warning alarm is reported.
  Always was not checked, so the accumulated value is not reset.
- When the 6th collection is in the Abnormal range, the 7th collection is in the Normal range, and the 8th collection is in the Abnormal range:
  In the past three intervals for the 8th collection, Warning was exceeded twice and Abnormal was exceeded twice. Therefore, Abnormal exceeds the 2/3 threshold.
  However, the previous alarm was Abnormal, so no alarm is reported.

(b) When the alarm damping is n/m (n<m) (Always is selected and All is cleared)

If **Always** is selected and **All** is cleared, the following occurs:

- This case specifies when the alarm is to be reported. This is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations. You can use this to control the frequency of the alarm.
- The instance that indicates the highest severity at the time of reporting the alarm is reported.

This functionality is illustrated by the following examples:



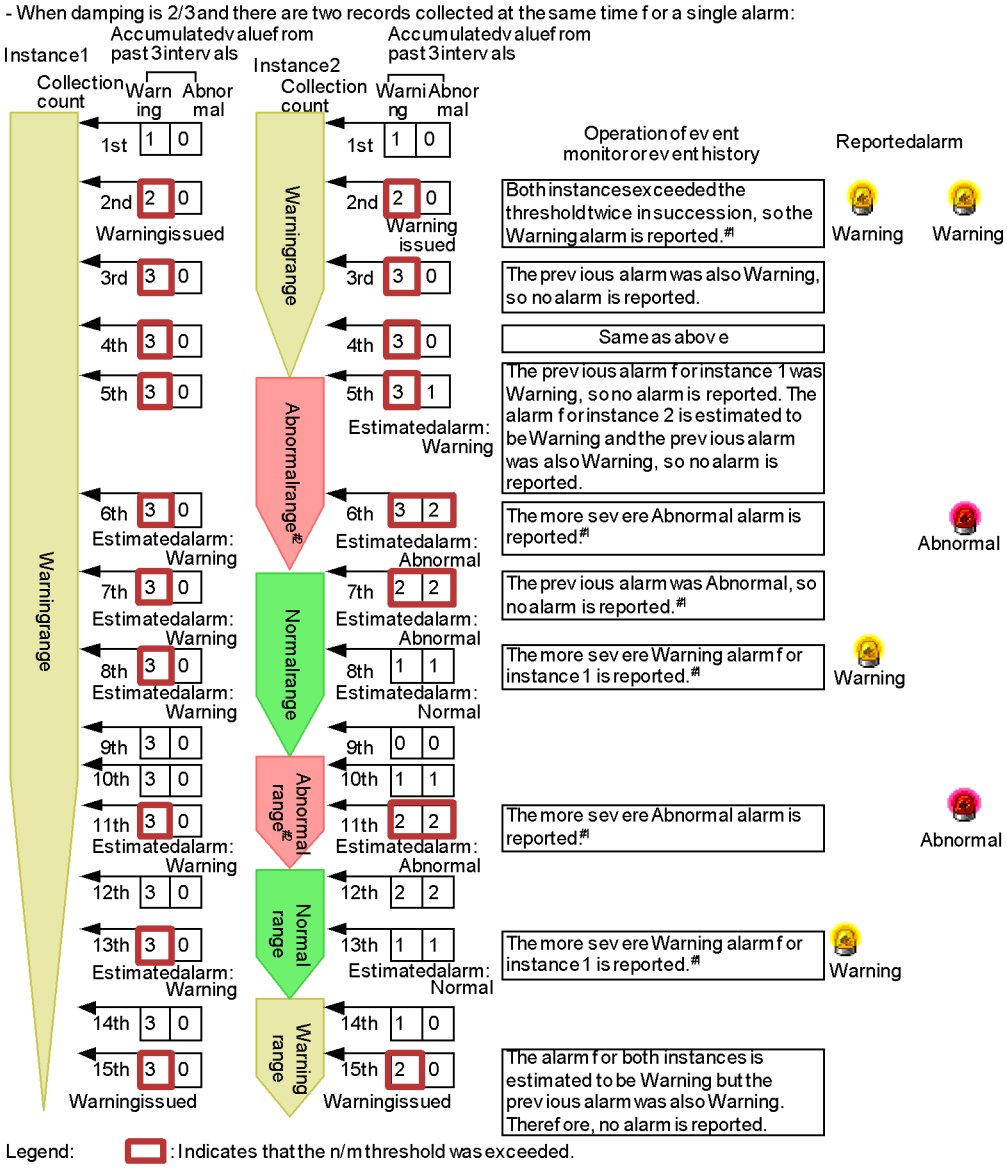
#1: Always was checked, so the accumulated value is reset when an alarm is reported.
#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

(c) When the alarm damping is n/m (n<m) (Always is cleared and All is selected)

If **Always** is cleared and **All** is selected, the following occurs:

- This case specifies when the status of the alarm changes. The status change is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations.
- The alarm is reported only when the status of the alarm changes from the previously reported status.
- If the status is Warning or Abnormal, the alarm statuses of all the instances that meet the status condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:



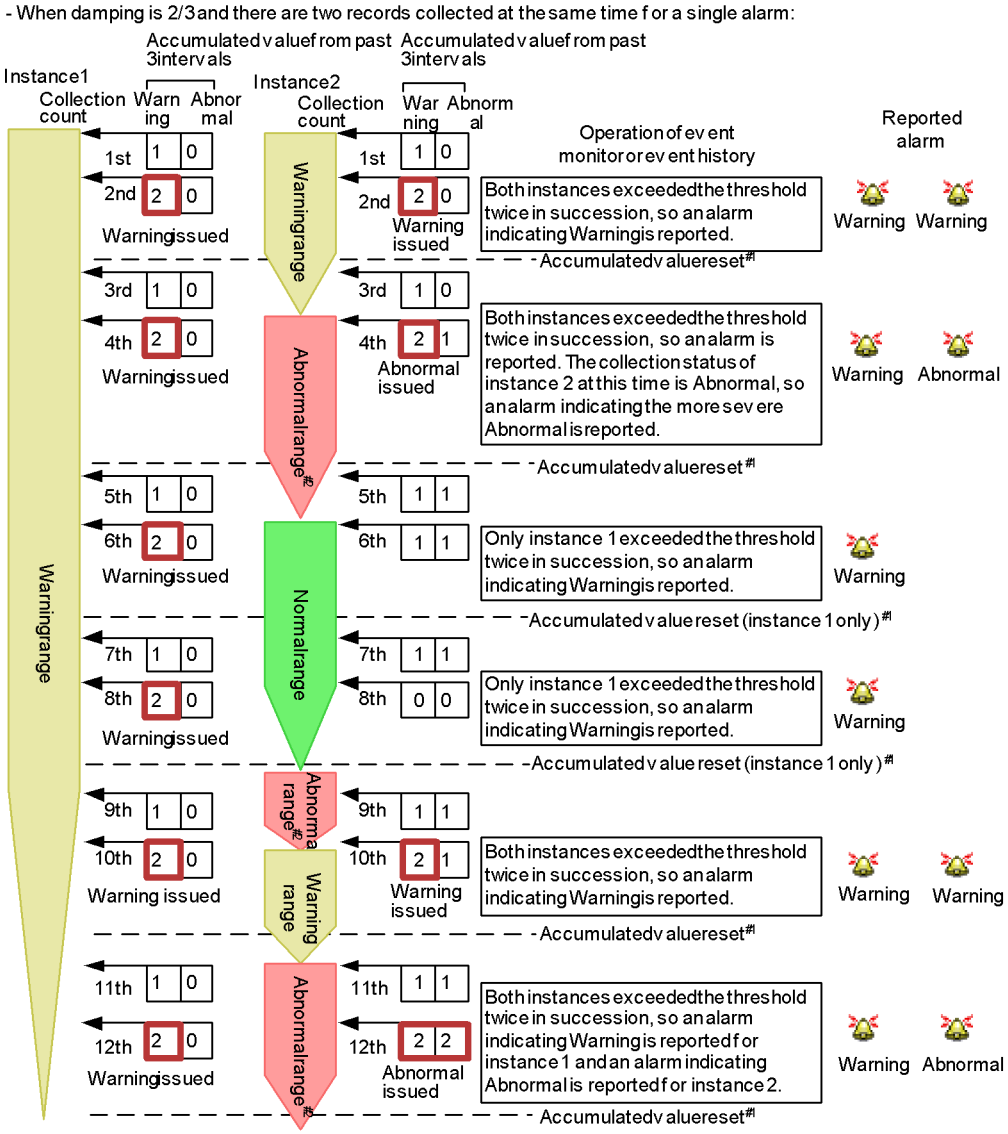
#1: Always was not checked, so the accumulated value is not reset.
#2: In the abnormal range, the conditions for the warning range are also met. The accumulated value therefore continues to be counted in Warning.

(d) When the alarm damping is n/m (n<m) (Always is selected and All is selected)

If **Always** is selected and **All** is selected, the following occurs:

- This case specifies when the alarm is to be reported. This is defined by specifying the number of times a threshold is exceeded for a specified number of evaluations. You can use this to control the frequency of the alarm.
- All of the instances that meet the Warning or Abnormal condition at the time of reporting the alarm are reported.

This functionality is illustrated by the following examples:



6.9.3 Notes on evaluating alarms

- Limitation on the number of instances evaluated in an alarm

If multi-instance records are collected in PFM - Agent or PFM - RM, the maximum number of instances handled by a collection is 32,767. When alarms are bound to PFM - Agent or PFM - RM, up to 32,767 instances are evaluated. More than 32,767 instances cannot be evaluated.

- Interval for evaluating the alarm

  An alarm is evaluated at fixed intervals. The interval is the record collection interval for each agent. For details on the collection interval of each record, see the appropriate chapters (the Collection Interval value of each record) that describe records of each PFM - Agent or PFM - RM manual.

  To modify the record collection interval, perform the following procedure:

  1. From the browser of the monitoring console, log on to PFM - Web Console.
  2. In the tab frame of the main window, select the **Services** tab.
  3. Select the monitoring agent that the alarm is bound to.
  4. In the method frame, select **Properties**.
  5. Expand the `Detail Records` or `Interval Records` folder.
  6. Change the value of the **Collection Interval** property.
  7. The record (performance data) collection interval changes to the value you set.

- Alarm condition-dependent alarm evaluation

  Details of an alarm evaluation depend on the alarm conditions and the type of record to be evaluated. The following table describes the differences among alarm evaluations for various combinations of alarm conditions.

  Table 6-4: Differences among alarm evaluations for various alarm conditions

Conditional expression	Record type	Always	All	Alarm evaluation (notification)
When **Monitor whether the value exists** is not selected	Single-row record[#1]	N	N	• If the Abnormal condition is met, and the previously reported alarm was other than Abnormal (red), the Abnormal (red) alarm is reported. • If the Abnormal condition is not met but the Warning condition is met, and the previously reported alarm was other than Warning (yellow), the Warning (yellow) alarm is reported. • If neither of the above cases is met, and the previously reported alarm was Abnormal (red) or Warning (yellow), the Normal (green) alarm is reported.
		N	Y	

Conditional expression	Record type	Always	All	Alarm evaluation (notification)
		Y	N	If either the Abnormal or Warning condition is met, the Abnormal or Warning alarm is reported, regardless of any previously reported alarm.
		Y	Y	
	Multi-row record[#2]	N	N	• If one instance is found that meets the Abnormal condition, and the previously reported alarm was other than Abnormal (red), the Abnormal (red) alarm is reported for that instance. • If no instance is found that meets the Abnormal condition, one instance is found that meets the Warning condition, and the previously reported alarm was other than Warning (yellow), the Warning (yellow) alarm is reported for that instance. • If none of the collected instances match the cases above, and the previously reported alarm was Abnormal (red) or Warning (yellow), the Normal (green) alarm is reported. Note: As soon as any instance is found that meets the condition, the alarm evaluation is ended. Therefore, all of the collected instances are not always evaluated.

Conditional expression	Record type	Always	All	Alarm evaluation (notification)
		N	Y	• If, after all of the collected instances are evaluated, one or more instances are found that meet the Abnormal condition, and the previously reported alarm was other than Abnormal (red), the Abnormal (red) alarm is reported for each of those instances. • If, after all of the collected instances are evaluated, no instance is found that meets the Abnormal condition, one or more instances are found that meet the Warning condition, and the previously reported alarm was other than Warning (yellow), the Warning (yellow) alarm is reported for each of those instances. • If none of the collected instances match the cases above, and the previously reported alarm was Abnormal (red) or Warning (yellow), the Normal (green) alarm is reported. Note: Because all of the instances are evaluated, more than one alarm can be reported in one interval.
		Y	N	• As soon as one instance is found that meets the Abnormal condition, the Abnormal alarm is reported based on that instance, regardless of any previously reported alarm. • As soon as one instance is found that meets the Warning condition but no instance has been found that meets the Abnormal condition yet, the Warning alarm is reported based on that instance, regardless of any previously reported alarm. Note: As soon as any instance is found that meets the condition, the alarm evaluation is ended. Therefore, all of the collected instances are not always evaluated.
		Y	Y	For each instance that meets either the Abnormal or Warning condition, the Abnormal or Warning alarm is reported. Note: Because all of the instances are evaluated, more than one alarm might be reported in one interval.

Conditional expression	Record type	Always	All	Alarm evaluation (notification)
When **Monitor whether the value exists** is selected	Multi-row record[#2]	N	N	All of the collected instances are checked for the value specified in **Alarm Wizard - The value whose existence is to be monitored**, and if no such value is found (the condition is not met), the Abnormal (red) alarm is reported.
		N	Y	Note: The alarm notifying no operation is reported only once. If no instance is collected, the alarm is not evaluated.
		Y	N	All of the collected instances are checked for the value specified in **Alarm Wizard - The value whose existence is to be monitored**, and if no such value is found (the condition is not met), the Abnormal (red) alarm is reported.
		Y	Y	Note: The alarm is reported every time. If no instance is collected, the alarm is not evaluated.

Legend:

Always: Whether **Always notify** is selected

All: Whether **Evaluate all data** is selected

Y: Used (selected)

N: Not used (not selected)

#1

Single-row record refers to a single-instance record.

#2

Multi-row record refers to a multi-instance record.

The alarm evaluation method is explained for various alarm conditions below.

When you set a value whose existence is to be monitored:

When you set a value whose existence is to be monitored, all fields in the specified record of PD and PI record types are evaluated to check for the specified value. If the value is not found, the alarm is reported once per interval.

When you set alarm conditions:

When you set alarm conditions, multiple records are collected in one interval for the record of PD and PI record types to be evaluated in this alarm. By default, as soon as the first instance is found that meets the conditional expression, the alarm is reported and the evaluation is ended. Therefore, all the performance data is not always evaluated. To evaluate the performance data of the PD record type in an alarm, select **Evaluate all data** in the **Advanced settings** tab of **Alarm Wizard - Main Information**.

- How alarms are evaluated differently when Damping is enabled

  In addition to the differences among alarm evaluations for various alarm conditions, if you set **Damping**, other differences are added to the alarm evaluation. The following table describes the differences among alarm evaluations for various alarm conditions with damping.

  Table 6-5: Differences among alarm evaluations with damping

Damping	Always	All	Alarm evaluation (notification)
Y	N	N	• The alarm is reported only when the status of the alarm changes from the previously reported status. • Based on the instance that indicates the highest severity at the time of reporting, the status of the alarm is reported. Note: Because the status of the alarm is determined by evaluating the damping condition, the status of the alarm might differ from the threshold of the reported instance.
Y	N	Y	• The alarm is reported only when the status of the alarm changes from the previously reported status. • If the status is Warning or Abnormal, the status of the alarm is reported based on all of the instances that meet the status condition at the time of reporting the alarm. Note: Because the status of the alarm is determined by evaluating the damping condition, the status of the alarm might differ from the threshold of the reported instance.
Y	Y	N	The instance that indicates the highest severity at the time of reporting the alarm is reported.
Y	Y	Y	• From the records that were collected at the same time, the instance that indicates the highest severity at the time of reporting the alarm for each record is reported.

Legend:

Always: Whether **Always notify** is selected

All: Whether **Evaluate all data** is selected

Y: Used (selected)

N: Not used (not selected)

The following table describes the differences when alarms are reported.

Damping	When the alarm is reported
n/m	The alarm is reported when the threshold is exceeded *n* times during *m* evaluations of the alarm. Subsequently, the alarm is reported every time the threshold is exceeded *n* times during *m* evaluations of the alarm.
n/n#	If the threshold continues to be exceeded, the alarm is reported every n evaluations. This is useful when you do not want alarms that have exceeded a threshold to be continuously reported.

#: If **Always notify** is selected and the threshold is exceeded during the first collection after collection is started, the alarm is issued regardless of the interval.

Chapter

7. Displaying Events

This chapter explains how to display events issued by a monitoring agent by using the monitoring console.

7.1 Displaying the latest events
7.2 Displaying the event history
7.3 Outputting the event history

7.1 Displaying the latest events

You can view information on the latest events from the Event Monitor window of PFM - Web Console. In this window, you can check the following three types of event information:

- Agent events

  Events that indicate changes in an agent's status

- Alarm events

  Events that indicate alarms that have been triggered by an agent

- Health check events

  Events issued in response to changes in the health check status

In the Event Monitor window, you can monitor the status change of an agent in real time since the display information is periodically updated automatically. You can also display only events that occurred in particular agents by setting the display conditions and color-code the events according to the event status.

You can also check event information using the Summary View displayed in the Agents tree information frame. In this case, only Abnormal and Warning statuses are displayed for the alarm and agent events. It does not show health check events. For details on summary display, see *3.3.5 Using summary display to check the operating status*.

7.1.1 Displaying the latest events information

Events are listed in chronological order in the Event Monitor window.

To confirm the latest events information in the Event Monitor window:

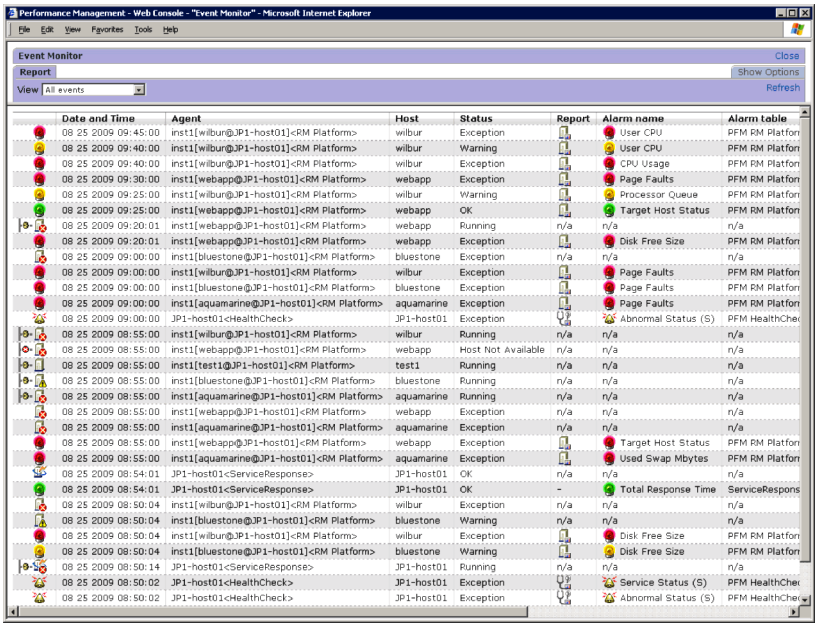
1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

2. From the menu bar frame of the main window, select the **Event Monitor** menu.

   The Event Monitor window appears as a separate window.

Figure 7-1: Example of the Event Monitor window



3. From the **View** menu in the Event Monitor window, select an event type you want to display.

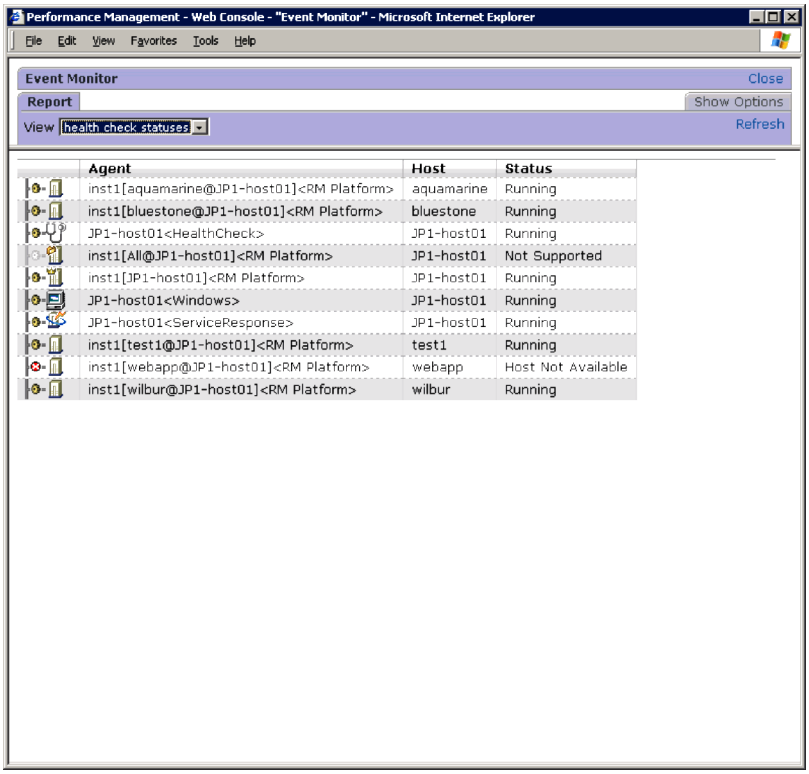
   From the following five items, select an event type you want to display in the Event Monitor window:

   - **All events**
   - **Agent events**
   - **Alarm events**
   - **Health check events**
   - **Health check statuses**

   The default is **All events**.

   Selecting an event type lists the appropriate events. However, when you select **Health check statuses**, only the icon, Agent, Host, and Status are displayed. The following figure shows an example of the Event Monitor window with **Health check statuses** selected:

Figure 7-2: Example of the Event Monitor window displayed when Health check statuses is selected



The following table describes the display items of the Event Monitor window.

Table 7-1: Display items of the Event Monitor window

Display Item	Description
Agent event	An event that indicates the status of an agent. Issues the event when the status of the agent that binds the alarm table changes. The meaning of the icons is as follows: The meaning depends on the type of PFM - Agent or PFM - RM. •  : Normal or not started status (unknown status) •  : Warning status •  : Abnormal status Note: If you select **Always notify** in the alarm definition, no agent event is issued, because the status change of agents is not monitored.
Alarm event	An event that indicates the occurrence of the alarm. Issues the event when it reaches the warning or abnormal threshold. The color meaning of the icons is as follows: •  (green): Normal status •  (yellow): Warning status •  (red): Abnormal status •  #: Alarms set to Always notify
Health check event	An event issued in response to changes in the health check status. The meanings of the icons are as follows: •  : Not Supported •  : Running •  : Incomplete •  : Stopped •  : Unconfirmed •  : Host Not Available

Display Item	Description
Date and Time	Displays the system time of the agent that issued the event, in the format corresponding to the locale. For details, see the chapter describing installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
Agent	Displays the service ID of the agent that is the source of the event occurrence.
Host	Displays the operating host name of the agent that is the source of the event occurrence.
Status	The meanings of the statuses are as follows: For agent events and alarm events: • OK: Normal • Exception: Abnormal • Warning: Warning • Inactive: Not started or an unknown status For health check events and health check statuses: • Not Supported: The agent does not support the health check function. • Running: The services on the agent are working normally. • Incomplete: Some functionality on the agent is unavailable. • Stopped: The service on the agent has stopped. • Unconfirmed: The health check function cannot confirm the status of the host. • Host Not Available: The host is stopped.
Report	Indicates whether a report associated with an event exists. • `n/a`: Reports on agent events do not exist • `-`: Reports on alarm events that do not exist •  : Reports exist (in Windows) •  : Reports exist (in UNIX)

Display Item	Description
Alarm name	Displays the icons and the alarm names detected. •  (green): Normal event •  (yellow): Warning event •  (red): Abnormal event •  #: Abnormal or warning event `n/a` is displayed for agent events and health check events. If you click the icon, the Alarm Properties window is displayed, and you can check the content of the alarm definition.
Alarm table	Displays the detected alarm table name. `n/a` is displayed for agent events and health check events.
Message	For an agent event: Displays messages output from an agent. The main messages to be displayed are as follows: - `Startup`: PFM - Agent or PFM - RM has started. - `Shutdown`: PFM - Agent or PFM - RM has stopped. - `State change`: The status of PFM - Agent or PFM - RM has changed. - `Heartbeat timeout`: The Agent Collector or Remote Monitor Collector service has changed to the busy or stop status. - `Heartbeat detected`: The Agent Collector or Remote Monitor Collector service has recovered from the busy or stop status. In addition to the above, messages starting with KAV might be displayed. When `Heartbeat timeout` is displayed, check the status of PFM - Agent or PFM - RM. If a message starting with KAV appears, see the chapter describing messages in the appropriate PFM - Agent or PFM - RM manual. When other messages are displayed, no actions are needed, because there are no such messages that indicate abnormality.

Display Item	Description
	For an alarm event: Displays the message text set in the alarm wizard. The main messages to be displayed are as follows: - `Alarm updated/deleted`: The alarm definition has been updated or deleted. - `Alarm deactivated`: The alarm has changed to the inactive state. - `Alarm cleared`: The alarm has been unbound. (This event also occurs when an alarm table whose alarm is occurring is imported using the GUI.) - `Alarm expired`: The current time exceeded the alarm evaluation time range. - `Heartbeat timeout`: The Agent Collector or Remote Monitor Collector service has entered a busy or stopped status. - `Heartbeat detected`: The Agent Collector or Remote Monitor Collector service has recovered from the busy or stop status. For a health check event: Displays the message text in the format `HC:` *health-check-status*. This area also displays message text describing the status of the agent, followed by the status of the service. For details on message display rules and examples, see the appendix describing data models in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Displays the message only when you select **Always notify** in the alarm definition.

Multi-instance records operate as follows:

- When any value in a warning or abnormal condition is detected in a target instance:

  The user-defined message set in the message text in an alarm definition is displayed. Additionally, the instance value for which a value over the threshold was detected is displayed if the measured value of the performance data in set in the message text.

- When conditions return to normal from abnormal or warning:

  Nothing is specified in the message text even though normal events are issued, because all the instance values become normal and the value that caused the event to occur is not determined.

4. Click the **Close** menu on the upper right of the window to close the window.

   The Event Monitor window closes.

7.1.2 Displaying a report associated with an alarm

If an alarm event is issued within the Performance Management system, the report associated with the alarm can be displayed from the Event Monitor window.

To display a report associated with an alarm:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

2. From the menu bar frame of the main window, select the **Event Monitor** menu.

   The Event Monitor window appears as a separate window. If a report associated with an alarm exists, the report icon (when Agent for Platform,  or ) is displayed in the **Report** column.

3. Click the report icon of the event whose report is displayed.

   The alarm report window appears as a separate window.

   If you want to close the Report window and the Event Monitor window, click the **Close** button in the upper-right corner of the window.

7.1.3 Displaying alarm properties

In the Event Monitor window, clicking the icon for the alarm event (Alarm icon) displays the Alarm Properties window. In the Alarm Properties window, you can check the content of the alarm definition for the alarm event displayed in the Event Monitor window.

To display alarm properties:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

2. From the menu bar frame of the main window, select the **Event Monitor** menu.

   The Event Monitor window appears as a separate window.

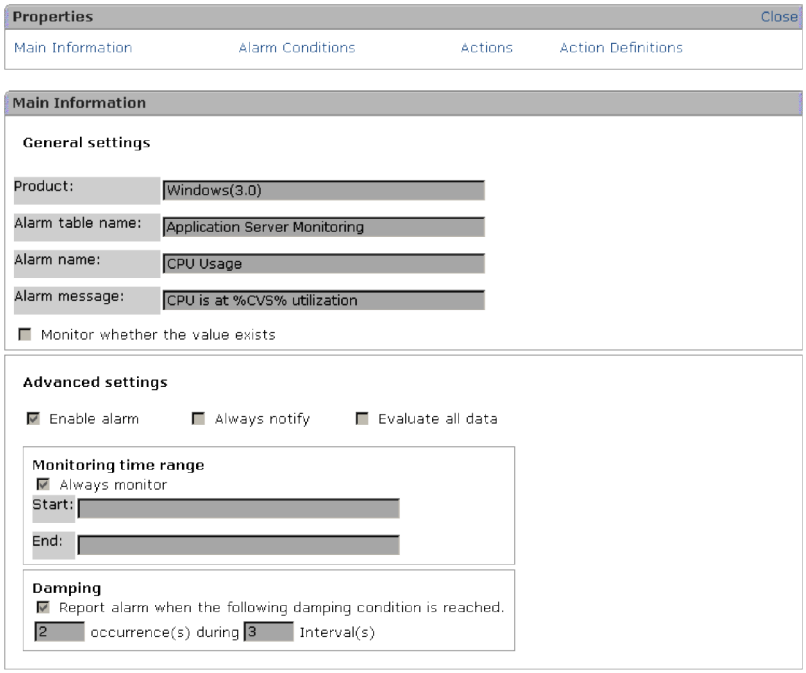
3. From the **View** menu of the Event Monitor window, select **Alarm events**.

   The alarm events are listed.

4. Click an alarm icon for an alarm event.

   The Alarm Properties window appears as a separate window, so you can confirm the content of the alarm definition.

Figure 7-3: Example of the Properties window



Selecting the following items enables you to jump to the view area for the appropriate settings.

Main Information

Jump to the view area for the main information.

Alarm Conditions

Jump to the view area for the alarm conditions.

Actions

Jump to the view area for the action settings to be executed.

Action Definitions

Jump to the view area for the action definitions.

If you want to close the Alarm Properties window and the Event Monitor window, click the **Close** button in the upper-right corner of the window.

Reference note:

If you have a user account with administrator user permissions, you can also

display the Alarm Properties window from the Alarms window. For details on how to confirm the alarm properties from the Alarms window, see *6.6.5 Displaying alarm properties (definitions)*.

7.1.4 Setting the display conditions for the Event Monitor window

You can set the display conditions for the Event Monitor window, such as the event display period and the maximum display count.

To set the display conditions:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

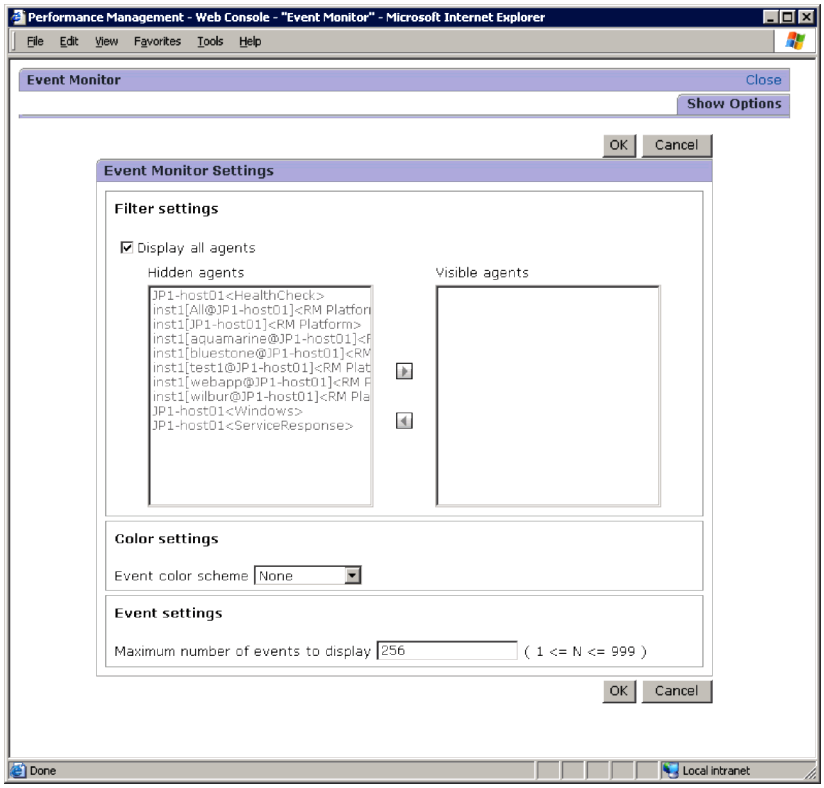
2. From the menu bar frame of the main window, select the **Event Monitor** menu.

   The Event Monitor window (**Report** tab's window) appears as a separate window.

3. Click the **Show Options** tab in the Event Monitor window.

   The window of the **Show Options** tab is displayed.

   Figure 7-4: Example of the Event Monitor window (Show Options tab)



4. Set the display condition.

   Set display conditions for the following items, if necessary:

   Filter Settings

   If you want to display the events that occurred in all the agents, select **Display all agents**. By default, this is selected.

   When you want to display only the specific agents, deselect **Display all agents** and using the move buttons (), move the agent to be displayed into **Visible agents** and move the agent not to be displayed into **Hidden agents**.

   When you, however, deselect **Display all agents**, no event can be displayed unless you specify at least one agent in **Visible agents**.

   Color Settings

   You can color-code events to be displayed in the Event Monitor window according to their status (normal, warning, or abnormal). By default, **Event color scheme** is **None** (no color-coded).

   If you want to color-code the events, from the **Event color scheme** pull-down menu, select the color (**Pastel colors** or **Bright colors**) to be color-coded.

   Event Settings

   You can set the maximum number of events (records) to be displayed in the Event Monitor window. When you set it, enter an integer from 1 to 999 in **Maximum number of events to display**. The default is 256.

5. Click the **OK** button.

   Accept the settings and return to the **Report** tab's window. In the **Report** tab's window, events are displayed according to the display conditions to be set.

Reference note:

The display conditions set in this operation are available during the session. When you log off, the display conditions are not saved and are reset to the initial values.

7.2 Displaying the event history

The information on the previous events that occurred in the Performance Management system can be checked from the PFM - Web Console Event History window.

One Event History window is displayed per agent. You can display the Event History window by specifying the date range for the data, an alarm name, the maximum number of records, and so on.

7.2.1 Displaying the event history

To check the information on the previous events that occurred in the Performance Management system:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. In the navigation frame of the Agents window, select the agent whose event history you want to display.

   When you want to select multiple agents, select **Multiselect**.

   The selected agents are marked with checkmarks.

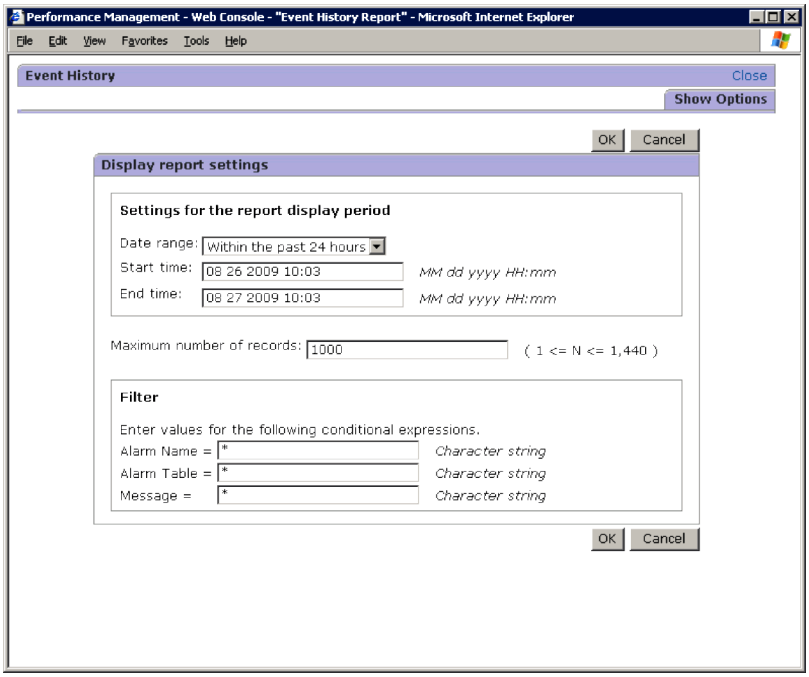
   Reference note:

   > If you do not select an agent, the histories of events that occurred in all the agents are displayed.

4. In the method frame of the Agents window, select the **Event History** method.

   The Event History window (**Show Options** tab's window) appears as a separate window.

Figure 7-5: Example of the Event History window (Show Options tab)



5. Set the individual items in **Settings for the report display period**.

   Set display conditions for the following items, if necessary:

   Date range

   When you set the date range for the data you want to display as an event history, select the appropriate date range from the **Date range** pull-down menu.

   The selectable values are as follows:

   - Specify when displayed

   - Within the past hour

   - Within the past 24 hours

   - Within the past 7 days

   - Within the past month

   - Within the past year

   The default is **Within the past 24 hours**.

   When you select something other than **Specify when displayed**, the dates

and times corresponding to the **Start time** and **End time** are automatically set.

Start time and **End time**

When you select **Specify when displayed** in **Date range**, set the Start time and End time of the date range for displaying the event.

You should specify the **Start time** and **End time** in a display format corresponding to the locale.

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

The range of dates and times you can specify is from 1971/01/01 00:00 to 2035/12/31 23:59. For the **End time**, specify a date and time after the **Start time** you specified.

Note that when you select something other than **Specify when displayed**, the appropriate date and time is automatically set. Additionally, if you change the date and time that are automatically displayed, settings for the **Date range** change to **Specify when displayed**.

6. Set the **Maximum number of records**.

Set the display conditions for the following items, if necessary:

Maximum number of records

The maximum number of events to be displayed as an event history in the **Report** tab's window can be an integer from 1 to 1440. The default is 1000.

However, you can specify the maximum number of records (`maxFetchCount`) from 1 to 2,147,483,647 in the initialization settings file (`config.xml`) of PFM - Web Console. In this case, you can specify the maximum number of records within the range of values you specified in the `config.xml` file.

7. Set the individual items in **Filter**.

Set the display conditions for the following items, if necessary:

Alarm Name

An alarm name of an event to be displayed can be any number of characters up to 2,048 bytes. Specifying an alarm name in this item enables an event at which the alarm occurred to be displayed.

By default, an asterisk (a wildcard character) is used.

Alarm Table

An alarm table name of an event to be displayed can be any number of characters up to 2,048 bytes. Specifying an alarm table name in this item enables you to display events that occurred and that are for alarms of the alarm table.

By default, an asterisk (a wildcard character) is used.

Message

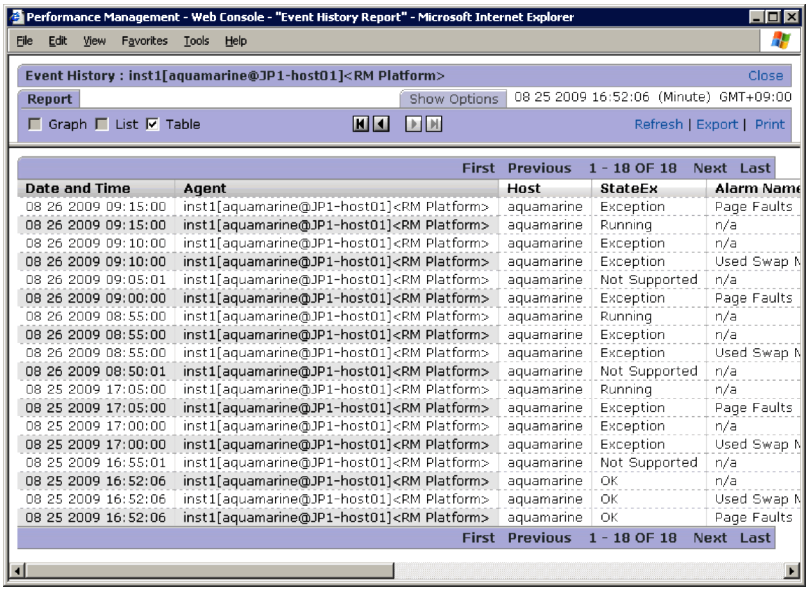
The message text of an event can be displayed using no more than 2,048 bytes. Specifying message text in this item enables you to display events that output the message text.

By default, an asterisk (a wildcard character) is used.

8. Click the **OK** button.

The Event History window (**Report** tab's window) appears.

Figure 7-6: Example of the Event History window



The following table describes the display items of the Event History window.

Table 7-2: Display items of the Event History window

Display Items	Description
Date and Time	Displays the system's date and time of the agent host, which is the source of the event occurrence, in the format corresponding to the locale. For details, see the chapter describing installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
Agent	Service ID of the agent that is the source of the event occurrence.
Host	Operating host name of the agent that is the source of the event occurrence.
StateEx	The meanings of the statuses are as follows: For agent events and alarm events: • **OK**: Normal • **Exception**: Abnormal • **Warning**: Warning • **Inactive**: Not started or an unknown status For health check events: • **Not Supported**: The agent does not support the health check function. • **Running**: The services on the agent are working normally. • **Incomplete**: Some functionality on the agent is unavailable. • **Stopped**: The service on the agent has stopped. • **Unconfirmed**: The health check function cannot confirm the status of the host. • **Host Not Available**: The host is stopped.
Alarm Name	The alarm names in the source of the event occurrence.
Alarm Table	The alarm table names in the source of the event occurrence.

Display Items	Description
Message	For an agent event: Displays messages output from an agent. The main messages to be displayed are as follows: - `Startup`: PFM - Agent or PFM - RM has started. - `Shutdown`: PFM - Agent or PFM - RM has stopped. - `State change`: The status of PFM - Agent or PFM - RM has changed. - `Heartbeat timeout`: The Agent Collector or Remote Monitor Collector service has changed to the busy or stop status. - `Heartbeat detected`: The Agent Collector or Remote Monitor Collector service has recovered from the busy or stop status. In addition to the above, messages starting with KAV might be displayed. When `Heartbeat timeout` is displayed, check the status of PFM - Agent or PFM - RM. If a message starting with KAV appears, see the chapter describing messages in the appropriate PFM - Agent or PFM - RM manual. When other messages are displayed, no actions are needed, because there are no such messages that indicate abnormality. For an alarm event: Displays the message text set in the alarm wizard. The main messages to be displayed are as follows: - `Alarm updated/deleted`: The alarm definition has been updated or deleted. - `Alarm deactivated`: The alarm has changed to the inactive state. - `Alarm cleared`: The alarm was unbound. - `Alarm expired`: The current time exceeded the alarm evaluation time range. - `Heartbeat timeout`: The Agent Collector or Remote Monitor Collector service has changed to the busy or stop status. - `Heartbeat detected`: The Agent Collector or Remote Monitor Collector service has recovered from the busy or stop status. For a health check event: Displays the message text in the format `HC:` *health-check-status*. This area also displays message text describing the status of the agent, followed by the status of the service. For details on message display rules and examples, see the appendix describing data models in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Multi-instance records operate as follows:

- When any of the values in a warning or abnormal condition is detected in a target instance:

  The user-defined message set in the message text in an alarm definition is displayed. Additionally, the instance value for which a value over the threshold was detected is displayed if the measured value of the performance data in set in the message text.

- When conditions return to normal from abnormal or warning:

  Nothing is specified in the message text even though normal events are issued, because all the instance values become normal and the value that caused the event to occur is not determined.

9. Click the **Close** menu in the upper-right corner of the window to close the window.

   The Event History window closes.

Supplemental information:

- If no displayable event exists, a message indicating this is displayed.
- The display conditions set in this operation are available only while the Event History window is being displayed, and the settings are not saved.

Reference note:

If the number of records exceeds the maximum number of records, the records from the oldest one to the maximum number of records are displayed.

7.3 Outputting the event history

This section explains how to output the event history in CSV or HTML format.

7.3.1 Outputting the event history in CSV format

To output event history data to a text file in CSV format:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. From the navigation frame in the Agents window, select an agent whose data you want to output in the CSV format.

   If you want to select multiple agents, select **Multiselect**.

   Each selected agent is marked with a checkmark.

   Reference note:

   > If you do not select an agent, the histories of events that occurred in all the agents are displayed.

4. In the method frame of the Agents window, select the **Event History** method.

   The Event History window appears as a separate window.

5. Select the **Export** menu on the menu bar in the Event History window.

   A dialog box to specify the output destination appears.

6. Specify where the file is to be saved and the file name, and then click the **Save** button.

   The event history data is output to a file.

7.3.2 Outputting the event history in HTML format

You can display event history data in a format suitable for printing or saving to disk.

To output event history data in HTML format:

1. From the monitoring console browser, log on to PFM - Web Console.

   The main window appears.

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

   The Agents window appears.

3. From the navigation frame in the Agents window, select an agent whose data you want to output in the HTML format.

   If you want to select multiple agents, select **Multiselect**.

   Each selected agent is marked with a checkmark.

   Reference note:

   > If you do not select an agent, the histories of events that occurred in all the agents are displayed.

4. In the method frame of the Agents window, select the **Event History** method.

   The Event History window opens in a new window.

5. Select the **Print** menu on the menu bar in the Event History window.

   The event history data appears in a new window in a format suitable for printing or saving to disk.

6. Print or save the report using your browser.

   When saving the report, use the option that saves the complete web page.

Chapter 8. Backing Up and Restoring Data

This chapter explains how to back up and restore a Performance Management system. The procedure is intended for system administrators.

It is important to consider backing up your Performance Management system as part of your backup plan for the entire system.

8.1 Overview of backing up and restoring data
8.2 Overview of partial backups
8.3 Backing up and restoring definition information
8.4 Backing up and restoring operation-monitoring data

8.1 Overview of backing up and restoring data

Some data used in Performance Management might be unrecoverable: for example, when the Performance Management system becomes inoperable due to a disk failure. To prepare for such situations, you need to back up the definition information and operation monitoring data periodically.

This section explains how to back up the information stored in Performance Management.

8.1.1 Data backup methods

In Performance Management, you can select the backup method according to the storage method used for the Store database. Store 1.0 allows for full backups only. Store 2.0 allows for partial backups as well as full backups. It also allows you to specify a backup directory. However, you can specify a backup directory only when backing up the data of the Agent Store or Remote Monitor Store service on the host where the backup command is being executed. For details on partial backups, see *8.2 Overview of partial backups*.

8.1.2 Information that needs to be backed up

The following two types of information must be backed up:

- Definition information required to operate Performance Management
- Operation monitoring data collected by Performance Management (performance data and event data)

8.2 Overview of partial backups

With Store 2.0, you can partially back up performance data. Partial backup is available only while the Agent Store or Remote Monitor Store service is running. Partial backups allow you to accumulate differential data by specifying a past backup directory as the backup destination.

(1) Data subject to back up

When backing up data, you need to specify the beginning and end of the backup period based on Greenwich Mean Time as a number of days relative to the execution date of the backup command. For example, if you want to perform a partial backup of the performance data from three days prior to the execution date (the backup date) up to the day before the execution date, specify 3 as the start of the backup period and 1 as the end. In this case, the backup operation applies to the data from three days to one day prior to execution of the backup command. When the backup command is executed, the data from the specified backup period is backed up to the backup directory.

Because the PD and PL databases and the per-minute and hourly records in the PI database are stored in multiple files that each contains the performance data for a particular day, the unit databases for the specified dates are backed up. The daily, weekly, monthly, and yearly records in the PI database are included in the backup data even when they contain data from outside the period defined by the specified start and end dates.

(2) Effectively using partial backups

(a) Minimizing duplicate backup data as much as possible

The Store 2.0 database is composed of multiple unit databases each covering a specific time period. Only the most recent unit database is updated. For example, when using unit databases that each contains the performance data for a specific day, the Agent sequentially writes data to the unit database for that day. However, the unit database from the previous day remains unchanged from its status at 23:59 GMT until its retention period expires and the file is deleted. Accordingly, by performing a partial backup of the data from the date when the previous backup was made to the day before the current backup date, you can back up data without acquiring the same day's unit database more than once.

Example: When the previous backup was acquired *n* days ago

```
jpctool db backup -id DS1inst1[host1] -d d:\backup01#
-partial (n+1),1
```

`D:\backup01` indicates the backup directory.

(b) Backing up the most recent data possible

To back up the latest database, use the following command:

Example: Backing up the latest version of the database

```
jpctool db backup -id DS1inst1[host1] -d d:\backup01#
-partial 0,0
```

`D:\backup01` indicates the backup directory.

(3) Example of performing a partial backup

The following is an example of performing a partial backup in the JST (Japan Standard Time, GMT + 9:00) time zone.

At 3 AM each day, an overnight batch job is executed that executes the following backup command targeting the instance `inst1` of the multi-instance Agent Store and Remote Monitor Store services with the product ID `Z`.

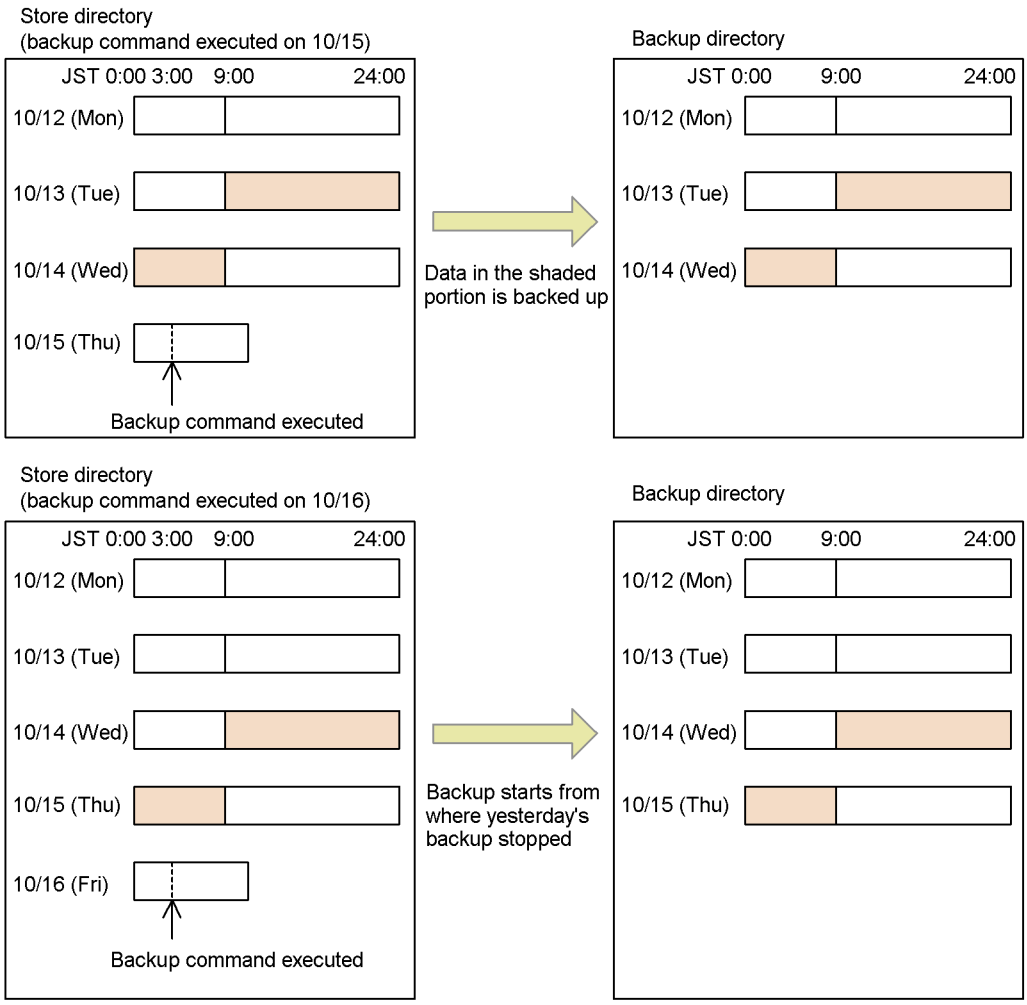
```
jpctool db backup -id DSinst1[host1] -partial 1,1
```

In this case, the unit database that covers the time that is the same as the backup command execution time on the date in the specified range is backed up. Now, suppose that the backup command is executed at 03:00 on October 15, in a week that begins on October 12.

1. The command is executed at 03:00 (JST) on October 15.
2. Taking into account the 9-hour difference, 03:00 JST on October 15 is 18:00 GMT on October 14.
3. Because the command specifies `-partial 1,1` (one day ago), the partial backup applies to the data between 00:00 AM and 23:59 PM (GMT) on October 13.
4. Again, taking into account the 9-hour difference, the backup range from 00:00 GMT to 23:59 GMT on October 13 is from 09:00 JST on October 13 to 09:00 JST on October 14.

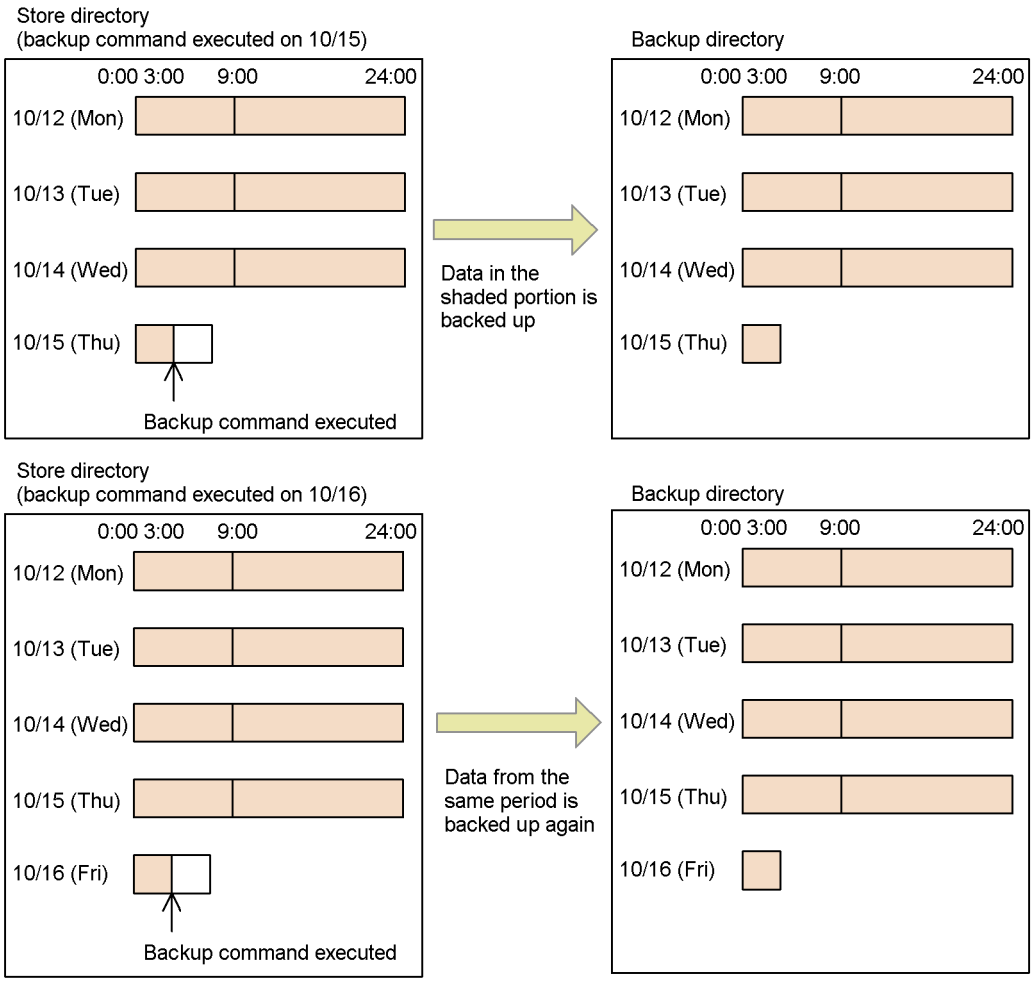
Therefore, in the case of per-minute records, the data from 09:00 on October 13 until 09:00 on October 14 JST is backed up. If the backup command is executed again at the same time on the following day, you can start backing up from where you stopped on the previous day. The following figure shows the backup range for per-minute records.

Figure 8-1: Backup range for per-minute records



In the case of weekly records, because the unit database that covers the specified period is backed up, this results in the data from 09:00 on October 12 to 03:00 on October 15, including the latest data, being backed up. If the backup command is executed again at the same time on the following day, all of the data from the beginning of the week (October 12) onward is backed up again. The following figure shows the backup range for weekly records.

Figure 8-2: Backup range for weekly records



8.3 Backing up and restoring definition information

The following definition information in Performance Management needs to be backed up:

- Report definition information

  Definition information required for displaying reports.

- Alarm definition information

  Definition information required for issuing alarms.

- Service definition information

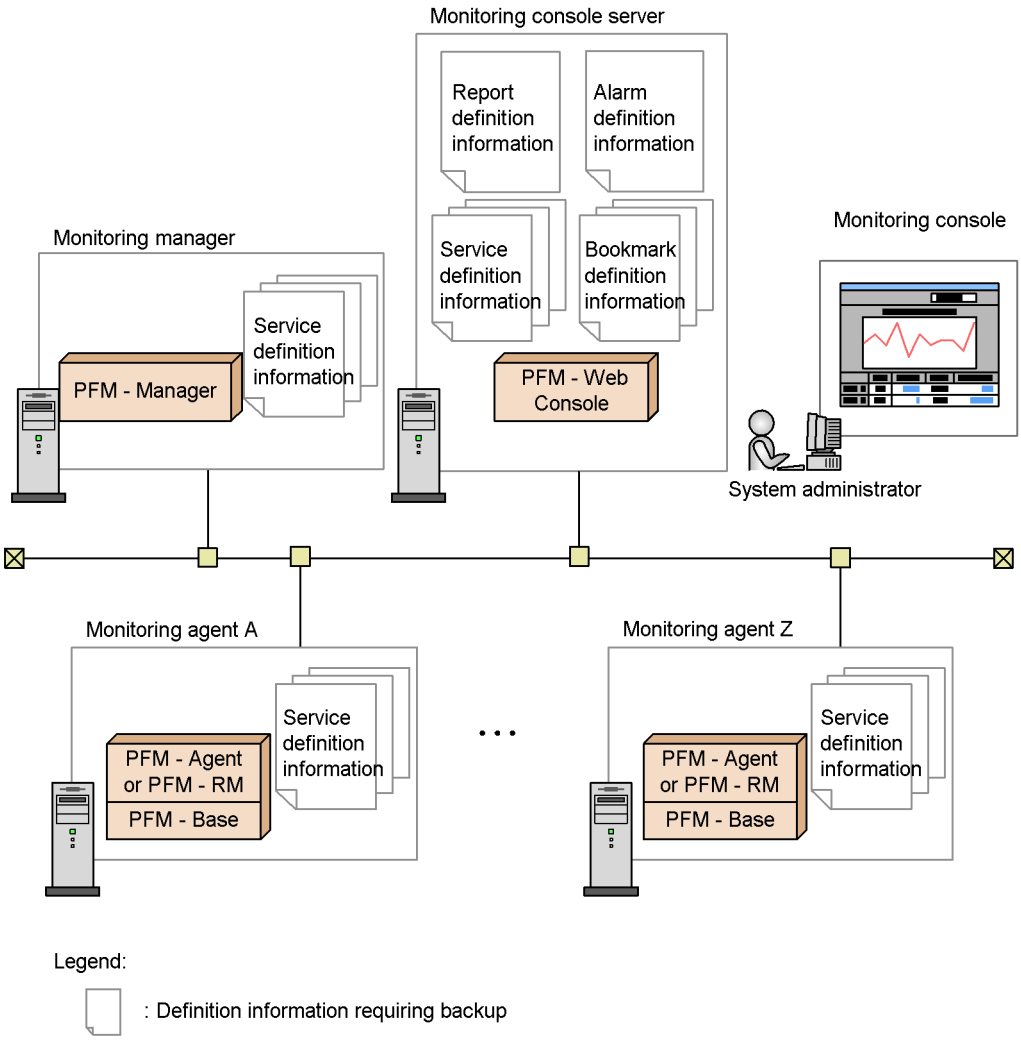
  Definition files required for starting Performance Management. This information is in PFM - Manager, PFM - Web Console, PFM - Base, PFM - Agent, and PFM - RM.

- Bookmark definition information

  Bookmark definition information set per user. This information is in PFM - Web Console.

The following figure shows the definition information that needs to be backed up.

Figure 8-3: Definition information that needs to be backed up in Performance Management



Point:

If you change the configuration or settings for Performance Management, it is recommended that you back up the definition information.

8.3.1 Backing up and restoring report definition information

This section explains how to back up and restore report definition information.

(1) Backing up report definition information

To back up report definition information, export the definition information.

For details on how to export the report definition information, see *5.3.13 Exporting reports*.

(2) Restoring report definition information

To restore report definition information, import the exported definition information.

For details on how to restore the report definition information, see *5.3.14 Importing a report*.

8.3.2 Backing up and restoring alarm definition information

This section describes backing up and restoring alarm definition information.

(1) Backing up alarm definition information

To back up alarm definition information, export the definition information.

For details on how to export the alarm definition information, see *6.4.10 Exporting alarm tables*.

(2) Restoring alarm definition information

To restore alarm definition information, import the exported definition information.

For details on how to restore the alarm definition information, see *6.4.11 Importing alarm tables*.

8.3.3 Backing up and restoring service definition information

You have to back up and restore the service definition information on the hosts for PFM - Manager, PFM - Web Console, PFM - Base, PFM - Agent, and PFM - RM respectively.

The following gives cautionary notes on backing up and restoring the service definition information:

Notes:

- Before you back up or restore the service definition information, you should stop all of the Performance Management programs and services on the local host.
- If Performance Management runs on a logical host, you should back up and restore the service definition information on the physical host of each Performance Management program. Before you do so, you should stop all of the Performance Management programs and services on the physical host.
- If you restore the service definition information only to the PFM - Agent or PFM - RM host, node information on the instance and others added after backup remain on the host of PFM - Manager and PFM - Web Console. In this case, do the

following operations to delete the unnecessary agent information:

To delete the unnecessary agent information:

1. Execute the `jpctool service delete` command.
2. Restart the PFM - Manager programs and services.
3. Restart the PFM - Web Console programs and services.

- If PFM - Manager is used to back up or restore service definition information when a PFM - Agent or PFM - RM instance is added to the system or a port used to communicate with PFM - Agent or PFM - RM is dynamic, the port used when the data is backed up might differ from the port used after the data is restored. If this occurs, PFM - Manager might not be able to communicate with PFM - Agent or PFM - RM, or PFM - Web Console might not be able to display information correctly. In such a case, restart the relevant PFM - Agent or PFM - RM services.

(1) Backing up and restoring service definition information for PFM - Manager

The following describes how to back up and restore the service definition information for PFM - Manager:

Backup

Copy the PFM - Manager service definition information file to the backup target. For details about the PFM - Manager service definition information file requiring a backup, see *(a) In Windows* or *(b) In UNIX*.

Note:

When backing up PFM - Manager, note the product version number for the backed-up environment. For details on product version numbers, see the *Release Notes*.

Restoration

When restoring PFM - Manager settings information, confirm that the following prerequisites are met, and copy the backup files to their original locations. Overwrite the settings information file on the host by using the backed up settings information file. If PFM - Manager runs on a logical host, overwrite the service definition information file on the physical host and in the environment directory.

Prerequisite conditions

- PFM - Manager is installed.
- The PFM - Manager services have stopped.

Note:

To restore PFM - Manager settings information, the product version number for the environment from which the information was backed up must match that of the environment where it is to be restored. For details on product version numbers, see the *Release Notes*. The following examples show when restoration can be performed and when it cannot be:

Example where restoration is allowed

Settings information backed up for PFM - Manager 08-11 can be restored to PFM - Manager 08-11.

Examples where restoration is not allowed

Settings information backed up for PFM - Manager 08-00 cannot be restored to PFM - Manager 08-11.

Settings information backed up for PFM - Manager 08-11 cannot be restored to PFM - Manager 08-11-04.

(a) In Windows

The following table describes the service definition information files to be backed up for PFM - Manager.

Table 8-1: Service definition information files to be backed up (in Windows)

Type	File name	Description
PFM - Manager	*installation-folder*\jpchosts	Host information configuration file for Performance Management
	*installation-folder**.ini	Settings file common to Performance Management
	installation-folder\bin\action*.ini	Settings file for the Action Handler service
	installation-folder\bin\statsvr*.ini	Settings file for the Status Server service
	installation-folder\mgr\clator*.ini	Settings file for the Correlator service
	installation-folder\mgr\manager*.ini	Settings file for the Master Manager service
	installation-folder\mgr\manager*.DB	Database file for the Master Manager service
	installation-folder\mgr\manager*.IDX	Index file for the Master Manager service

Type	File name	Description
	installation-folder\mgr\manager*.DAT	Data model file for the Master Manager service
	installation-folder\mgr\store*.ini	Settings file for the Master Store service
	installation-folder\mgr\store*.DAT	Data model file for the Master Store service
	installation-folder\mgr\namesvr*.ini	Settings file for the Name Server service
	installation-folder\mgr\namesvr*.DB	Database file for the Name Server service
	installation-folder\mgr\namesvr*.IDX	Index file for the Name Server service
	installation-folder\mgr\trapgen*.ini	Settings file for the Trap Generator service
	installation -folder\mgr\viewsvr*.ini	Settings file for the View Server service
	installation-folder\mgr\viewsvr\data*	User definition information file for the View Server service
	installation-folder\mgr\viewsvr\reports*	Report definition information file for the View Server service
	installation-folder\agt0\agent*.ini	Settings file for the Agent Collector service (files for the health check agent)
	installation-folder\agt0\store*.ini	Settings file for the Agent Store service (files for the health check agent)
PFM - Manager (for logical host use)	*environment-directory*#1\jp1pc*.ini	Settings file common to Performance Management
	environment-directory#1\jp1pc\bin\action*.ini	Settings file for the Action Handler service
	installation-folder\bin\statsvr*.ini #2	Settings file for the Status Server service
	environment-directory#1\jp1pc\mgr\clator*.ini	Settings file for the Correlator service

Type	File name	Description
	environment-directory[#1]\jp1pc\mgr\manager*.ini	Settings file for the Master Manager service
	environment-directory[#1]\jp1pc\mgr\manager*.DB	Database file for the Master Manager service
	environment-directory[#1]\jp1pc\mgr\manager*.IDX	Index file for the Master Manager service
	environment-directory[#1]\jp1pc\mgr\manager*.DAT	Data model file for the Master Manager service
	environment-directory[#1]\jp1pc\mgr\store*.ini	Settings file for the Master Store service
	environment-directory[#1]\jp1pc\mgr\store*.DAT	Data model file for the Master Store service
	environment-directory[#1]\jp1pc\mgr\namesvr*.ini	Settings file for the Name Server service
	environment-directory[#1W]\jp1pc\mgr\namesvr*.DB	Database file for the Name Server service
	environment-directory[#1]\jp1pc\mgr\namesvr*.IDX	Index file for the Name Server service
	environment-directory[#1]\jp1pc\mgr\trapgen*.ini	Settings file for the Trap Generator service
	environment-directory[#1]\jp1pc\mgr\viewsvr*.ini	Settings file for the View Server service
	environment-directory[#1]\jp1pc\mgr\viewsvr\data*	User definition information file for the View Server service
	environment-directory[#1]\jp1pc\mgr\viewsvr\reports*	Report definition information file for the View Server service
	environment-directory[#1]\jp1pc\agt0\agent*.ini	Settings file for the Agent Collector service (files for the health check agent)
	environment-directory[#1]\jp1pc\agt0\store*.ini	Settings file for the Agent Store service (files for the health check agent)

#1

The environment directory is a directory on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

(b) In UNIX

The following table describes the service definition information files to be backed up for PFM - Manager.

Table 8-2: Service definition information files to be backed up (in UNIX)

Type	File name	Description
PFM - Manager	/opt/jp1pc/jpchosts	Host information configuration file for Performance Management
	/opt/jp1pc/*.ini	Settings file common to Performance Management
	/opt/jp1pc/bin/action/*.ini	Settings file for the Action Handler service
	/opt/jp1pc/bin/statsvr/*.ini	Settings file for the Status Server service
	/opt/jp1pc/mgr/clator/*.ini	Settings file for the Correlator service
	/opt/jp1pc/mgr/manager/*.ini	Settings file for the Master Manager service
	/opt/jp1pc/mgr/manager/*.DB	Database file for the Master Manager service
	/opt/jp1pc/mgr/manager/*.IDX	Index file for the Master Manager service
	/opt/jp1pc/mgr/manager/*.DAT	Data model file for the Master Manager service
	/opt/jp1pc/mgr/store/*.ini	Settings file for the Master Store service
	/opt/jp1pc/mgr/store/*.DAT	Data model file for the Master Store service
	/opt/jp1pc/mgr/namesvr/*.ini	Settings file for the Name Server service

Type	File name	Description
	/opt/jp1pc/mgr/namesvr/*.DB	The database file for the Name Server service
	/opt/jp1pc/mgr/namesvr/*.IDX	Index file for the Name Server service
	/opt/jp1pc/mgr/trapgen/*.ini	Settings file for the Trap Generator service
	/opt/jp1pc/mgr/viewsvr/*.ini	Settings file for the View Server service
	/opt/jp1pc/mgr/viewsvr/jpcvsvr	Settings file for the View Server service
	/opt/jp1pc/mgr/viewsvr/data/*	User definition information file for the View Server service
	/opt/jp1pc/mgr/viewsvr/Reports/*	Report definition information file for the View Server service
	/opt/jp1pc/agt0/agent/*.ini	Settings file for the Agent Collector service (files for the health check agent)
	/opt/jp1pc/agt0/store/*.ini	Settings file for the Agent Store service (files for the health check agent)
PFM - Manager (for logical host use)	/*environment-directory*[#1]/jp1pc/*.ini	Settings file common to Performance Management
	/*environment-directory*[#1]/jp1pc/bin/action/*.ini	Settings file for the Action Handler service
	/opt/jp1pc/bin/statsvr/*.ini[#2]	Settings file for the Status Server service
	/*environment-directory*[#1]/jp1pc/mgr/clator/*.ini	Settings file for the Correlator service
	/*environment-directory*[#1]/jp1pc/mgr/manager/*.ini	Settings file for the Master Manager service
	/*environment-directory*[#1]/jp1pc/mgr/manager/*.DB	Database file for the Master Manager service

Type	File name	Description
	/*environment-directory*[#1]/jp1pc/mgr/manager/*.IDX	Index file for the Master Manager service
	/*environment-directory*[#1]/jp1pc/mgr/manager/*.DAT	Data model file for the Master Manager service
	/*environment-directory*[#1]/jp1pc/mgr/store/*.ini	Settings file for the Master Store service
	/*environment-directory*[#1]/jp1pc/mgr/store/*.DAT	Data model file for the Master Store service
	/*environment-directory*[#1]/jp1pc/mgr/namesvr/*.ini	Settings file for the Name Server service
	/*environment-directory*[#1]/jp1pc/mgr/namesvr/*.DB	Database file for the Name Server service
	/*environment-directory*[#1]/jp1pc/mgr/namesvr/*.IDX	Index file for the Name Server service
	/*environment-directory*[#1]/jp1pc/mgr/trapgen/*.ini	Settings file for the Trap Generator service
	/*environment-directory*[#1]/jp1pc/mgr/viewsvr/*.ini	Settings file for the View Server service
	/*environment-directory*[#1]/jp1pc/mgr/viewsvr/jpcvsvr	Settings file for the View Server service
	/*environment-directory*[#1]/jp1pc/mgr/viewsvr/data/*	User definition information file for the View Server service
	/*environment-directory*[#1]/jp1pc/mgr/viewsvr/Reports/*	Report definition information file for the View Server service
	/*environment-directory*[#1]/jp1pc/agt0/agent/*.ini	Settings file for the Agent Collector service (files for the health check agent)
	/*environment-directory*[#1]/jp1pc/agt0/store/*.ini	Settings file for the Agent Store service (files for the health check agent)

#1

The environment directory is a directory on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

(2) Backing up and restoring service definition information for PFM - Web Console

The following describes how to back up and restore the service definition information for PFM - Web Console:

Backup

Copy the PFM - Web Console service definition information file to the backup target. For details on the PFM - Web Console service definition information files to be backed up for Windows and UNIX, see Table *8-3 Service definition information files to be backed up (in Windows)* and Table *8-4 Service definition information files to be backed up (in UNIX)*, respectively.

Note:

When backing up PFM - Web Console, make sure that you manage the product version number in the environment where the backup is acquired. For details on product version numbers, see the *Release Notes*.

Restoration

When restoring PFM - Web Console settings information, confirm that the following prerequisites are met, and copy the backup files to their original locations. Overwrite the settings information file on the host by using the backed up settings information file. If PFM - Web Console runs on a logical host, overwrite the service definition information file on the physical host and in the environment directory.

Prerequisite conditions

- PFM - Web Console is installed.
- The PFM - Web Console services have stopped.

Note:

To restore PFM - Web Console settings information, the product version number for the environment from which the information was backed up must match that of the environment where it is to be restored. For details on product version numbers, see the *Release Notes*. The following examples show when restoration can be performed and when it cannot be:

Example where restoration is allowed

Settings information backed up for PFM - Web Console 08-11 can be restored to PFM - Web Console 08-11.

Examples where restoration is not allowed

Settings information backed up for PFM - Web Console 08-00 cannot be restored to PFM - Web Console 08-11.

Settings information backed up for PFM - Web Console 08-11 cannot be restored to PFM - Web Console 08-11-04.

(a) In Windows:

The following table describes the service definition information files to be backed up for PFM - Web Console.

Table 8-3: Service definition information files to be backed up (in Windows)

Type	File name	Description
PFM - Web Console	*installation-folder*\conf*	Settings file for PFM - Web Console
	installation-folder\bookmarks*	Bookmark definition information file for PFM - Web Console
	installation-folder\cmdkey*	Authentication key file for the PFM - Web Console command
	installation-folder\CPSB\httpsd\conf*.conf	Settings file for PFM - Web Console
	installation-folder\CPSB\CC\web\redirector\workers.properties	Settings file for PFM - Web Console
	installation-folder\CPSB\CC\web\containers\PFMWebConsole\usrconf*.cfg	Settings file for PFM - Web Console
	installation-folder\CPSB\CC\web\containers\PFMWebConsole\usrconf\usrconf.properties	Settings file for PFM - Web Console

Type	File name	Description
PFM - Web Console (for logical host use)	*installation-folder*\conf*	Settings file for PFM - Web Console
	environment-directory#\jp1pcWebCon\bookmarks*	Bookmark definition information file for PFM - Web Console
	installation-folder\cmdkey*	Authentication key file for the PFM - Web Console command
	installation-folder\CPSB\httpsd\conf*.conf	Settings file for PFM - Web Console
	installation-folder\CPSB\CC\web\redirector\workers.properties	Settings file for PFM - Web Console
	installation-folder\CPSB\CC\web\containers\PFMWebConsole\usrconf*.cfg	Settings file for PFM - Web Console
	installation-folder\CPSB\CC\web\containers\PFMWebConsole\usrconf\usrconf.properties	Settings file for PFM - Web Console

#

The environment directory is a folder on the shared disk created when a logical host is created.

For details on how to back up and restore the definition information for bookmarks, see *8.3.4 Backing up and restoring bookmark definition information*.

(b) In UNIX

The following table describes the service definition information files to be backed up for PFM - Web Console.

Table 8-4: Service definition information files to be backed up (in UNIX)

Type	File name	Description
PFM - Web Console	/opt/jp1pcwebcon/conf/*	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/bookmarks/*	Bookmark definition information file for PFM - Web Console

Type	File name	Description
	/opt/jp1pcwebcon/cmdkey/*	Authentication key file for the PFM - Web Console command
	/opt/jp1pcwebcon/CPSB/httpsd/conf/*.conf	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/CPSB/CC/web/redirector/workers.properties	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/*.cfg	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/usrconf.properties	Settings file for PFM - Web Console
PFM - Web Console (for logical host use)	/opt/jp1pcwebcon/conf/*	Settings file for PFM - Web Console
	environment-directory# /jp1pcwebCon/bookmarks/*	Bookmark definition information file for PFM - Web Console
	/opt/jp1pcwebcon/cmdkey/*	Authentication key file for the PFM - Web Console command
	/opt/jp1pcwebcon/CPSB/httpsd/conf/*.conf	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/CPSB/CC/web/redirector/workers.properties	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/*.cfg	Settings file for PFM - Web Console
	/opt/jp1pcwebcon/CPSB/CC/web/containers/PFMWebConsole/usrconf/usrconf.properties	Settings file for PFM - Web Console

#

The environment directory is a folder on the shared disk created when a logical host is created.

For details on how to back up and restore the definition information for bookmarks, see *8.3.4 Backing up and restoring bookmark definition information*.

(3) Backing up and restoring service definition information for PFM - Base

The following describes how to back up and restore the service definition information for PFM - Base:

Backup

Copy the PFM - Base service definition information file to the backup target. For details on the PFM - Base service definition information file requiring a backup, see *(a) In Windows* or *(b) In UNIX* below.

Note:

When backing up PFM - Base, note the product version number for the backed-up environment. For details on product version numbers, see the *Release Notes*.

Restoration

When restoring PFM - Base settings information, confirm that the following prerequisites are met, and copy the backup files to their original locations. Overwrite the settings information file on the host by using the backed up settings information file. If PFM - Base runs on a logical host, overwrite the service definition information file on the physical host and in the environment directory.

Prerequisite conditions

- PFM - Base is installed.
- The PFM - Base services have stopped.

Note:

To restore PFM - Base settings information, the product version number for the environment from which the information was backed up must match that of the environment where it is to be restored. For details on product version numbers, see the *Release Notes*. The following examples show when restoration can be performed and when it cannot be:

Example where restoration is allowed

Settings information backed up for PFM - Base 08-11 can be restored to PFM - Base 08-11.

Examples where restoration is not allowed

Settings information backed up for PFM - Base 08-00 cannot be restored to PFM - Base 08-11.

Settings information backed up for PFM - Base 08-11 cannot be restored to PFM - Base 08-11-04.

(a) In Windows

The following table describes the service definition information files to be backed up for PFM - Base.

Table 8-5: Service definition information files to be backed up (in Windows)

Type	File name	Description
PFM - Base	*installation-folder*\jpchosts	Host information configuration file for Performance Management
	*installation-folder**.ini	Settings file common to Performance Management
	installation-folder\bin\action*.ini	Settings file for the Action Handler service
	installation-folder\bin\statsvr*.ini	Settings file for the Status Server service
PFM - Base (for logical host use)	*environment-directory*#1\jp1pc*.ini	Settings file common to Performance Management
	environment-directory#1\jp1pc\bin\action*.ini	Settings file for the Action Handler service
	installation-folder#2\bin\statsvr*.ini	Settings file for the Status Server service

#1

The environment directory is a folder on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

(b) In UNIX

The following table describes the service definition information files to be backed up for PFM - Base.

Table 8-6: Service definition information files to be backed up (in UNIX)

Type	File name	Description
PFM - Base	`/opt/jp1pc/jpchosts`	Host information configuration file for Performance Management
	`/opt/jp1pc/*.ini`	Settings file common to Performance Management
	`/opt/jp1pc/bin/action/*.ini`	Settings file for the Action Handler service
	`/opt/jp1pc/bin/statsvr/*.ini`	Settings file for the Status Server service
PFM - Base (for logical host use)	*/environment-directory*[#1]`/jp1pc/*.ini`	Settings file common to Performance Management
	/environment-directory[#1]`/jp1pc/bin/action/*.ini`	Settings file for the Action Handler service
	`/opt/jp1pc/bin/statsvr/*.ini`[#2]	Settings file for the Status Server service

#1

The environment directory is a directory on the shared disk created when a logical host is created.

#2

The settings file for the Status Server service exists only on the physical host even if the service runs on a logical host.

(4) Backing up and restoring service definition information for PFM - Agent

The following explains how to back up and restore the service definition information for PFM - Agent:

Backup

Copy the PFM - Agent service definition information file to the backup target. For details on the PFM - Agent service definition information file requiring a backup, see *(a) In Windows* or *(b) In UNIX*.

Note:

When backing up PFM - Agent, note the product version number for the backed-up environment. For details on product version numbers, see the *Release Notes*.

Restoration

When restoring PFM - Agent settings information, confirm that the following prerequisites are met, and copy the backup files to their original locations. Overwrite the settings information file on the host by using the backed up settings information file. If PFM - Agent runs on a logical host, overwrite the service definition information file on the physical host and in the environment directory.

Prerequisite conditions

- PFM - Agent is installed.
- The PFM - Agent services have stopped.

Note:

To restore PFM - Agent settings information, the product version number for the environment from which the information was backed up, must match that of the environment where it is to be restored. For details on product version numbers, see the *Release Notes*. The following examples show when restoration can be performed and when it cannot be:

Example where restoration is allowed

Settings information backed up for PFM - Agent 08-11 can be restored to PFM - Agent 08-11.

Examples where restoration is not allowed

Settings information backed up for PFM - Agent 08-00 cannot be restored to PFM - Agent 08-11.

Settings information backed up for PFM - Agent 08-11 cannot be restored to PFM - Agent 08-11-04.

All of the files listed below are common service definition information files that you need to back up for any PFM - Agent type. In addition to these files, you might need to back up PFM - Agent type-specific service definition information files. For details on the PFM - Agent-specific service definition information file requiring a backup, see the appropriate PFM - Agent manual.

(a) In Windows

The following table describes the service definition information files to be backed up for PFM - Agent.

Table 8-7: Service definition information files to be backed up (in Windows)

Type	File name	Description
PFM - Agent	*installation-folder**xxxx*[#1]`\agent\*.ini`	Settings file for the Agent Collector service
	*installation-folder**xxxx*[#1]`\agent\`*instance-name*[#2]`\*.ini`	Settings file for the Agent Collector service
	*installation-folder**xxxx*[#1]`\store\*.ini`	Settings file for the Agent Store service
	*installation-folder**xxxx*[#1]`\store\`*instance-name*[#2]`\*.ini`	Settings file for the Agent Store service
PFM - Agent (for logical host use)	*environment-directory*[#3]`\jp1pc\`*xxxx*[#1]`\agent\*.ini`	Settings file for the Agent Collector service

Type	File name	Description
	environment-directory[#3]\jp1pc*xxxx*[#1]\agent*instance-name**.ini	Settings file for the Agent Collector service
	environment-directory[#3]\jp1pc*xxxx*[#1]\store*.ini	Settings file for the Agent Store service
	environment-directory[#3]\jp1pc*xxxx*[#1]\store*instance-name*[#2]*.ini	Settings file for the Agent Store service

#1

xxxx represents the service key of the PFM - Agent. For details on the service key for each PFM - Agent instance, see the section that describes naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

These are folders that exist when running in an instance environment. In an instance configuration, one folder is created for each instance.

#3

The environment directory is a folder on the shared disk created when a logical host is created.

In PFM - Agent for Platform (Windows), the backup also applies to the following file:

- Application definition file (*installation-folder*\agtt\agent\jpcapp)

(b) In UNIX

The following table describes the definition information files to be backed up for PFM - Agent.

Table 8-8: Definition information files to be backed up (in UNIX)

Type	File name	Description
PFM - Agent	/opt/jp1pc/*xxxx*[#1]/agent/*.ini	Settings file for the Agent Collector service
	/opt/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/*.ini	Settings file for the Agent Collector service
	/opt/jp1pc/*xxxx*[#1]/store/*.ini	Settings file for the Agent Store service

Type	File name	Description
	/opt/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/*.ini	Settings file for the Agent Store service
PFM - Agent (for logical host use)	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/*.ini	Settings file for the Agent Collector service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/*.ini	Settings file for the Agent Collector service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/store/*.ini	Settings file for the Agent Store service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/*.ini	Settings file for the Agent Store service

#1

xxxx represents the service key of the PFM - Agent. For details on the service key for each PFM - Agent instance, see the section that describes naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

These are directories when running in an instance environment. In an instance configuration, one directory is created for each instance.

#3

The environment directory is a directory on the shared disk created when a logical host is created.

For PFM - Agent for Platform (UNIX), back up the following files as well.

- Application definition file (/opt/jp1pc/agtu/agent/jpcapp)

To be backed up if log information collection is set.

- Event file (/opt/jp1pc/agtu/agent/evfile)

To be backed up if workgroup information is set.

- Workgroup file (/opt/jp1pc/agtu/agent/wgfile)

(5) Backing up and restoring service definition information for PFM - RM

The following explains how to back up and restore the service definition information for PFM - RM:

Backup

Copy the PFM - RM service definition information file to the backup target. For details on the PFM - RM service definition information file requiring a backup, see *(a) In Windows* or *(b) In UNIX*.

Note:

When backing up PFM - RM, note the product version number for the backed-up environment. For details on product version numbers, see the *Release Notes*.

Restoration

When restoring PFM - RM settings information, confirm that the following prerequisites are met, and copy the backup files to their original locations. Overwrite the settings information files on the host with the corresponding backup files. If PFM - RM runs on a logical host, overwrite the service definition information file on the physical host and in the environment directory.

Prerequisite conditions

- PFM - RM is installed.
- The PFM - RM services have stopped.

Note:

To restore PFM - RM settings information, the product version number for the environment from which the information was backed up, must match that of the environment where it is to be restored. For details on product version numbers, see the *Release Notes*. The following examples show when restoration can be performed and when it cannot be:

Example where restoration is allowed

Settings information backed up for PFM - RM 09-00 can be restored to PFM - RM 09-00.

Examples where restoration is not allowed

Settings information backed up for PFM - RM 09-00 cannot be restored to PFM - RM 09-10.

Settings information backed up for PFM - RM 09-00 cannot be restored to PFM - RM 09-00-04.

All of the files listed below are common service definition information files that you need to back up for any PFM - RM type. In addition to these files, you might need to back up PFM - RM type-specific service definition information files. For details on the PFM - RM type-specific service definition information files to be backed up, see the

appropriate PFM - RM manual.

(a) In Windows:

The following table describes the service definition information files to be backed up for PFM - RM.

Table 8-9: Service definition information files to be backed up (in Windows)

Type	File name	Description
PFM - RM	*installation-folder**xxxx*[#1]\agent*.ini	Settings file for the Remote Monitor Collector service
	*installation-folder**xxxx*[#1]\agent*instance-name*[#2]*.ini	Settings file for the Remote Monitor Collector service
	*installation-folder**xxxx*[#1]\agent*instance-name*[#2]\groups*.ini	Settings file for the Remote Monitor Collector service
	*installation-folder**xxxx*[#1]\agent*instance-name*[#2]\targets*.ini	Settings file for the Remote Monitor Collector service
	*installation-folder**xxxx*[#1]\store*.ini	Settings file for the Remote Monitor Store service
	*installation-folder**xxxx*[#1]\store*instance-name*[#2]*.ini	Settings file for the Remote Monitor Store service
PFM - RM (for logical host use)	*environment-directory*[#3]\jp1pc*xxxx*[#1]\agent*.ini	Settings file for the Remote Monitor Collector service
	environment-directory[#3]\jp1pc*xxxx*[#1]\agent*instance-name**.ini	Settings file for the Remote Monitor Collector service
	environment-directory[#3]\jp1pc*xxxx*[#1]\agent*instance-name*\groups*.ini	Settings file for the Remote Monitor Collector service
	environment-directory[#3]\jp1pc*xxxx*[#1]\agent*instance-name*\targets*.ini	Settings file for the Remote Monitor Collector service

Type	File name	Description
	environment-directory[#3]\jp1pc*xxxx*[#1]\store*.ini	Settings file for the Remote Monitor Store service
	environment-directory[#3]\jp1pc*xxxx*[#1]\store*instance-name*[#2]*.ini	Settings file for the Remote Monitor Store service

#1

xxxx indicates the service key of each PFM - RM. For details on the PFM - RM service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

One folder is created for each instance.

#3

The environment directory is a folder on the shared disk created when a logical host is created.

(b) In UNIX:

The following table describes the definition information files to be backed up for PFM - RM.

Table 8-10: Definition information files to be backed up (in UNIX)

Type	File name	Description
PFM - RM	/opt/jp1pc/*xxxx*[#1]/agent/*.ini	Settings file for the Remote Monitor Collector service
	/opt/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/*.ini	Settings file for the Remote Monitor Collector service
	/opt/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/groups/*.ini	Settings file for the Remote Monitor Collector service
	/opt/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/targets/*.ini	Settings file for the Remote Monitor Collector service

Type	File name	Description
	/opt/jp1pc/*xxxx*[#1]/store/*.ini	Settings file for the Remote Monitor Store service
	/opt/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/*.ini	Settings file for the Remote Monitor Store service
PFM - RM (for logical host use)	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/*.ini	Settings file for the Remote Monitor Collector service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/*.ini	Settings file for the Remote Monitor Collector service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/groups/*.ini	Settings file for the Remote Monitor Collector service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/targets/*.ini	Settings file for the Remote Monitor Collector service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/store/*.ini	Settings file for the Remote Monitor Store service
	/*environment-directory*[#3]/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/*.ini	Settings file for the Remote Monitor Store service

#1

xxxx indicates the service key of each PFM - RM. For details on the PFM - RM service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

One directory is created for each instance.

#3

The environment directory is a directory on the shared disk created when a logical host is created.

8.3.4 Backing up and restoring bookmark definition information

This section describes backing up and restoring bookmark definition information in the following cases:

- When bookmark definition information is located in the default directory
- When you want to change the location of bookmark definition information to a different directory
- When you want to change the PFM - Manager host connection, and inherit the bookmarks created before the change
- When you want to migrate PFM - Manager and PFM - Web Console to a cluster configuration, and inherit the bookmarks that existed before the migration

Note:

When backing up or restoring the bookmark definition information, make sure that the related directories are manually copied to an appropriate location after stopping the PFM - Web Console service. However, you should back up and restore the entire directory that contains the bookmark definition information as well as a part of files and directories at one time.

(1) When bookmark definition information is located in the default directory

The default location of the bookmark definition information and bookmark folders is as follows:

installation-folder[#]`\bookmarks` (in Windows)

`/opt/jp1pcwebcon`[#]`/bookmarks` (in UNIX)

#

When PFM - Web Console is run on a logical host in a cluster system, this directory is replaced with the environment directory. The *environment directory* is a directory created on the shared disk when setting up Performance Management in a logical host environment.

This subsection describes how to back up and restore the entire directory containing bookmark definition information.

This subsection assumes that the name of the host running PFM - Manager to which PFM - Web Console is connected is called `hostA`.

■ In Windows:

Bookmark installation folder (default)
installation-folder`\bookmarks\hostA\0`

Backup procedure

To back up the bookmark information, copy the entire `0` folder to a different location.

Restoration procedure

To restore the bookmark information, copy the entire `0` folder into *installation-folder*`\bookmarks\hostA`.

- **In UNIX:**

Bookmarks installation directory
`/opt/jp1pcwebcon/bookmarks/hostA/0`

Backup procedure

To back up the bookmark information, copy the entire `0` directory to a different location.

Restoration procedure

To restore the bookmark information, copy the entire `0` directory into `/opt/jp1pcwebcon/bookmarks/hostA`.

(2) When you want to change the location of bookmark definition information to a different directory

First, change the setting for the location of the bookmark definition information to a different directory. Then, transfer the existing definition information to the new directory.

(a) Setting an installation folder for bookmark definition information

You can set a folder to store the bookmark definition information for the bookmark Repository in the Windows initialization file (`config.xml`).

The steps to set an installation folder for the bookmark definition information for the Windows initialization file (`config.xml`) are given below. For running on a logical host, use the same installation folder for both the executing node and the standby node.

To set an installation folder for the bookmark definition information for the Windows initialization file (`config.xml`):

1. Open the Windows initialization file (`config.xml`).

   The Windows initialization file (`config.xml`) is in the following location:

   installation-folder`\conf\config.xml`

2. Set the installation folder for the bookmark definition information.

   Set the installation folder for the `<bookmark>` tag immediate after the `<format>` tag in the `<vsa>` tag of the Windows initialization file (`config.xml`).

The installation folder that has been specified will be automatically created when the PFM - Web Console service starts.

When Running on a Non-Cluster System:

For example, specify the following when you want the `c:\common\bookmarks` to be an installation folder:

```
</format>

<bookmark>
<!-- The directory where bookmark repository is stored.
Default : <install directory>\bookmarks -->
<param name="bookmarkRepository"
value="c:\common\bookmarks"/>
</bookmark>

</vsa>
```

When Running on a Logical Host:

Specify a folder on the shared disk as an installation folder for the bookmark definition information.

For example, specify the following when you want the *environment-directory*`\jp1pcWebCon\common\bookmarks` to be an installation folder:

```
</format>

<bookmark>
<!-- The directory where bookmark repository is stored.
Default : <install directory>\bookmarks -->
<param name="bookmarkRepository"
value="environment-directory\jp1pcWebCon\common\bookmarks"/>
</bookmark>

</vsa>
```

3. Save the Windows initialization file (`config.xml`) edited in step 2.
4. Restart the PFM - Web Console service.

   The Windows initialization file (`config.xml`) is loaded when a PFM - Web Console service starts. Restart the PFM - Web Console service for the changed

settings in the settings file to take effect. However, for the standby node, there is no need to restart it here because it is automatically restarted when a failback occurs.

Notes:

- If you change any areas other than those mentioned above in the initialization file (`config.xml`), PFM - Web Console might not operate correctly.
- If running the programs on a cluster system, restart the PFM - Web Console service from the cluster software.

(b) Making a new directory inherit bookmark definition information

This subsection describes how to inherit existing bookmark definition information for a new installation directory. This subsection assumes that the name of the host running PFM - Manager to which PFM - Web Console is connected is called `hostB`.

■ In Windows:

This example assumes the following installation folders:

Old bookmark installation folder
installation-folder`\bookmarks\hostB\0`

New bookmark installation folder
`C:\user1\bookmarks`

To make a new folder inherit existing bookmarks:

1. Stop the PFM - Web Console service.

   For details on stopping services, see *1.3.2 Stopping monitoring console server services*.

2. Back up the `hostB` subfolder found in the old bookmark installation folder.

   To back up the subfolder, copy it to a different location.

3. Change the bookmarks installation folder defined in the initialization file (`config.xml`) to a new bookmarks installation folder.

4. Create the new bookmark installation folder.

5. Copy the folder backed up in step 2 into the new bookmark installation folder.

   The `hostB` subfolder should now exist in the `C:\user1\bookmarks` folder.

6. Start the PFM - Web Console service.

   For details on starting services, see *1.2.2 Starting services on the monitoring console server*.

■ **In UNIX:**

This example assumes the following bookmark installation directories:

Old bookmark installation directory
`/opt/jp1pcwebcon/bookmarks/hostB/0`

New bookmark installation directory
`/opt/user1/bookmarks`

To make a new directory inherit existing bookmarks:

1. Stop the PFM - Web Console service.

   For details on stopping services, see *1.3.2 Stopping monitoring console server services*.

2. Back up the `hostB` subdirectory found in the old bookmark installation directory.

   To back up the subdirectory, copy it to a different location.

3. Change the bookmarks installation directory defined in the initialization file (`config.xml`) to a new bookmarks installation directory.

4. Create the new bookmark installation directory.

5. Copy the directory backed up in step 2 into the new bookmark installation directory.

   The `hostB` subdirectory should now exist in the `/opt/user1/bookmarks` directory.

6. Start the PFM - Web Console service.

   For details on starting services, see *1.2.2 Starting services on the monitoring console server*.

(3) When you want to change the PFM - Manager host connection, and inherit the bookmarks created before the change

If the PFM - Manager host connection is changed while using bookmarks, the bookmarks created before the change cannot be inherited. Recreate the bookmarks on the new PFM - Manager host.

(4) When you want to migrate PFM - Manager and PFM - Web Console to a cluster configuration, and inherit the bookmarks that existed before the migration

Contrary to case (3), where a new host connection is unable to inherit existing bookmarks, a logical host can inherit existing bookmarks when you switch over PFM - Manager and PFM - Web Console from physical host use to logical host use. This is because information from PFM - Agent and PFM - RM connected to PFM - Manager in the physical host environment is inherited by PFM - Manager running in the logical host environment.

In Windows:

This example assumes the following conditions, including the host names:

When a physical host is used:

- PFM - Manager host name: `hostE`

- PFM - Manager host name for the connection destination of PFM - Web Console: `hostE`

- Bookmarks installation folder for PFM - Web Console:
  installation-folder`\jp1pcwebcon\bookmarks\0`

When a logical host is used:

- PFM - Manager logical host name: `lhostE`

- PFM - Manager host name for the connection destination of PFM - Web Console: `lhostE`

- Bookmarks installation folder for PFM - Web Console:
  environment-directory`\jp1pcwebcon\bookmarks`

To make a new folder inherit existing bookmarks:

1. Stop the PFM - Web Console service.#
2. Back up the `0` subfolder found in the bookmark installation folder for physical host use.

   To back up the subfolder, copy it to a different location.
3. Change the bookmarks installation folder defined in the initialization file (`config.xml`) to a new bookmarks installation folder to be used when a logical host is operated.
4. Create a bookmarks installation folder to be used when a logical host is operated.
5. Create an `lhostE` folder under the bookmark installation folder for logical host use.
6. Copy the `0` subfolder backed up in step 2 into the new `lhostE` folder.

   The `lhostE` subfolder should now exist in the *environment-directory*`\jp1pcwebcon\bookmarks\lhostE` folder.
7. Start the PFM - Web Console service.#

#

For details on stopping and starting services, see *9.6.1 Starting and stopping Performance Management in a cluster system*.

In UNIX:

This example assumes the following conditions, including the host names:

When a physical host is used:

- PFM - Manager host name: `hostE`
- PFM - Manager host name for the connection destination of PFM - Web Console: `hostE`
- Bookmarks installation directory for PFM - Web Console: `/opt/jp1pcwebcon/bookmarks/hostE/0`

When a logical host is used:

- PFM - Manager logical host name: `lhostE`
- PFM - Manager host name for the connection destination of PFM - Web Console: `lhostE`
- Bookmarks installation directory for PFM - Web Console: *environment-directory*`/jp1pcwebcon/bookmarks`

To make a new directory inherit existing bookmarks:

1. Stop the PFM - Web Console service.#
2. Back up the `0` subdirectory found in the bookmark installation directory for physical host use.

   To back up the subdirectory, copy it to a different location.
3. Edit the initialization file (`config.xml`) so that the bookmark installation directory points to the bookmark installation directory for logical host use.
4. Create a bookmarks installation directory to be used when a logical host is operated.
5. Create an `lhostE` subdirectory under the bookmark installation directory for logical host use.
6. Copy the `0` subdirectory backed up in step 2 into the new `lhostE` directory.

   The `0` subdirectory should now exist in the *environment-directory*`/jp1pcwebcon/bookmarks/lhostE` directory.
7. Start the PFM - Web Console service.#

#

For details on stopping and starting services, see *9.6.1 Starting and stopping Performance Management in a cluster system*.

Note

- If the installation folder for the bookmark definition information is not changed from the default directory, the installation folder and the definition information file are deleted automatically at uninstallation. If the installation folder is changed, it is not deleted automatically. Delete it manually, if necessary.
- Bookmark definition information consists of multiple files. For this reason, when an error occurs during the creation, update, or deletion of the definition information file and the processing cannot continue, the integrity of the definition information file might be compromised. In such cases, modify or discard the corrupted information.

8.4 Backing up and restoring operation-monitoring data

There are two types of Performance Management operation monitoring data that must be backed up.

- Event data

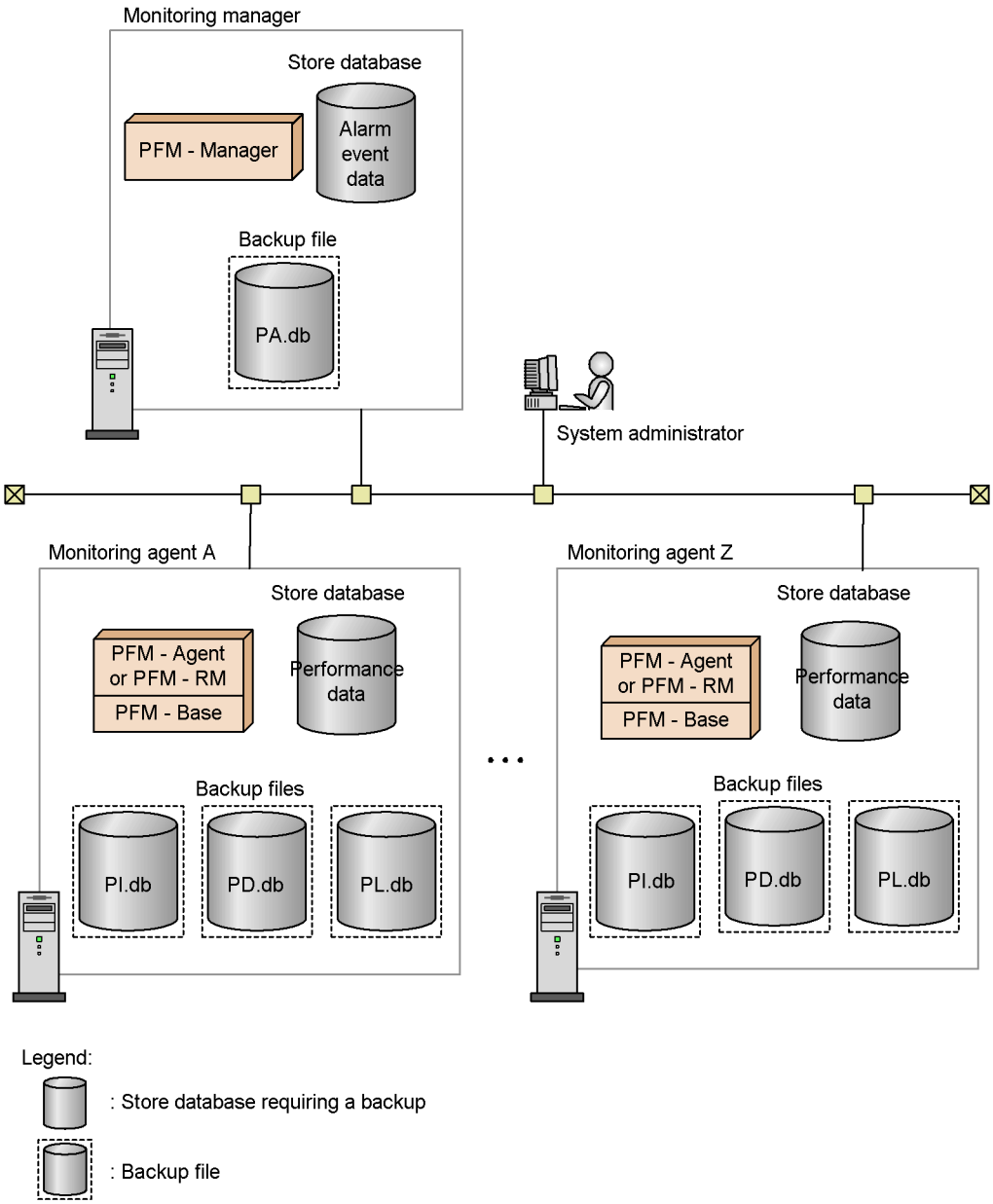
  Data of accumulated events that occurred in Performance Management. The data is stored in the Store database and managed in PFM - Manager.

- Performance data

  Data of accumulated performance information collected from the monitoring target program of the monitoring agent by using PFM - Agent or PFM - RM. The data is stored in the Store database and managed in PFM - Agent or PFM - RM.

The following figure shows the operation monitoring data that must be backed up.

Figure 8-4: Operation monitoring data that must be backed up in Performance Management



To back up the operation monitoring data, you can use the `jpctool db backup` command. You must execute the `jpctool db backup` command on a host where

PFM - Manager is installed. You can also execute the command on a host where PFM - Agent or PFM - RM is installed, specifying the `-alone` or `-direct` option.

When using Store 2.0, you can perform a partial backup by specifying the `-partial` option.

To restore the operation monitoring data, use the `jpctool db restore` command. You must execute the `jpctool db restore` command on the PFM - Manager, PFM - Agent, or PFM - RM host where the database to be restored is backed up.

However, to execute the `jpctool db backup` and `jpctool db restore` commands, the following user permissions are required:

- In Windows: user with Administrator permissions or Backup Operator permissions
- In UNIX: root user permissions

Next are a couple cautionary notes on backing up and restoring the operation monitoring data:

Notes:

- If the data model version of the Store database that is backed up using the `jpctool db backup` command differs from the version of the Store database to be restored, the Store database cannot be restored.
- If a service key of the data to be restored differs from that of the data that is backed up using the `jpctool db backup` command, the Store database cannot be restored.

8.4.1 Backing up and restoring the event data

The following describes how to back up and restore event data by using the `jpctool db backup` command and the `jpctool db restore` command.

(1) Backing up the event data

To back up event data:

1. Log on to the PFM - Manager host.
2. Execute the `jpctool service list` command, and make sure that the services have started.

   Make sure that the Name Server, Master Manager, and Master Store services are running.

   For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.
3. Execute the `jpctool db backup` command.

When Running on a Non-Cluster System:

Back up the event data in the Store database of PFM -Manager. Execute the following command. `PS1001` indicates the service ID for the Master Store service.

```
jpctool db backup -id PS1001
```

By default, executing this command creates the backup file named `PA.DB` in the backup directory on the PFM - Manager host.

- In Windows:

  installation-folder`\mgr\store\backup\`*generation-number*#`\PA.DB`

- In UNIX:

  `/opt/jp1pc/mgr/store/backup/`*generation-number*#`/PA.DB`

When Running on a Logical Host:

Back up the event data in the Store database of the PFM -Manager on the logical host. Execute the following command: `PS1001` indicates the service ID for the Master Store service.

```
jpctool db backup -id PS1001 -lhost logical-host-name
```

By default, executing this command creates the backup file named `PA.DB` in the backup directory on the shared disk.

- In Windows:

  environment-directory`\jp1pc\mgr\store\backup\`*generation-number*#`\PA.DB`

- In UNIX:

  environment-directory`/jp1pc/mgr/store/backup/`*generation-number*#`/PA.DB`

#

The generation number is assigned in ascending order from *01*. The

maximum generation number is the value specified in the `Backup Save` in the `jpcsto.ini` file. By default, the maximum generation number is *05*.

For further details on the `jpctool db backup` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*. For details on service IDs, see the section that describes service naming rules in an appendix of the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

(2) Restoring event data

To restore event data:

1. Log on to the PFM - Manager host.
2. Execute the `jpcspm stop` command to stop the PFM - Manager service.

   For details on how to stop the PFM - Manager service, see *1.3 Stopping services*. For further details on the `jpcstop` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
3. Check the storage location for the backup file.

   For details on the default backup destination for the event data, see step 3 of *(1) Backing up the event data*.
4. Execute the `jpctool db restore` command.

   When Running on a Non-Cluster System:

   For example, execute the following command to restore the event data in *installation-folder*`\mgr\store\backup\01`. (`Manager` indicates the service key for PFM - Manager):

   ```
   jpctool db restore -key Manager -d
   "installation-folder\mgr\store\backup\01"
   ```

   When Running on a Logical Host:

   For example, execute the following command to restore the event data in *environment-directory*`\jp1pc\mgr\store\backup\01` on the logical host `jp1-ha1`. (`Manager` indicates the service key for PFM - Manager):

   ```
   jpctool db restore -key Manager -d
   "environment-directory\jp1pc\mgr\store\backup\01" -lhost jp1-ha1
   ```

   For further details on the `jpctool db restore` command, see the chapter that

describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

5. Execute the `jpcspm start` command to start the PFM - Manager services.

   Start the PFM - Manager services.

   For details on how to start the PFM - Manager services, see *1.2 Starting services*. For further details on the `jpcspm start` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

Note:

Restoring event data sometimes causes a delay in restarting the services, because the index of the database has to be rebuilt when the services start up again.

8.4.2 Backing up and restoring the performance data

The following describes how to back up and restore performance data using the `jpctool db backup` command and the `jpctool db restore` command.

(1) Backing up the performance data

To back up the performance data:

1. Log on to the PFM - Manager host.
2. Execute the `jpctool service list` command, and make sure that the services have started.

   Make sure that the Name Server, Master Manager, and Agent Store or Remote Monitor Store services, which manage the performance data to be backed up, have started.

   For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.
3. Execute the `jpctool db backup` command.

   When Running on a Non-Cluster System:

   For example, execute the following command when you want the performance data in the Store database of PFM - Agent for Oracle on the `host02` host to be backed up:

   ```
   jpctool db backup -id OS* -host host02
   ```

   By default, executing the command creates the backup file named as shown below in the directory on the PFM - Agent or PFM - RM host:

- In Windows:

  *installation folder**xxxx*[#1]\store*instance-name*[#2]\backup*generation-number*[#3]*database-ID*[#4].DB

- In UNIX:

  /opt/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/backup/*generation-number*[#3]/*database-ID*[#4].DB

When Running on a Logical Host:

For example, execute the following command when you want the performance data in the Store database of PFM - Agent for Oracle on the jp1-ha2 logical host to be backed up:

```
jpctool db backup -id OS* -lhost jp1-ha2
```

By default, executing the command creates the backup file named as shown below in the directory on the shared disk:

- In Windows:

  environment-directory\jp1pc*xxxx*[#1]\store*instance-name*[#2]\backup*generation-number*[#3]*database-ID*[#4].DB

- In UNIX:

  environment-directory/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/backup/*generation-number*[#3]/*database-ID*[#4].DB

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on the PFM - Agent or PFM - RM service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

Created when PFM - Agent or PFM - RM is in the instance environment.

#3

The generation number is assigned in ascending order from *01*. The maximum generation number is the value specified in the Backup Save in the jpcsto.ini file. By default, the maximum generation number is *05*.

#4

The following are the database IDs:

PI: Database for records of the PI record type

PD: Database for records of the PD record type

PL: Database for records of the PL record type

However, you can also back up the performance data on a host where PFM - Agent or PFM - RM is installed. To perform backup on a host where PFM - Agent or PFM - RM is installed, specify the `-alone` or `-direct` option in the `jpctool db backup` command.

For further details on the `jpctool db backup` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

(2) Restoring the performance data

To restore the performance data:

1. Log on to the PFM - Agent or PFM - RM host that stores the backup file.
2. Execute the `jpcspm stop` command to stop the PFM - Agent or PFM - RM service.

   For details on how to stop the PFM - Agent or PFM - RM service, see *1.3 Stopping services*. For further details on the `jpcspm stop` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.
3. Check the storage location for the backup file.
4. Execute the `jpctool db restore` command.

   When Running on a Non-Cluster System:

   For example, execute the following command when you want the performance data in the `oracleA` instance of PFM - Agent for Oracle on the *installation-folder*`\agto\store\oracleA\backup\01` to be restored: `Oracle` indicates the service key for PFM - Agent.

   ```
   jpctool db restore -key Oracle -d
   "installation-folder\agto\store\oracleA\backup\01" -inst oracleA
   ```

   When Running on a Logical Host:

   For example, execute the following command when you want the performance

data in the `oracleA` instance of PFM - Agent for Oracle on the *environment-directory*`\jp1pc\agto\store\oracleA\backup\01` of the `jp1-ha2` logical host to be restored (`Oracle` indicates the service key for PFM - Agent):

```
jpctool db restore -key Oracle -d
"installation-folder\agto\store\oracleA\backup\01" -lhost jp1-ha2
-inst oracleA
```

For further details on the `jpctool db restore` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*. For details on the service key for each PFM - Agent or PFM - RM instance, see the section that describes naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

5. Execute the `jpcspm start` command to start the PFM - Agent or PFM - RM service.

   For details on how to start the PFM - Agent or PFM - RM service, see *1.2 Starting services*.

   For further details on the `jpcspm start` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

Note 1:

Restoring performance data sometimes causes a delay in restarting the services, because the index of the database has to be rebuilt when the services are started up again.

Note 2:

Backup data cannot be restored to a Store database that uses different Store version. You can only restore backup data acquired from a database set up to use Store 2.0 to a database that uses Store 2.0. Similarly, you can only restore backup data acquired from a database set up to use Store 1.0 to a database that uses Store version is 1.0.

8.4.3 Partially backing up performance data (Store 2.0)

To partially back up performance data:

1. Log on to the PFM - Manager host.
2. Execute the `jpctool service list` command, and make sure that the services have started.

Make sure that the Name Server, Master Manager, and Agent Store or Remote Monitor Store services, which manage the performance data to be backed up, have started.

For further details on the `jpctool service list` command, see the chapter that describes the command in the manual *Job Management Partner 1/ Performance Management Reference*.

3. Execute the `jpctool db backup` command.

   When Running on a Non-Cluster System:

   For example, execute the following command when you want to perform a partial backup of the performance data from three days ago until yesterday in the Store database of PFM - Agent for Oracle on the `host02` host:

   ```
   jpctool db backup -id OS* -host host02  -partial 3,1
   ```

   By default, executing the command creates the backup file named as shown below in the directory on the PFM - Agent or PFM - RM host:

   - In Windows:

     installation-folder`\`*xxxx*[#1]`\store\`*instance-name*[#2]`\partial\st`*database-ID*[#3]

   - In UNIX:

     `/opt/jp1pc/`*xxxx*[#1]`/store/`*instance-name*[#2]`/partial/st`*database-ID*[#3]

   When Running on a Logical Host:

   For example, execute the following command when you want to perform a partial backup of the performance data from three days ago until yesterday in the Store database of PFM - Agent for Oracle on the logical host `jp1-ha2`:

   ```
   jpctool db backup -id OS* -lhost jp1-ha2  -partial 3,1
   ```

   By default, executing the command creates backup files in the following directory on the shared disk:

   - In Windows:

     environment-directory`\jp1pc\`*xxxx*[#1]`\store\`*instance-name*[#2]`\partial\st`*database-ID*[#3]

   - In UNIX:

environment-directory/jp1pc/*xxxx*[#1]/store/*instance-name*[#2]/partial/st*database-ID*[#3]

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on the PFM - Agent or PFM - RM service keys, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

Created when PFM - Agent or PFM - RM is in the instance environment.

#3

The following are the database IDs:

PI: Database for records of the PI record type

PD: Database for records of the PD record type

PL: Database for records of the PL record type

You can also back up the performance data on a host where PFM - Agent or PFM - RM is installed. To perform backup on a host where PFM - Agent or PFM - RM is installed, specify the `-alone` or `-direct` option in the `jpctool db backup` command.

For further details on the `jpctool db backup` command, see the chapter that describes the command in the manual *Job Management Partner 1/Performance Management Reference*.

The following table describes the directories and file structure used for the files produced by a partial backup:

Table 8-11: Directories and file structure for partial backups

Directory or file	Record type			Format	Min.	Max.	Description
	PI	PD	PL				
ST*XX*	Y	Y	Y	n/a	n/a	n/a	n/a
Summary block	Y	N	N	*n*	1	6	Summary block (for PI records) 1: Minute 2: Hour 3: Day 4: Week 5: Month 6: Year

Directory or file	Record type			Format	Min.	Max.	Description
	PI	PD	PL				
Year	Y	Y	Y	*YYYY*	1900	2027	Year
Month and day	Y	Y	Y	*MMDD*	0101	1231	Month and day
Generation number	Y	Y	Y	*nnn*	001	002	Generation number
record-type.DB	Y	Y	Y	n/a	n/a	n/a	Database file for each record type

Legend:

Y: Is an applicable file or directory.

N: Is not an applicable file or directory.

n/a: Not applicable

XX: Database ID

PI: Database for records of the PI record type

PD: Database for records of the PD record type

PL: Database for records of the PL record type

Chapter 9. Cluster System Configuration and Operation

This chapter describes the installation and setup methods, as well as the flow of processing, for running Performance Management in a cluster system.

9.1 Overview and design of cluster systems
9.2 Configuration of a cluster system (in Windows)
9.3 Changing the cluster system configuration (in Windows)
9.4 Configuration of a cluster system (in UNIX)
9.5 Changing the cluster system configuration (in UNIX)
9.6 Cluster system operations
9.7 Failure recovery in a cluster system
9.8 Notes on cluster systems

9.1 Overview and design of cluster systems

This section describes an overview of cluster systems and the architecture design for running Performance Management in a cluster system.

9.1.1 Overview of cluster systems

Cluster systems are used to link multiple servers and run them as a single system. Cluster systems can be generally classified in the following two types:

- HA (High Availability) cluster systems
- Load-balancing cluster systems

Note:

In this section, *cluster system* refers to an HA cluster system.

(1) Overview of HA cluster systems

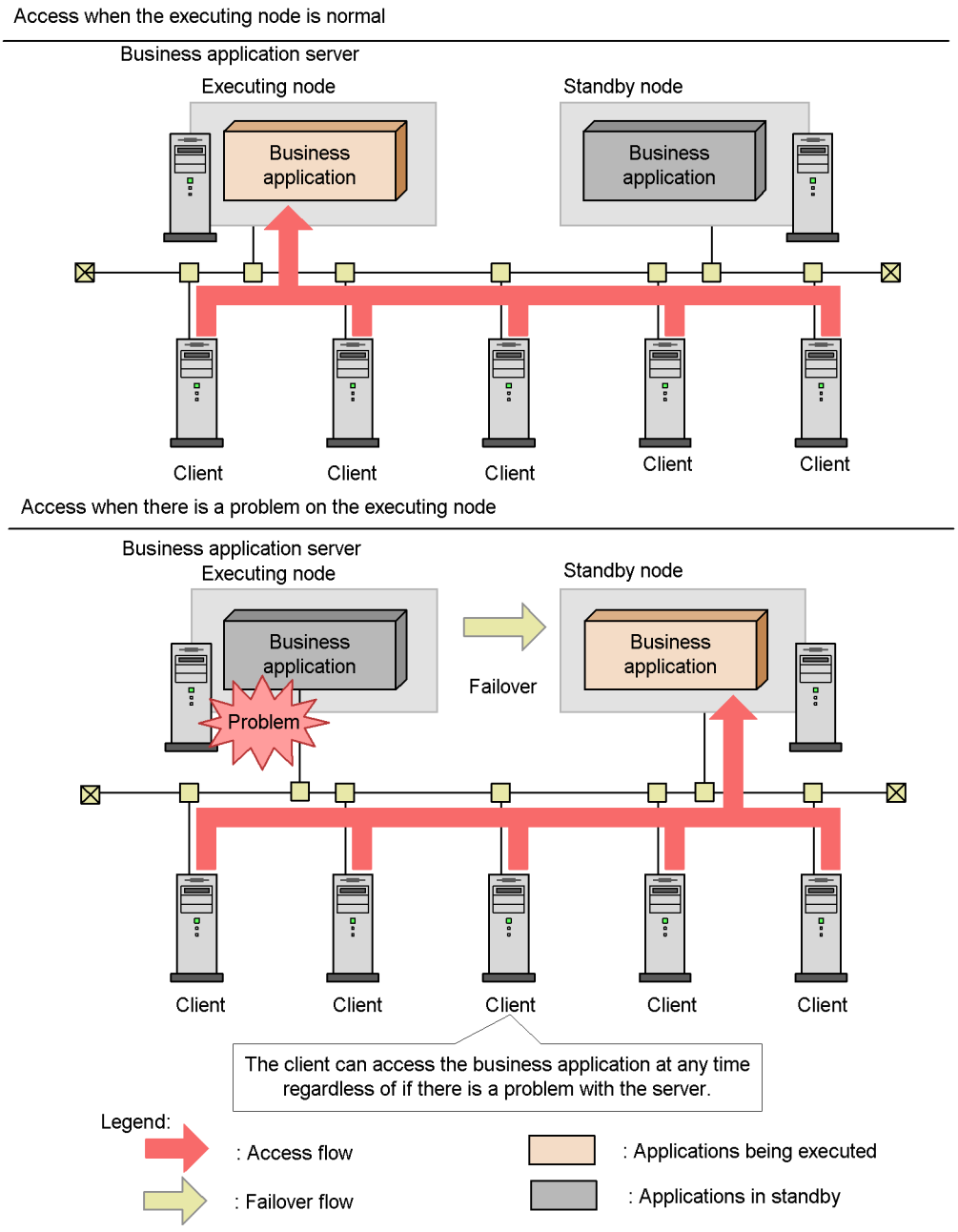
The purpose of *HA cluster systems* is to enhance the availability of the entire system. HA cluster systems are often used in application servers and database servers for mission-critical systems that require high availability.

HA cluster systems include a redundant server for each server that makes up the system. In an HA cluster system, if problems occur in a server that is executing a job, a different server that has been standing by will continue the processing of the job. This is called a *failover*.

Of each of the server systems that make up a cluster system, the system that is executing jobs is called the *executing node* and the system that is standing by to continue the processing when a problem occurs on the executing node is called the *standby node*.

The following figure shows the flow of access when a problem occurs on the executing node.

Figure 9-1: Flow of access when a problem occurs on the executing node of an HA cluster system



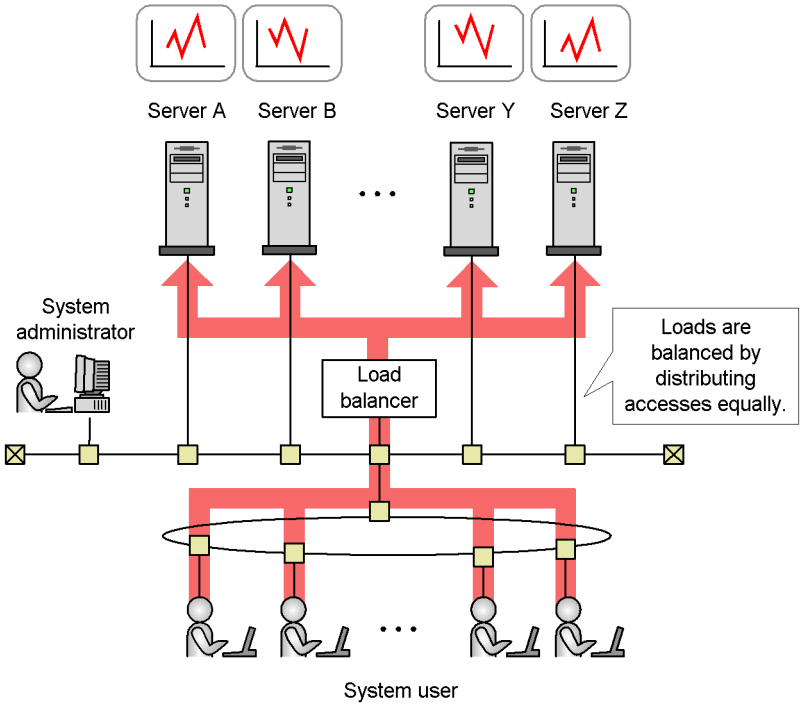
The software that controls the entire HA cluster system is called the *cluster software*. The cluster software always monitors the servers and, if a problem occurs, automatically switches the server for executing a job from that on the executing node to that on the standby node. Therefore, cluster systems are also called *node switching systems*.

(2) Overview of load-balancing cluster systems

Load-balancing cluster systems balance the processing load across multiple servers. They are often used in systems that require high processing performance.

Load-balancing cluster systems place multiple servers in parallel to balance processes, keep the load on any single server low, and increase the processing performance of the entire system. Even if a problem occurs on a server, switching processes to a different node can enhance the availability of the system.

Figure 9-2: Flow of access in a load-balancing cluster system



Supplemental information:

Examples of load-balancing cluster systems include systems that balance servers to receive requests, such as Web systems, and Oracle Real Application Cluster systems. In addition, business applications that run on load-balancing cluster systems require programs that can allocate processes to multiple nodes.

9.1.2 Designing a cluster configuration

Performance Management can monitor operations in a cluster system. This subsection describes designs for cluster configurations for Performance Management.

(1) Examining the configuration in HA cluster systems

This subsection describes the cluster configurations for Performance Management. Running the Performance Management programs on the logical host environment of an HA cluster system is referred to as *logical host use*.

(a) Cluster configuration of PFM - Manager

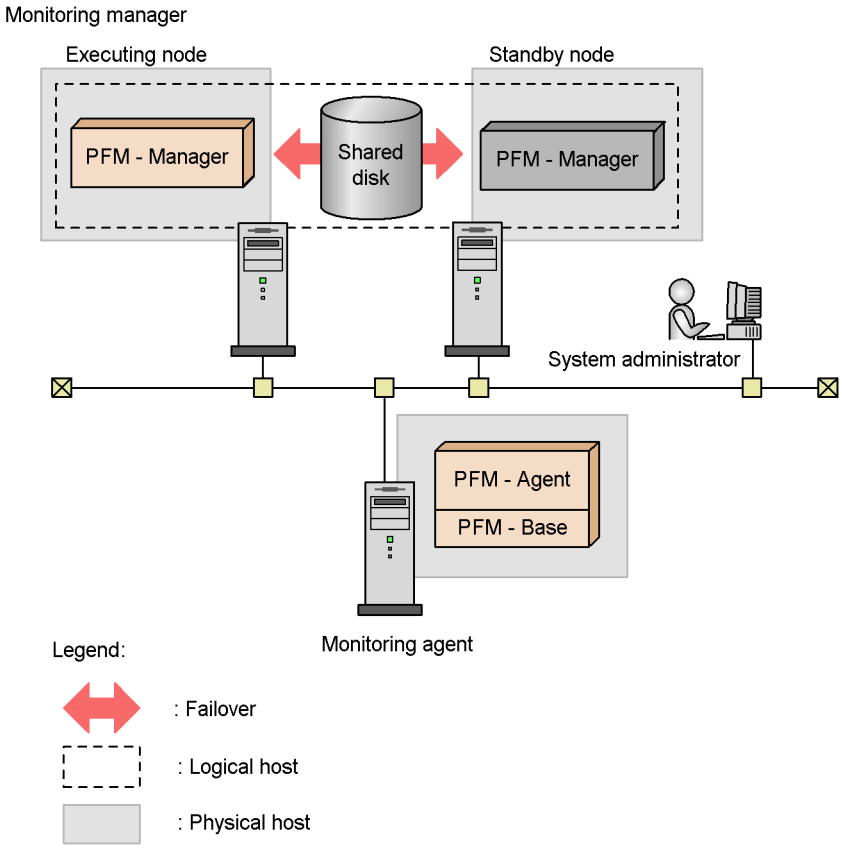
PFM - Manager can run on a logical host of a cluster system that has an active-standby configuration.

Even if a problem occurs on the executing node where PFM - Manager is executed, operation monitoring is continued by failing over to the standby node.

When PFM - Manager is used on a logical host, definition information and event data are stored on a shared disk and inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows the configuration when using PFM - Manager on a logical host.

Figure 9-3: Cluster configuration of PFM - Manager



Only a single instance of PFM - Manager can be executed at a time on a single node.

(b) Cluster configuration of PFM - Web Console

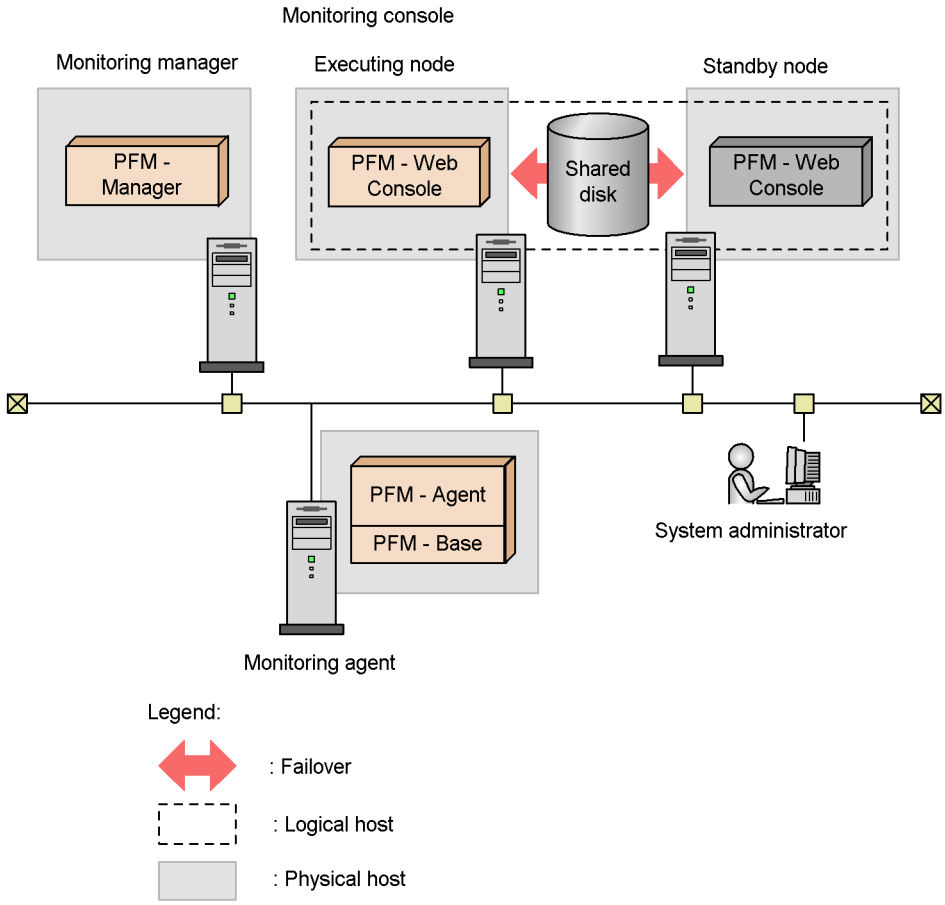
PFM - Web Console can run on a logical host of a cluster system that has an active-standby configuration.

Even if a problem occurs on the executing node where PFM - Web Console is executed, operation monitoring is continued by failing over to the standby node.

If PFM - Web Console is used on a logical host, bookmark definitions are stored on a shared disks so that such information can be inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows the configuration when using PFM - Web Console on a logical host.

Figure 9-4: Cluster configuration of PFM - Web Console



Only a single instance of PFM - Web Console can be executed at a time on a single node.

(c) Cluster configuration of PFM - Base

PFM - Base is compatible with cluster systems that have an active-active configuration. PFM - Base can be used on a logical host if located on the same logical host as PFM - Agent or PFM - RM.

(d) Cluster configuration of PFM - Agent

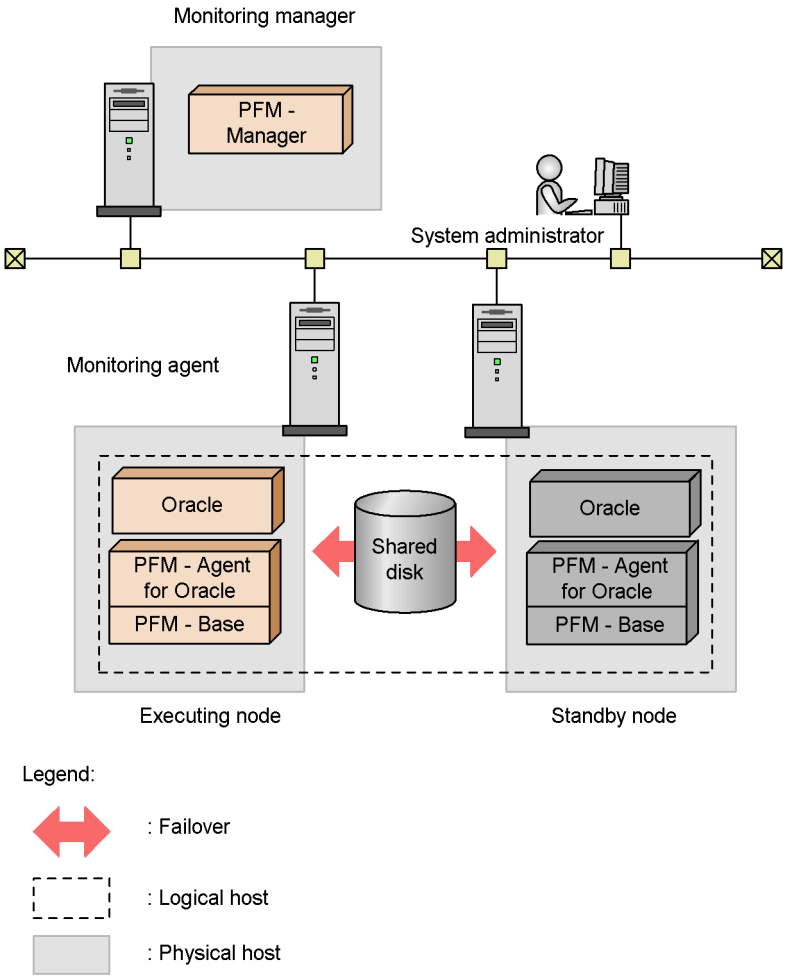
Different cluster systems support different PFM - Agents. When the program to be monitored is running in a logical host environment, only some types of PFM - Agents will be able to run in that logical host environment.

If PFM - Agent is used on a logical host, definition information and performance data

are stored on shared disks so that they can be inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows an example of a configuration that monitors an Oracle cluster system with PFM - Agent for Oracle on a logical host.

Figure 9-5: Cluster configuration for PFM - Agent (PFM - Agent for Oracle)



Supplemental information:

PFM - Agent is used in a configuration that is compatible with the application that is being monitored. Therefore, there are some PFM - Agents that are used on a logical host and others that are used on a physical host. For example, PFM - Agent for Oracle is used on a logical host since PFM - Agent for Oracle monitors Oracle

in a cluster configuration, on the other hand, PFM - Agent for Platform is used on a physical host to monitor the OSs on each node since PFM - Agent for Platform monitors OS performances. For details, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent manual.

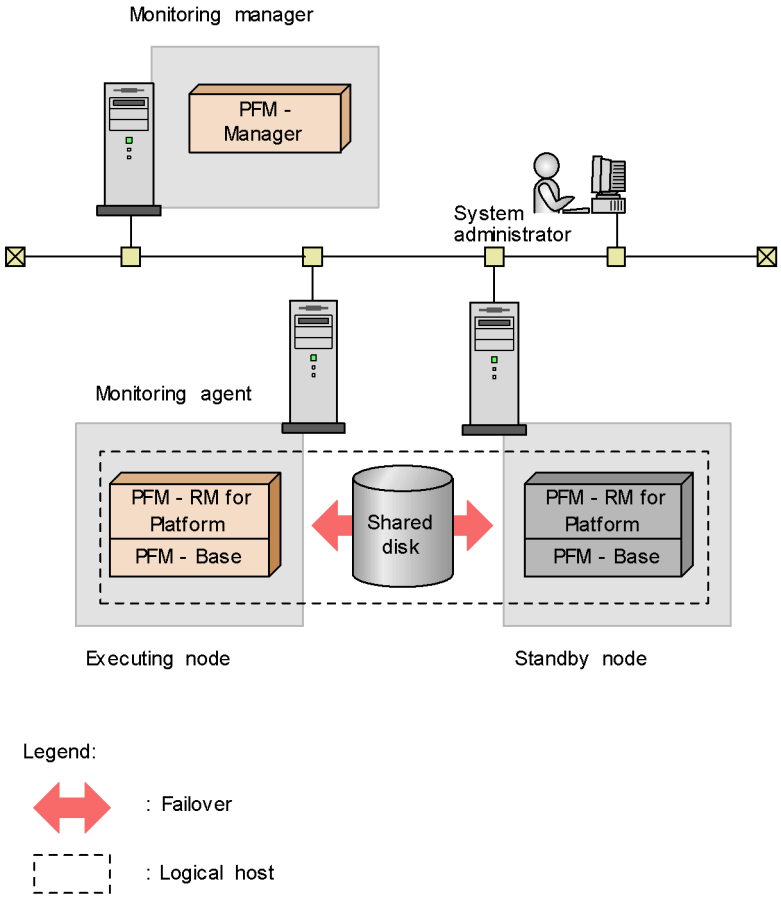
(e) Cluster configuration of PFM - RM

Different cluster systems support different PFM - RM products. Some PFM - RM products can also be used on a logical host. For details on whether the PFM - RM product you are using can be used in a cluster system, see the applicable PFM - RM manual.

If PFM - RM is used on a logical host, definition information and performance data are stored on the shared disks so that they can be inherited when a failover occurs. If there are multiple instances of Performance Management on a single logical host, each instance uses the same shared directory.

The following figure shows an example of the configuration when using PFM - RM for Platform on a logical host.

Figure 9-6: Cluster configuration of PFM - RM (PFM - RM for Platform)



(2) Examining the configuration in load-balancing cluster systems

This subsection describes the cluster configuration for Performance Management in load-balancing cluster systems.

(a) Cluster configuration of PFM - Manager

The PFM - Manager processing cannot be balanced across multiple nodes.

PFM - Manager must be used on a physical host or HA cluster system, rather than a load-balancing cluster system.

(b) Cluster configuration of PFM - Web Console

The PFM - Web Console processing cannot be balanced across multiple nodes.

PFM - Web Console must be used on a physical host or HA cluster system, rather than

a load-balancing cluster system.

(c) Cluster configuration of PFM - Base

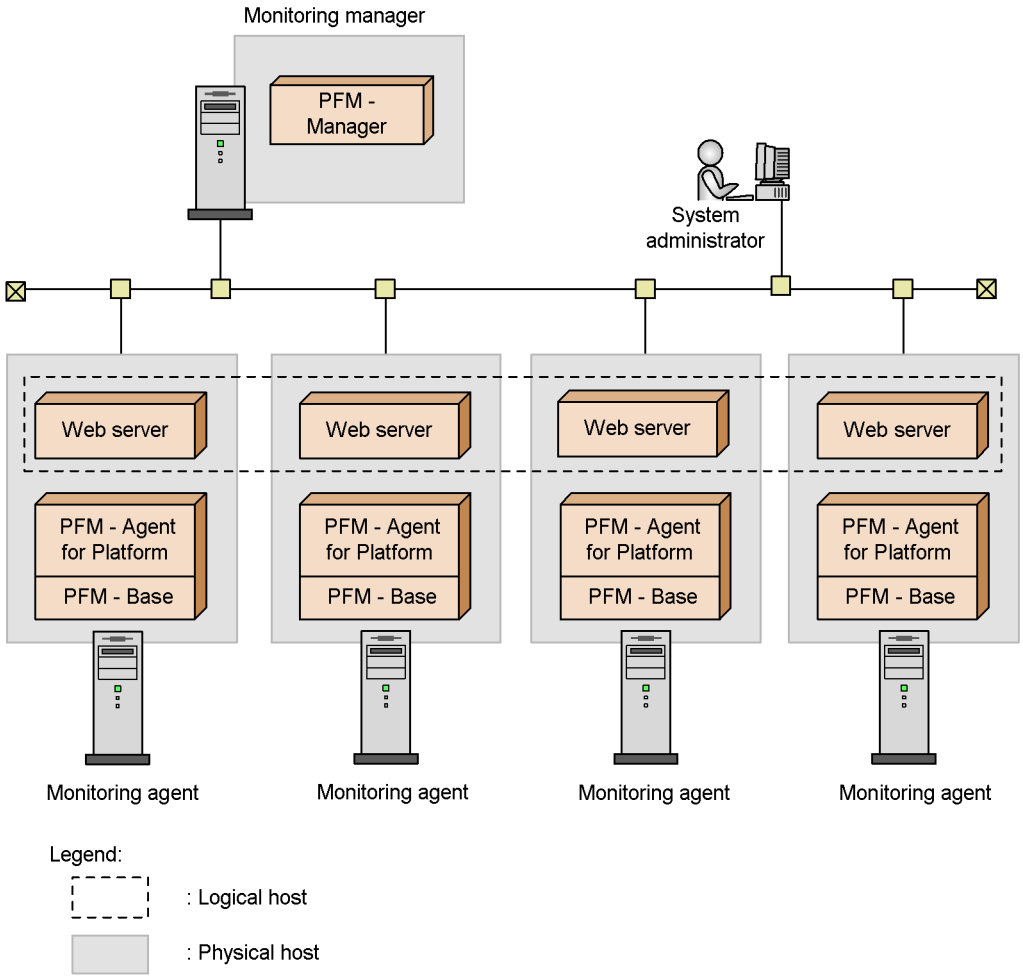
The configuration follows that of PFM - Agent or PFM - RM.

(d) Cluster configuration of PFM - Agent

This subsection describes how PFM - Agent for Platform is used on each node of a load-balancing cluster system.

PFM - Agent for Platform monitors OS performances. Therefore, even in a cluster system, PFM - Agent for Platform is executed on physical hosts to monitor the OSs on each physical host. PFM - Agent for Platform must be used in the same manner as a system that is not a cluster system. Even when used in a cluster system, PFM - Agent for Platform is not registered in the cluster software.

Figure 9-7: Cluster configuration of PFM - Agent (PFM - Agent for Platform)



For details on the cluster configuration of PFM - Agents, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent manual.

(e) Cluster configuration of PFM - RM

Depending on the PFM - RM product you are using, it might not be possible to use PFM - RM in a load-balancing cluster system. For details, see the chapters that describe operations on cluster systems in the appropriate PFM - RM manual.

9.1.3 Designing the network configuration

When Performance Management is used on a logical host, it is necessary to configure a network so that communication is possible by using logical host names and logical

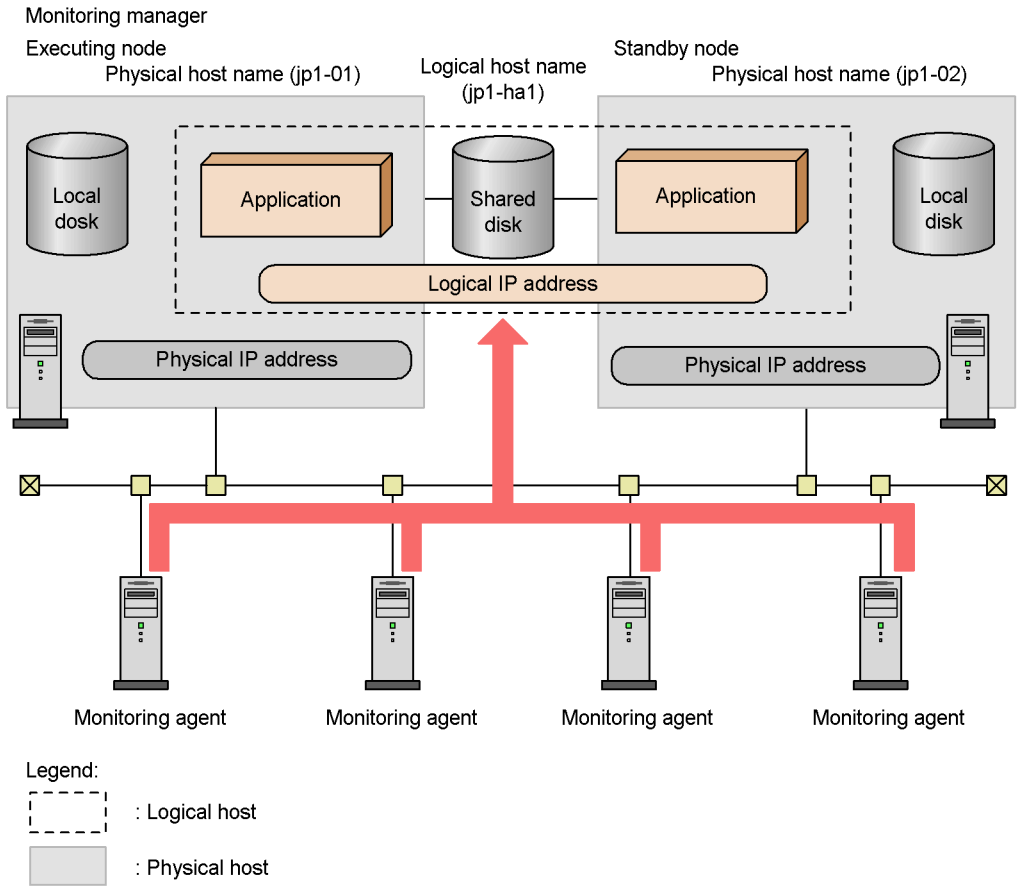
IP addresses.

A *logical host* is a logical node that is controlled by cluster software and a unit of failover. A logical host has a *logical host name* and a *logical IP address*. Applications store data on shared disks and communicate via logical IP addresses, so that they are not dependant on physical nodes and can perform failover.

A *physical host* is a physical node. The host name used by a physical host (the host name displayed when the `hostname` command is executed) is called the *physical host name*, and the IP address compatible with a physical host name is called the *physical IP address*.

The following figure shows an overview of physical and logical hosts.

Figure 9-8: Overview of physical and logical hosts



9.1.4 Designing the data configuration

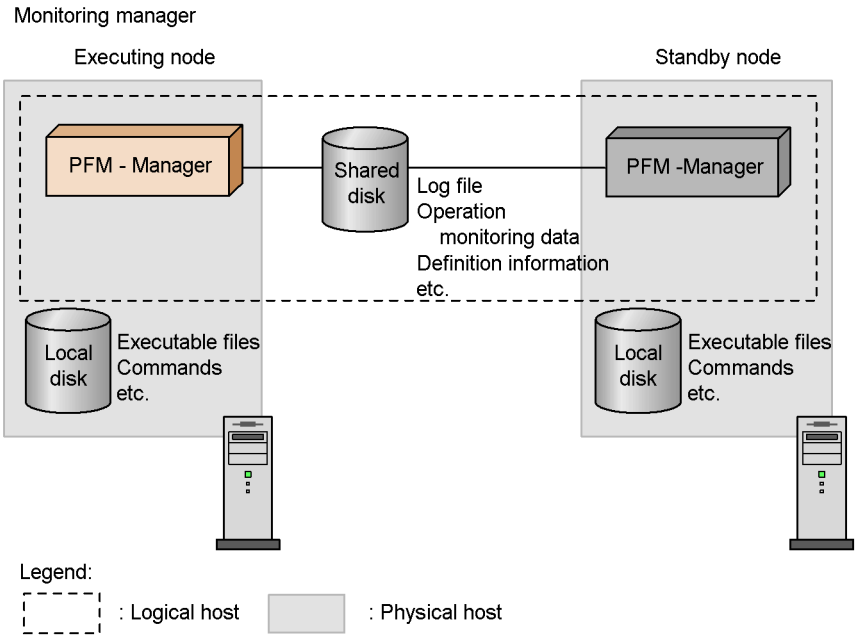
If Performance Management is used for a logical host, it is necessary to examine the data volume required for shared disks in addition to the volume required when using Performance Management on a non-cluster system on shared disks.

Each cluster system has a *shared disk* that is shared between the executing node and standby node when a failover occurs. In addition, each executing node and standby node has *local disks* that are specific to each physical host and cannot be taken over by a different node.

With Performance Management, when a logical host environment is set up, an *environment directory* is created on the shared disk. This environment directory stores the definition files and operation monitoring data required for switching nodes when a failover occurs. The execution files and commands required to run Performance Management are stored on local disks.

The following figure shows the data configuration for Performance Management when used on a logical host.

Figure 9-9: Data configuration for Performance Management when using a logical host



Supplemental information:

Some definition information and log files are located on local disks.

For details on the formula used to calculate the disk capacity required for logical host operation with Performance Management, see the sections that describe the exclusively occupied disk space when running on a cluster system in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

9.1.5 Operation design in cluster systems

Considerations for what security policy to use for managing Performance Management users and what items to monitor are the same as for non-cluster systems.

However, some naming rules for service names and process names, and some setting methods for executing actions on logical hosts when alarm events occur are different from those used in non-cluster systems. For details, see *9.6.1(3) Service names* and *9.6.6 Performing realtime operation monitoring by alarms in a cluster system*.

9.1.6 Designing the failover policy

When an error occurs in PFM - Agent or PFM - RM, and the node on which the program is running fails over, the business applications running on the logical host monitored by the PFM - Agent or PFM - RM might be affected. Therefore, you should decide whether nodes should fail over when a problem occurs in PFM - Agent or PFM - RM.

Supplemental information:

To avoid affecting business operations, you might use the following operation policy: "If a problem occurs in PFM - Agent or PFM - RM, the system will attempt to restart PFM - Agent or PFM - RM on that node, but the problem will not trigger a failover."

9.2 Configuration of a cluster system (in Windows)

This section describes the operations for setting up a Performance Management system in a cluster systems. The following topics are described in this section:

- PFM -Manager installation and setup
- PFM - Web Console installation and setup
- PFM -Manager unsetup and uninstallation
- PFM - Web Console unsetup and uninstallation

9.2.1 Before installation and setup

This subsection describes the items to check before installing and setting up Performance Management in a cluster system.

(1) Prerequisite conditions

The prerequisite conditions for using Performance Management in a cluster system are described below.

(a) Cluster system

Make sure that the following conditions are satisfied:

- The cluster system is controlled by cluster software.
- Settings are made so that the starting and stopping of Performance Management used on a logical host are controlled by cluster software.

Note:

Suppressing dialog boxes when errors occur

- Because a failover might not be performed if an application error dialog box is displayed in Dr. Watson, you need to suppress the display of error dialog boxes. However, note that, if error notification is suppressed, information acquisition when an application error occurs might be affected.
- If an application error occurs in Windows, a dialog box for reporting the error to Microsoft sometimes appears. If this dialog box is displayed, a failover might not be performed, therefore, you need to suppress such error notification.

  For details on how to do this, see the OS documentation.

(b) Shared disks

Make sure that the following conditions are satisfied:

- Each logical host has a shared disk, and the disk can be taken over by from the executing node by the standby node.
- Shared disks are physically connected to each node via Fibre Channel or SCSI. Configurations in which the shared disk is a network drive or disk replicated over a network are not supported.
- When a failover occurs, if some processes are still using the shared disks, make sure it is still possible to force shared disks offline via cluster software or by other means and perform a failover.
- If multiple Performance Management programs are executed on a single logical host, make sure the directory names for the shared disks are the same. For Store databases, make sure the storage destination can be changed to allow storage in a different directory on the same shared disk.

(c) Logical host name, logical IP address

Make sure that the following conditions are satisfied:

- There is a logical host name and corresponding logical IP address for each logical host, and switching from the executing node to the standby node can be performed.
- The logical host and logical IP address are set in the `hosts` file and on the name server.
- If using a DNS a logical host name is specified without a domain name, instead of by using a FQDN.
- Each physical host name and logical host name is unique within the system.

Notes regarding logical host names:

- Do not use a physical host name (a host name displayed using the `hostname` command) for a logical host name. Otherwise, normal communication processing might be prevented.
- Logical host names must consist of from 1 to 32 bytes alphanumeric characters.
- `localhost`, an IP addresses, or a hyphen (-) cannot be used for a logical host name.

(2) Checking the setup environment

In addition to the environment information normally required to set up Performance Management, the following information is required to set up Performance Management used on a logical host.

Table 9-1: Information required to set up PFM - Manager to be used on a logical host (in Windows)

Item	Example
Logical host name	`jp1-ha1`
Logical IP address	`172.16.92.100`
Shared disk	`S:\jp1`

If multiple instances of Performance Management that use a single logical host, each instance uses the directory of the same shared disk.

(3) Notes about upgrading when a logical host is used

To upgrade PFM - Manager on a logical host, you must place a shared disk online on either an executing or a standby node.

However, there is no need to place a shared disk online to upgrade PFM - Web Console in a cluster environment.

9.2.2 Installing and setting up PFM - Manager

This subsection describes the methods for installing and setting up PFM - Manager in a cluster system.

(1) Process flow for installation and setup

The following figure shows the process flow for installation and setup of PFM - Manager used on a logical host.

Figure 9-10: Process flow for installation and setup of PFM - Manager used on a logical host (in Windows)

Notes:

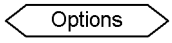
- When PFM - Manager in a logical host environment is set up, PFM - Manager on the physical host environment can no longer be executed. However, the Action Handler service can still be executed, because it uses PFM - Agent or PFM - RM in the physical host environment.

  When unsetup is performed on PFM - Manager in a logical host environment, PFM - Manager in the physical host environment can once again be executed.
- When PFM - Manager is set up in a logical host environment, the logical host environment inherits the PFM - Manager definitions from the physical host environment. However, the content of the Store database is not inherited. If unsetup is performed on PFM - Manager in the logical host environment, the definitions for the logical host environment and the Store database are deleted, and therefore switching to the physical host environment is not possible.
- Do not manually set `JPC_HOSTNAME` as an environment variable, because `JPC_HOSTNAME` is used by Performance Management as an environment variable. If you specify this setting, Performance Management will not run correctly.
- For PFM - Manager version 09-00 or later, when you set up a new instance of PFM - Manager in a logical host environment, the settings of the health check function in the physical host environment are inherited by the logical host environment. If necessary, you must modify the settings of the health check function.
- In a logical host environment, the function for setting monitoring-host names cannot be used. The `jpccomm.ini` file on a logical host is ignored, and the host name for the logical host is used.

The installation and setup procedures for PFM - Manager and the setting procedures for the cluster software are explained below.

In the procedure explanation, the image 

indicates items to be performed on the executing node, and the image 

indicates items to be performed on the standby node. In addition, the image 

indicates setup items that are either required depending on the environment or can be performed if you want to set a value other than the default settings.

(2) Installation procedure 

Perform a new installation of PFM - Manager on the executing node and the standby

node. The installation procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

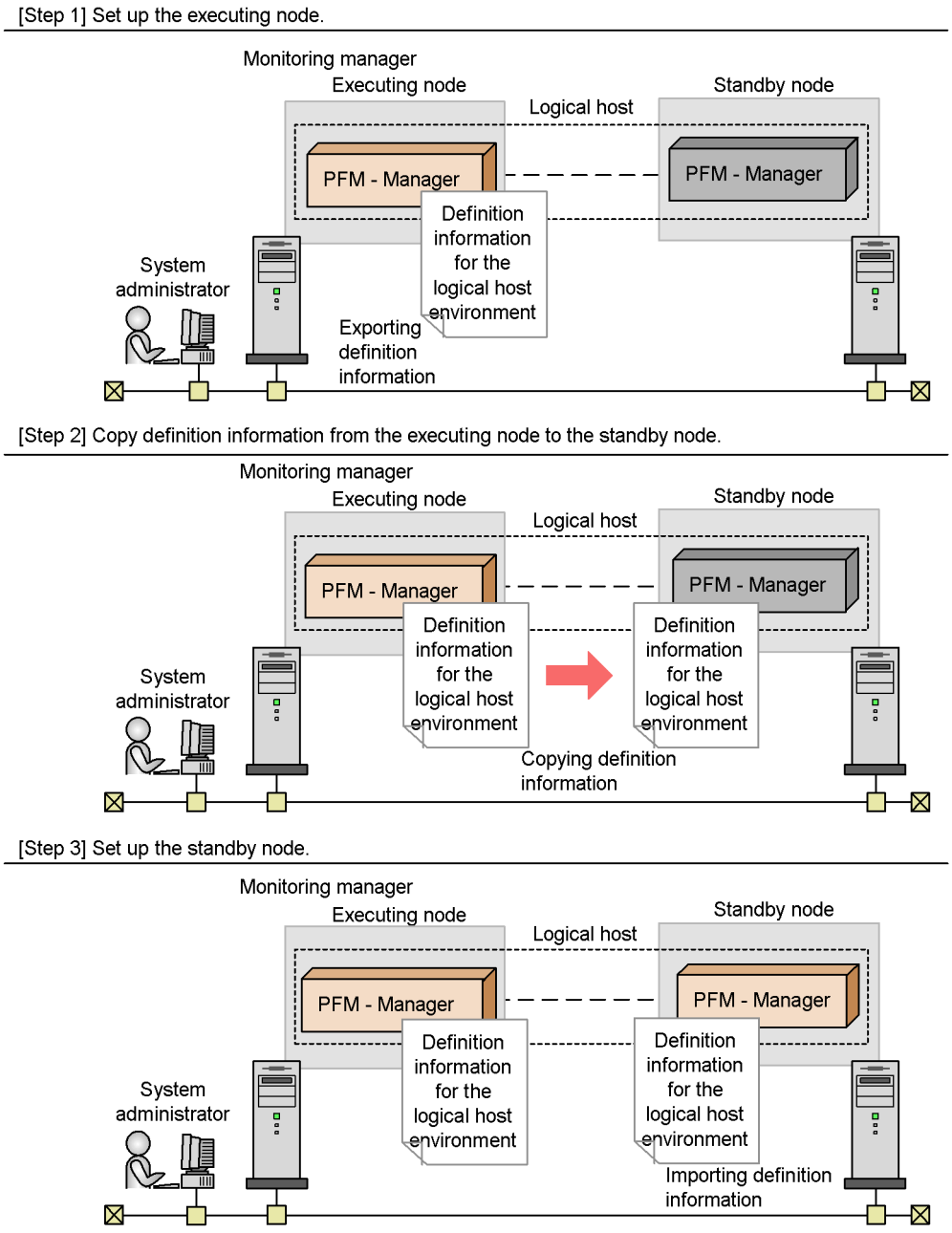
Note:

The installation destination is the local disk. Do not install PFM - Manager on the shared disk.

(3) Setup procedure

Perform PFM - Manager setup on the executing node first. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the setup content from the executing node to the standby node.

Figure 9-11: Method for applying the content set up on the executing node to the standby node



Each setup procedure is explained below.

(a) Performing an additional setup for PFM - Agent or PFM - RM information

Executing Standby Options

To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Manager for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

The setup procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

Note:

If you add another PFM - Agent or PFM - RM to the same host as PFM - Manager, an additional setup is not required.

(b) Making sure the shared disk is online

Executing

Make sure that the shared disk is online on the executing node. If the shared disk is not online, place it online by using the cluster software and the volume manager.

(c) Setting up a logical host for PFM - Manager

Executing

Set up the logical host environment for PFM - Manager on the executing node. Before performing setup, stop all the Performance Management programs and services throughout the entire system.

To set up a logical host:

1. Create a logical host environment.

   Execute the `jpcconf ha setup` command to create a logical host environment for PFM - Manager.

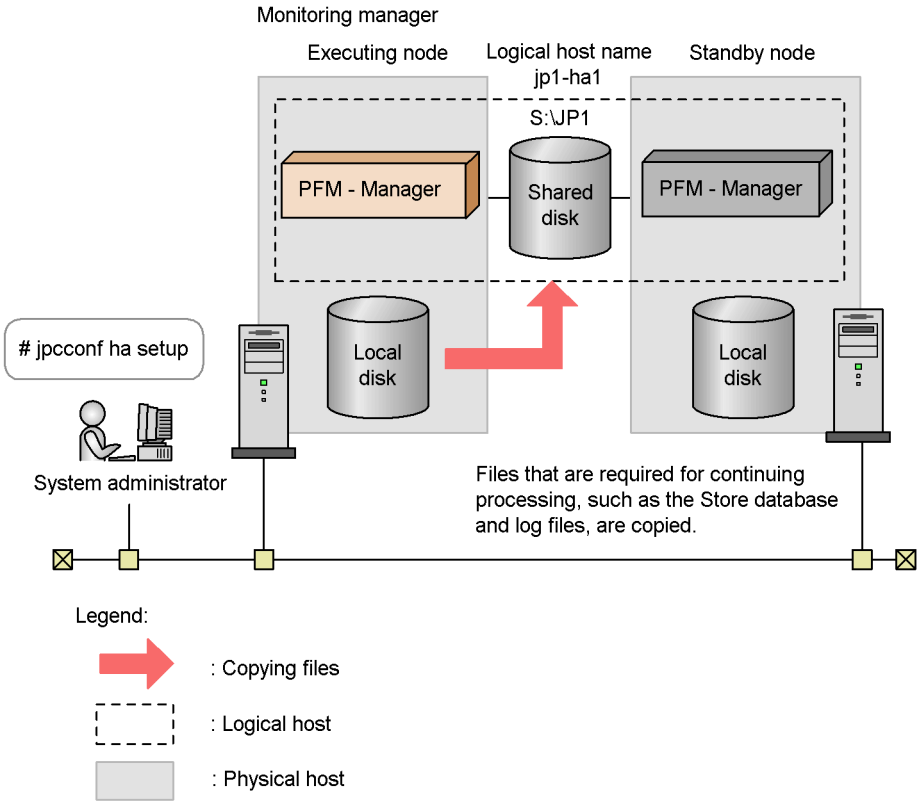
   Use `-lhost` to specify the logical host name. For DNS operations, specify a logical host name that does not include a domain name. Specify the `-d` environment directory name for the directory name of the shared disk.

   For example, execute the following command to set up a logical host with `jp1-ha1` as the logical host name and `S:\jp1` as the environment directory.

```
jpcconf ha setup -key Manager -lhost jp1-ha1 -d S:\jp1
```

When this command is executed, the `jp1pc` directory is created under `S:\jp1`, and the files required in the logical environment are copied to the environment directory. The following figure shows an example.

Figure 9-12: Execution example of the jpcconf ha setup command



When the command is executed, the required data is copied from the local disk of the executing node to the shared disk, and the settings required for use on the logical host are performed.

For details on the `jpcconf ha setup` command, see the chapters that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Check the settings for the logical host environment.

   Execute the `jpcconf ha list` command to check the settings for the logical host, and make sure that the logical host environment that has been created is

correct.

```
jpcconf ha list -key all
```

An example of executing this command is as follows:

```
C:\>jpchasetup list all

Logical Host Name      Key     Environment Directory                    [Instance Name]
---------------------- ------- ---------------------------------------- ----------------------------
jp1-ha1                mgr     "S:\jp1\jp1pc"

KAVE05136-I The logical host startup information listing ended normally.
```

For details on the `jpcconf ha list` command, see the chapters that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

(d) Performing a setup for a logical host of PFM - Agent or PFM - RM

Executing Options

This procedure is required only when PFM - Agent or PFM - RM needs to be set up on the same logical host as PFM - Manager.

For details on the setup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

(e) Specifying network settings

Executing

To use the logical host names for communications between PFM - Manager and PFM - Web Console, add the following line to the *environment-directory*`\jp1pc\mgr\viewsvr\jpcvsvr.ini` file.

`java.rmi.server.hostname=`*logical-host-name*

For details on host names used for communications between PFM - Manager and PFM - Web Console, see the sections that describe port numbers in an appendix of the manual *Job Management Partner 1/Performance Management Reference*.

In addition, use the following procedure when changing IP addresses and port numbers according to the network configuration:

- Setting the IP address

  Options

  To set the IP addresses, directly edit the content of the `jpchosts` file. If you have

edited the `jpchosts` file, copy the file from the executing node to the standby node.

For details on setting IP addresses, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Setting port numbers Options

This procedure is necessary only when running Performance Management in a network environment with a firewall.

For Performance Management communications via a firewall, use the `jpcconf port define` command to set a port number.

For example, execute the following command to set all port numbers for services that exist on the host with the logical host name `jp1-ha1` specified in the fixed values.

```
jpcconf port define -key all -lhost jp1-ha1
```

When this command is executed, definitions of the port numbers and service names (TCP service name beginning with `jp1pc` by default) for Performance Management are added to the services file.

For details on setting port numbers, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

For details on the `jpcconf port define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(f) Changing the log file size Options

The operating status of Performance Management is output to a dedicated log file called the *common message log*. By default, the common message log uses two 2,048-KB files. This setting is required only if you want to change this file size.

For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(g) Specifying settings for the authentication mode Options

This setting is required only if you want to change the authentication mode of Performance Management from PFM authentication mode to JP1 authentication

mode.

For details, see *2. Managing User Accounts*.

(h) Changing the storage locations of event data

Options

The settings below are required if you want to change the storage destination, backup destination, or export destination of the event data managed by PFM - Manager.

By default, event data is stored in the following locations:

- Data storage folder: *environment-directory*`\jp1pc\mgr\store\`
- Backup folder: *environment-directory*`\jp1pc\mgr\store\backup\`
- Export folder: *environment-directory*`\jp1pc\mgr\store\dump\`

For details on how to change a destination, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(i) Specifying settings for action log output

Options

This setting is required if you want to output an action log when an alarm is issued. An action log is log information output in conjunction with the alarm function, when an aspect of the system (such as the system load) exceeds a threshold. For details on how to set this option, see the section describing action log output in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(j) Configuring the health check function

Executing Options

To configure the health check function:

1. Check the settings of the health check function.

   Execute the following command on the PFM - Manager host on the executing node to display the setting of the health check function.

   ```
   jpcconf hc display
   ```

   When the command is executed, the setting for the health check function appears as follows:

   - If the health check function is enabled: `available`
   - If the health check function is disabled: `unavailable`

   For details on the `jpcconf hc display` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance*

Management Reference.

2. Change the setting of the health check function.

   Execute the following command on the PFM - Manager host on the executing node to set up the health check function, if necessary.

   - To enable the health check function: `jpcconf hc enable`
   - To disable the health check function: `jpcconf hc disable`

   For details on the `jpcconf hc enable` and `jpcconf hc disable` commands, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

(k) Exporting the logical host environment definitions

Executing

When a logical host environment for PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file. To set up a different instance of Performance Management on the same logical host, perform an export after all setup procedures are completed.

To export the environment definitions:

1. Execute the `jpcconf ha export` command.

   Export the logical host environment definitions to the desired file.

   For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file.

   ```
   jpcconf ha export -f lhostexp.conf
   ```

   If the health check function is enabled for the PFM - Manager in the logical host environment you are exporting, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be exported.

   For details on the `jpcconf ha export` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(l) Copying the file containing the logical host environment definitions to the standby node

Executing Standby

Copy the file that has been exported in step (f) from the executing node to the standby node, so that it will be applied on the standby node.

Next, use operations of the cluster software or volume manager software to place the shared disk online, and finish the operations on the executing node. If this shared disk

will continue to be used, it is not necessary to take it offline.

(m) Importing the file containing the logical host environment definitions

Standby

Import the exported file copied from the executing node to the standby node.

To import the exported file containing the logical host environment definitions:

1. Execute the `jpcconf ha import` command.

   Import the logical host environment definitions to the standby node.

   For example, execute the following command if the export file name is `lhostexp.conf`.

   ```
   jpcconf ha import -f lhostexp.conf
   ```

   When the `jpcconf ha import` command is executed, the environment settings for the standby node are changed to the same environment as for the executing node. Therefore, the necessary settings are made to use PFM - Manager on a logical host.

   If the health check function is enabled for the PFM - Manager in the logical host environment you are importing, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be imported.

   For details on the `jpcconf ha import` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Check the settings for the logical host environment.

   Execute the `jpcconf ha list` command in the same manner as for the executing node, to check the settings of the logical host.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

   For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Cluster software setting procedure

Cluster software settings are required for both the executing node and the standby node.

The procedure is as follows:

(a) Registering PFM - Manager in the cluster software

Executing Standby

To use PFM - Manager on a logical host, register it in the cluster software, and set the cluster software to control the starting and stopping of PFM - Manager.

For details on how to register PFM - Agents or PFM - RM in the cluster software, see the chapters that describe operations in cluster systems in the appropriate PFM - Agent or PFM - RM manual.

The setting contents for registering PFM - Manager in the cluster software are described below by using items for registration in Windows MSCS as examples. For PFM - Manager, register the services listed in the following table in the cluster.

Table 9-2: PFM - Manager services to be registered in the cluster software

No.	Name	Service name	Dependencies
1	PFM - Name Server [*LHOST*]	JP1PCMGR_PN [*LHOST*]	IP address resources Physical disk resources#
2	PFM - Name Server [*LHOST*]	JP1PCMGR_PN [*LHOST*]	#1 cluster resources
3	PFM - Master Store [*LHOST*]	JP1PCMGR_PS [*LHOST*]	#2 cluster resources
4	PFM - View Server [*LHOST*]	JP1PCMGR_PP [LHOST]	#5 cluster resources
5	PFM - Correlator [*LHOST*]	JP1PCMGR_PE [*LHOST*]	#3 cluster resources
6	PFM - Trap Generator [*LHOST*]	JP1PCMGR_PC [*LHOST*]	#5 cluster resources
7	PFM - Action Handler [*LHOST*]	JP1PCMGR_PH [*LHOST*]	#3 cluster resources
8	PFM - Agent Store for HealthCheck [*LHOST*]	JP1PCAGT_0S [*LHOST*]	#3 cluster resources
9	PFM - Agent for HealthCheck [*LHOST*]	JP1PCAGT_0A [*LHOST*]	#8 cluster resources

#: The shared disk drive that hosts the logical host environment directory created according to *(c)* in *(3)* above.

Place the logical host name wherever [*LHOST*] appears. The following is an example for a Name Server service for which the logical host name is `jp1-ha1`:

- Name

  `PFM - Name Server [jp1-ha1]`

- Service name

  `JP1PCMGR_PN [jp1-ha1]`

For MSCS, these services are registered as MSCS resources. The settings for each resource are as follows. The setting items for MSCS are indicated by [ ].

- [**Resource Type**] is registered as `General-Purpose Service`.
- Set [**Name**], [**Dependency**], and [**Service Name**] as shown in *Table 9-2 PFM - Manager services to be registered in the cluster software*.

  [**Name**] is the name for displaying the service, and [**Service Name**] is the name for specifying the service to be controlled by MSCS.

  For example, when you register the `PFM - Master Store [LHOST]` service into the cluster software, because the `PFM - Master Store [LHOST]` service must have a dependent relationship with the No. 2 cluster resource, configure the `PFM - Master Store [LHOST]` service so that it has a dependent relationship with the `PFM - Master Manager [LHOST]` service.

- Do not set [**Startup Parameter**] and [**Duplicate Registry**].
- Specify the settings for the [**Details**] tab in Properties according to whether a failover is performed when a problem occurs in Performance Management.

  For example, in order to enable failovers when problems occur in PFM - Manager, check the check boxes for [**Restart**] and [**Apply to Group**], and then set [**Threshold**], which indicates the number of times to attempt restarts, to `3`, as a guide.

Note:

Starting and stopping of services registered on a cluster are controlled by the cluster software. Therefore, set [**Startup Type**] to [**Manual**] so that automatic startup is not performed when the OS starts up on the executing node and the standby node. Services are set to [**Manual**] immediately after setup by the `jpcconf ha setup` command. In addition, do not use the following command to perform a forced stop.

`jpcspm stop -key all -lhost` *`logical-host-name`* `-kill immediate`

(b) Checking starting and stopping from the cluster software

Executing

Standby

Perform operations to start and stop PFM - Manager from the cluster software in each

node, and make sure that the operations are normal.

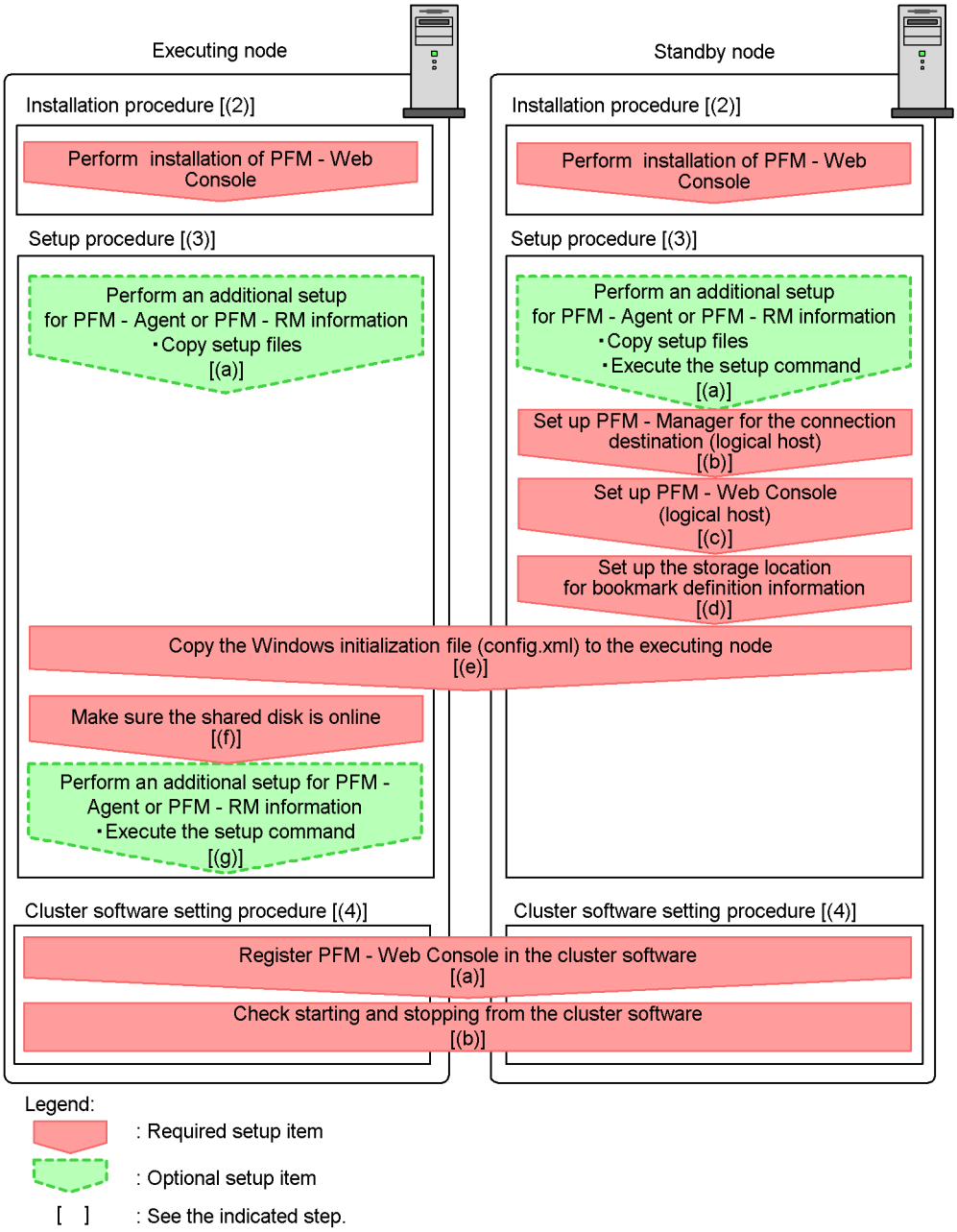
9.2.3 Installing and setting up PFM - Web Console

This subsection describes the methods for installing and setting up PFM - Web Console in a cluster system.

(1) Process flow for installation and setup

The following figure shows the process flow for installation and setup of PFM - Web Console used on a logical host.

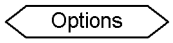
Figure 9-13: Process flow for installation and setup of PFM - Web Console used on a logical host



The procedures for installation, setup, and cluster software setting are explained below.

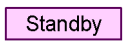
In the procedure explanation, the image 

indicates the items to be performed on the executing node, and the image 

indicates the items to be performed on the standby node. In addition, the image 

indicates the setup items required depending on the environment, and the optional setup items for when changing the default settings.

(2) Installation procedure 



Perform a new installation of PFM - Web Console on the executing node and the standby node. The installation procedure is the same as for a non-cluster system.

For details on the installation procedure, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Notes:

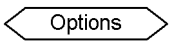
- The installation destination is the local disk. Do not perform installation on the shared disk.
- Install each PFM - Web Console for both the executing node and the standby node in a location with the same path.

(3) Setup procedure

When using PFM - Web Console on a logical host, the environment configurations on the executing node and the standby node have to be the same.

Each of the setup types for PFM - Web Console is explained below.

(a) Performing an additional setup for PFM - Agent or PFM - RM information 



To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Web Console for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Notes:

- You do not need to register PFM - Agent or PFM - RM if you add the same version of PFM - Agent or PFM - RM with the same product ID to a Performance Management system in which the PFM - Agent or PFM - RM information has already been registered.
- Set up the latest version of PFM - Agent or PFM - RM if you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host.

To perform an additional setup for the agent information in PFM - Web Console, see the process flow shown in Figure 9-13.

To register the agent information in PFM - Web Console:

1. Copy the setup file. Executing Standby

   Copy the PFM - Agent or PFM - RM setup files to the following locations on the PFM - Web Console executing and standby nodes.

   pfm - web console-installation-folder\setup

   The setup file to be copied and the relevant procedure are the same as for when an additional setup is performed for PFM - Manager. For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

2. Execute the setup command on the standby node. Standby

   Execute the jpcwagtsetup command on the standby node, and register the agent information.

   Execute the command as follows:

   ```
   jpcwagtsetup
   ```

   For details on the jpcwagtsetup command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

Supplemental information:

When you register the agent information of PFM - Agent or PFM - RM in PFM - Web Console, you must restart PFM - Web Console. However, the restart after step 2 is not required because PFM - Web Console restarts when a failover occurs.

(b) Setting up PFM - Manager for the connection destination (logical host)

Standby

On the standby node, set the IP address and host name for PFM - Manager to which PFM - Web Console connects in the Windows initialization file (`config.xml`). If the PFM - Manager to connect is running on the cluster system, set the logical IP address or the logical host name.

To set up PFM - Manager for the connection destination:

1. Open the Windows initialization file (`config.xml`).

   Use a text editor or XML editor to open the *installation-folder*`\conf\config.xml` file.

2. Set the IP address or host name for the PFM - Manager host to be connected.

   Enter the following tag immediately after the `<vserver-connection>` tag within the `<vsa>` tag:

   `<param name="host" value="`*IP-address-or-host-name*`"/>`

   For example, if the IP address of the PFM - Manager host to be connected is *10.210.24.56*, make the following settings:

```
    <vsa>
        <vserver-connection>
            <param name="host" value="10.210.24.56"/>
            <!-- The host computer name to which PFM View
Server uses.
                 Specifiable values: 1024 to 65535
                 Default           : 22286
             -->
            <param name="port" value="22286"/>
        </vserver-connection>
```

3. Save the Windows initialization file (`config.xml`) edited in step 2.

Note:

If areas other than those specified are changed in the Windows initialization file (`config.xml`), PFM - Web Console might not operate correctly.

(c) Setting up PFM - Web Console (logical host)

Standby

Set the logical IP address or logical host name for PFM - Web Console in the Windows initialization file (`config.xml`) on the standby node.

To set a logical host for PFM - Web Console:

1. Open the Windows initialization file (`config.xml`).

   Use a text editor or XML editor to open the *installation-folder*`\conf\config.xml` file.

2. Set the logical IP address or logical host name for the PFM - Web Console host.

   Enter the following tag in the `<vserver-connection>` tag within the `<vsa>` tag:

   ```
   <param name="ownHost"
   value="logical-IP-address-or-logical-host-name"/>
   ```

   For example, if the logical IP address of the PFM - Web Console host is *10.210.26.18*, make the following settings:

   ```
       <vsa>
           <vserver-connection>
               <param name="host" value="10.210.24.56"/>
               <!-- The host computer name to which PFM View
   Server uses.
                    Specifiable values: 1024 to 65535
                    Default           : 22286
               -->
               <param name="port" value="22286"/>
               <param name="ownHost" value="10.210.26.18"/>

          </vserver-connection>
   ```

3. Save the Windows initialization file (`config.xml`) edited in step 2.

Note:

If areas other than those specified are changed in the Windows initialization file (`config.xml`), PFM - Web Console might not operate correctly.

(d) Setting up the storage location for bookmark definition information

Standby

Set the folder to store the bookmark definition information in the Windows initialization file (`config.xml`) on the standby node. Specify an installation folder on the shared disk to ensure switching for the bookmark definition information when a failover occurs.

To set the storage location for bookmark definition information:

1. Open the Windows initialization file (config.xml).

   Use a text editor or XML editor to open the *installation-folder*\conf\config.xml file.

2. Set the folder for storing the bookmark definition information.

   Set the installation folder in the <bookmark> tag immediately after the <format> tag within the <vsa> tag in the Windows initialization file (config.xml).

   The installation folder that has been set will be automatically created when the PFM - Web Console service starts.

   For example, use the following setting to make *environment-directory*\jp1pcWebCon\common\bookmarks the installation folder.

```
</format>

<bookmark>
<!-- The directory where bookmark repository is stored.
Default : <install directory>\bookmarks -->
<param name="bookmarkRepository"
value="environment-directory\jp1pcWebCon\common\bookmarks"/>
</bookmark>

</vsa>
```

3. Save the Windows initialization file (config.xml) edited in step 2.

Note:

If areas other than those specified are changed in the Windows initialization file (config.xml), PFM - Web Console might not operate correctly

(e) Copying the Windows initialization file (config.xml) to the executing node

Standby Executing

Copy the Windows initialization file (config.xml) edited in (b), (c), and (d) to the executing node.

Copy the file to the following location on the executing node:

installation-folder\conf

(f) Make sure the shared disk is online Executing

Make sure that the shared disk is online on the execution node. If the shared disk is not

online, place it online through the operation of the cluster software and the volume manager.

(g) Performing an additional setup for PFM - Agent or PFM - RM information

Executing Options

Use the setup files copied in (a) to perform an additional setup of the agent information for PFM - Agent or PFM - RM on the execution node.

To add the PFM - Agent information:

1. Stop the PFM - Web Console services on the executing node.

   Use the `jpcwstop` command to stop the services if the PFM - Web Console services are not registered with the cluster software.

   When making changes to the Performance Management configuration such as adding PFM - Agent or PFM - RM after the services are registered with the cluster software, use the cluster software to stop the services. For details on changing the configuration of the cluster system, see *9.3 Changing the cluster system configuration (in Windows)*.

2. Execute the setup command on the executing node.

   Execute the command as follows:

   ```
   jpcwagtsetup
   ```

   For details on the `jpcwagtsetup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

3. Start the PFM - Web Console service on the executing node.

   Start the PFM - Web Console services stopped in step 1.

(4) Cluster software setting procedure

Set PFM - Web Console in the cluster software. Perform this setting in both the executing node and the standby node.

The procedure is as follows:

(a) Registering PFM - Web Console in the cluster software

Executing Standby

To use PFM - Web Console in a logical host environment, register it in the cluster software, and then set the cluster software to control the starting and stopping of PFM - Web Console.

The setting contents for registering PFM - Web Console in the cluster software are described below by using items for registration in Windows MSCS as examples. For PFM - Web Console, perform an additional registration of the services listed in the following table in the same cluster group as for PFM - Manager.

Table 9-3: PFM - Web Console services to be registered in the cluster software

No.	Name	Service name	Dependencies	Startup parameter
1	PFM - Web Console	PFM-WebConsole	IP address resources Physical disk resources#	`--ntservice` (Two hyphens are required.)
2	PFM - Web Service	PFM-WebService	#1-1 cluster resources (PFM - Web Console)	`--ntservice` (Two hyphens are required.)

#: The shared disk drive that hosts the logical host environment directory created according to *(d)* in *(4)* above.

For MSCS, these services are registered as MSCS resources. The settings for each resource are as follows. The setting items for MSCS are indicated by [ ].

- [**Resource Type**] is registered as `General-Purpose Service`.
- Set [**Name**], [**Dependency**], [**Service Name**], and [**Startup Parameter**] as shown in *Table 9-3 PFM - Web Console services to be registered in the cluster software*.

  [**Name**] is the name for displaying the service, and [**Service Name**] is the name for specifying the service to be controlled by MSCS.
- Do not set [**Duplicate Registry**].
- Select [**Restart**] on the [**Details**] tab in Properties. Set [**Threshold**] (the number of times to attempt restarts) to `3`, as a guide.

Note:

Starting and stopping of services registered on a cluster are controlled by the cluster software. Therefore, set [**Startup Type**] to [**Manual**] so that automatic startup is not performed when the OS starts up on the executing node and the standby node.

(b) Checking starting and stopping from the cluster software

Executing

Standby

Perform operations to start and stop PFM - Web Console in each node from the cluster software, and make sure that the operations are normal.

9.2.4 Installing an upgrade for PFM - Agent or PFM - RM

To install an upgrade for PFM - Agent or PFM - RM in a physical host environment where PFM - Agent, PFM - RM, or PFM - Manager is running in a logical host environment:

1. Use the cluster software to stop all of the PFM services on each logical host.
2. Use the `jpcspm stop -key jp1pc` command to stop all of the PFM services on both the executing and standby physical hosts.
3. Install PFM - Agent or PFM - RM on each applicable executing host by overwriting the previous installation.
4. Install PFM - Agent or PFM - RM on each applicable standby host by overwriting the previous installation.
5. Set up Performance Management so that it can run.
6. Use the cluster software to start all of the PFM services on each logical host.
7. Use the cluster software to start all of the PFM services on both the executing and standby physical hosts.

For details on PFM - Agent-specific or PFM - RM-specific considerations, see the corresponding PFM - Agent or PFM - RM manual and the *Release Notes*.

9.2.5 Unsetup and uninstallation of PFM - Manager

This subsection describes the methods for performing unsetup and uninstallation of PFM - Manager in a cluster system.

(1) Before unsetup and uninstallation

The following describes notes on performing unsetup and uninstallation of PFM - Manager:

Notes regarding the order of unsetup:

PFM - Manager is required to execute PFM - Agent or PFM - RM. Therefore, when performing unsetup on PFM - Manager, it is necessary to consider its relationship with PFM - Agent or PFM - RM in the system and determine the work order for unsetup. The work order when unsetup is required is the same as the order for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/*

Performance Management Planning and Configuration Guide.

Notes on stopping of services:

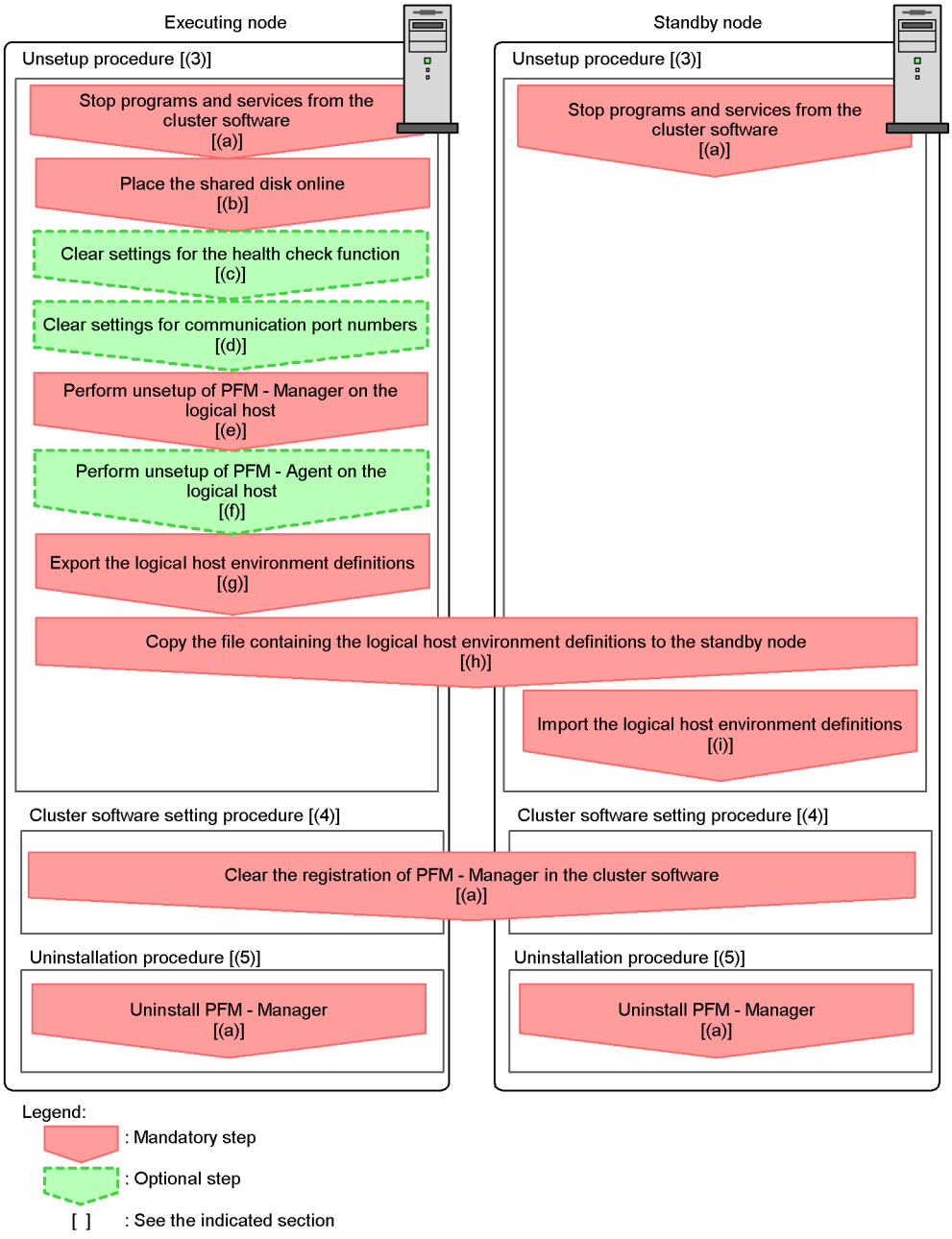
Stop all Performance Management programs and services running on the executing nodes and standby nodes on which unsetup is to be performed. Also, stop all PFM - Agent services across the Performance Management system connected to the PFM - Manager for which unsetup will be performed. For details on how to stop services, see *1. Starting and Stopping Performance Management*.

(2) Process flow for unsetup and uninstallation

The process flow for unsetup and uninstallation for PFM - Manager used on a logical host is explained below.

The following figure shows the process flow for uninstallation and unsetup.

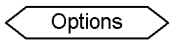
Figure 9-14: Process flow for unsetup and uninstallation of PFM - Manager used on a logical host (in Windows)



Next, the unsetup procedures, procedures for clearing cluster software settings, and uninstallation procedures for PFM - Manager and the setting procedures for cluster software are explained below.

In the procedure explanation, the image 

indicates the items to be performed on the executing node, and the image 

indicates the items to be performed on the standby node. In addition, the image 

indicates the setup items required depending on the environment, and the optional setup items for when changing the default settings.

(3) Unsetup procedure

First, perform unsetup on the executing node. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the unsetup content from the executing node to the standby node.

The procedure is as follows:

(a) Stopping from the cluster software 

Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

(b) Making sure the shared disk is online 

Make sure that the shared disk is online on the executing node. If the shared disk is not online, place it online through the operation of cluster software and the volume manager.

(c) Clearing settings for the health check function 

Execute the following command on the PFM - Manager host on the executing node to clear the settings for the health check function.

```
jpcconf hc disable
```

For details on the `jpcconf hc disable` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(d) Clearing settings for communication port numbers 

This procedure is required only when port numbers have been set using the `jpcconf`

`port define` command during the setup in an environment with a firewall.

To clear settings for communication port numbers:

1. Clear the settings for communication port numbers.

   Execute the `jpcconf port define` command to clear the settings for communication port numbers.

   For example, execute the following command to clear all the settings for port numbers for services that exist on the host with the logical host name `jp1-ha1`.

   ```
   jpcconf port define -key all -lhost jp1-ha1
   ```

   The `jpcconf port define` command is used to set the port numbers that are used for communications by PFM - Manager on the logical host or by other Performance Management programs. When entering a port number, a value of `0` will clear the setting. In addition, when this command is executed, the port numbers and service names (service names starting with `jp1pc` by default) for Performance Management defined in the services file are deleted.

   For details on the `jpcconf port define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(e) Performing unsetup of a logical host for PFM - Manager

Executing

To perform unsetup of a logical host for PFM - Manager:

1. Check the logical host settings.

   Check the current settings before performing unsetup on the logical host environment. Check the logical host name and shared disk path.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

   An example of executing this command is as follows:

```
C:\>jpchasetup list all

Logical Host Name          Key      Environment Directory                          [Instance Name]
-------------------------- -------- ---------------------------------------------- ----------------------------
jp1-ha1                    mgr      "S:\jp1\jp1pc"

KAVE05136-I The logical host startup information listing ended normally.
```

For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Delete the logical host environment for PFM - Manager.

   When the `jpcconf ha unsetup` command is executed, the settings for starting PFM - Manager on the logical host are deleted. In addition, the files for the logical host on the shared disk are also deleted. Execute the command as follows:

   ```
   jpcconf ha unsetup -key Manager -lhost jp1-ha1
   ```

   For details on the `jpcconf ha unsetup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

   Note:

   If the shared disk is offline, only the logical host settings will be deleted. The directories and files on the shared disk will not be deleted.

3. Check the logical host settings.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

   Make sure that PFM - Manager has been deleted from the logical host environment.

   For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(f) Performing unsetup for a logical host of PFM - Agent or PFM - RM Executing Standby

This procedure is required only when there is PFM - Agent or PFM - RM on the same logical host from which unsetup will also be performed for PFM - Manager.

Perform unsetup of PFM - Agent or PFM - RM. For details on the unsetup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

(g) Exporting the logical host environment definitions Executing

When a logical host environment to perform unsetup of PFM - Manager is created on the executing node, apply the settings information for the executing node to the

standby node. First, export the logical host environment definitions for the executing node to a file.

Note:

To perform unsetup of a different instance of Performance Management from the same logical host, perform the export after all unsetup procedures are completed.

To export the environment definitions:

1. Export the logical host environment definitions.

   For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file. The export file allows an arbitrary file name.

   ```
   jpcconf ha export -f lhostexp.conf
   ```

   For details on the `jpcconf ha export` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(h) Copying the file containing the logical host environment definitions to the standby node

Executing Standby

Copy the file that has been exported in step (f) from the executing node to the standby node, so that it will be applied on the standby node.

Next, use operations of the cluster software or volume manager software to place the shared disk online, and finish the operations on the executing node. If this shared disk will continue to be used, it is not necessary to take it offline.

(i) Importing the file containing the logical host environment definitions

Standby

Import the export file copied from the executing node to the standby node, so that it will be applied to the standby node.

Use the `jpcconf ha import` command to apply the Performance Management settings for the logical host created on the executing node to the standby node. If multiple instances of Performance Management have been set up on a single logical host, import all of the instances as one group.

To import the export file containing the logical host environment definitions:

1. Import the logical host environment definitions.

   Use the `jpcconf ha import` command to import the exported file of logical host environment definitions copied from the executing node to the standby node.

For example, execute the following command when the exported file name is `lhostexp.conf`.

```
jpcconf ha import -f lhostexp.conf
```

When the command is executed, the environment settings for the standby node are changed to the same environment settings specified for the executing node that has been exported. Therefore, the settings for running PFM - Manager on a logical host are deleted. If you perform unsetup of Performance Management on another logical host, the relevant settings are also deleted.

For details on the `jpcconf ha import` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Check the settings for the logical host environment.

   Execute the `jpcconf ha list` command in the same manner as for the executing node, to check the settings of the logical host.

   Execute the command as follows:

```
jpcconf ha list -key all
```

   For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Cluster software setting procedure

(a) Clearing the registration of PFM - Manager in the cluster software

Executing Standby

Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

(5) Uninstallation procedure Executing Standby

(a) Performing uninstallation of PFM - Manager

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure is the same as for a non-cluster system.

For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Notes:

- When performing uninstallation of PFM - Manager, stop all Performance Management programs and services on the node where uninstallation is to be performed.
- If uninstallation is performed on Performance Management without deleting the logical host environment, the environment directory might remain. When this happens, delete the environment directory.

9.2.6 Unsetup and uninstallation of PFM - Web Console

The procedures for performing unsetup and uninstallation of PFM - Web Console are explained below.

(1) Process flow for unsetup and uninstallation

The process flow for unsetup and uninstallation of PFM - Web Console used on a logical host in the cluster system is explained below.

The following figure shows the process flow for unsetup and uninstallation.

Figure 9-15: Process flow for unsetup and uninstallation of PFM - Web Console used on a logical host (in Windows)

Next, the unsetup procedures, procedures for clearing cluster software settings, and uninstallation procedures are explained below.

The image Executing indicates the items to be performed on the executing node, and the image Standby indicates the items to be performed on the standby node.

(2) Unsetup procedure

The procedure is as follows:

(a) Stopping from the cluster software Executing Standby

Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how

to stop programs and services, see the cluster software documentation.

(b) Making sure the shared disk is online Executing

Make sure that the shared disk is online. If the shared disk is not online, place it online through the operation of the cluster software and volume manager.

(3) Cluster software setting procedure

(a) Clearing the registration of PFM - Web Console from the cluster software

Executing Standby

Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

(4) Uninstallation procedure

(a) Performing uninstallation of PFM - Web Console Executing Standby

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure of PFM - Web Console is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note:

If the installation folder for the bookmark definition information has been changed from the default setting, it will not be deleted when performing uninstallation of PFM - Web Console. You need to delete it manually after performing the uninstallation.

9.3 Changing the cluster system configuration (in Windows)

After a system is configured and the operation started, as the business expands and processed data volume increases, the system's cluster configuration might need to be changed with the addition of servers or introduction of new applications.

For this reason, the following the Performance Management configuration changes need to be studied in response to changes in the cluster configuration of the monitoring target system:

- Addition of PFM - Agent or PFM - RM due to the addition of a monitored system
- Removal of PFM - Agent or PFM - RM due to the removal of a monitored system

This section describes the procedures for making changes to the Performance Management configuration when using a cluster system on a logical host.

9.3.1 Adding PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be added in order to monitor the performance of servers or applications that are newly added to a system.

When you add PFM - Agent or PFM - RM with a new product ID that has not previously been used in the Performance Management system, you need to set up the agent information in PFM - Manager and PFM - Web Console.

For details on product IDs, see the appropriate PFM - Agent or PFM - RM manual.

Point:

Agent information is a kind of information used by PFM - Manager and PFM - Web Console to manage and display PFM - Agent or PFM - RM.

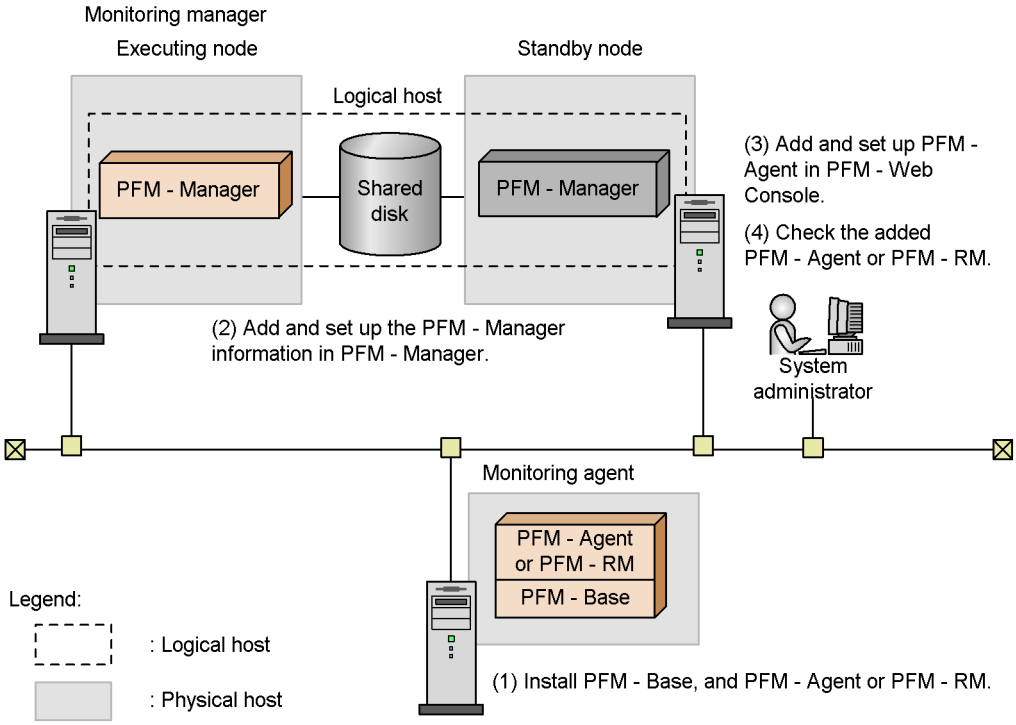
Notes:

- Stop PFM - Manager and all Performance Management programs and services on that node before adding PFM - Agent or PFM - RM. For details on how to stop services, see *1. Starting and Stopping Performance Management*.
- It is also necessary to stop PFM - Manager used on a logical host if work is being performed. An error might occur if you execute the `jpcconf agent setup` command or the `jpcwagtsetup` command to add PFM - Agent or PFM - RM before the Performance Management programs and services are completely stopped. In such a case, first make sure that all services have been completely stopped, and then re-execute the `jpcconf agent setup` command or the `jpcwagtsetup` command.

The following figure shows the process flow for adding PFM - Agent or PFM - RM to

a Performance Management system in a logical host environment.

Figure 9-16: Process flow for adding PFM - Agent or PFM - RM to a Performance Management system in a logical host environment



The procedure is as follows:

(1) Installing PFM - Base and either PFM - Agent or PFM - RM

Perform a new installation of PFM - Base and either PFM - Agent or PFM - RM on the host where Performance Management will be used to monitor performances.

For details on the installation procedure, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Performing an additional setup for PFM - Agent or PFM - RM information in PFM - Manager

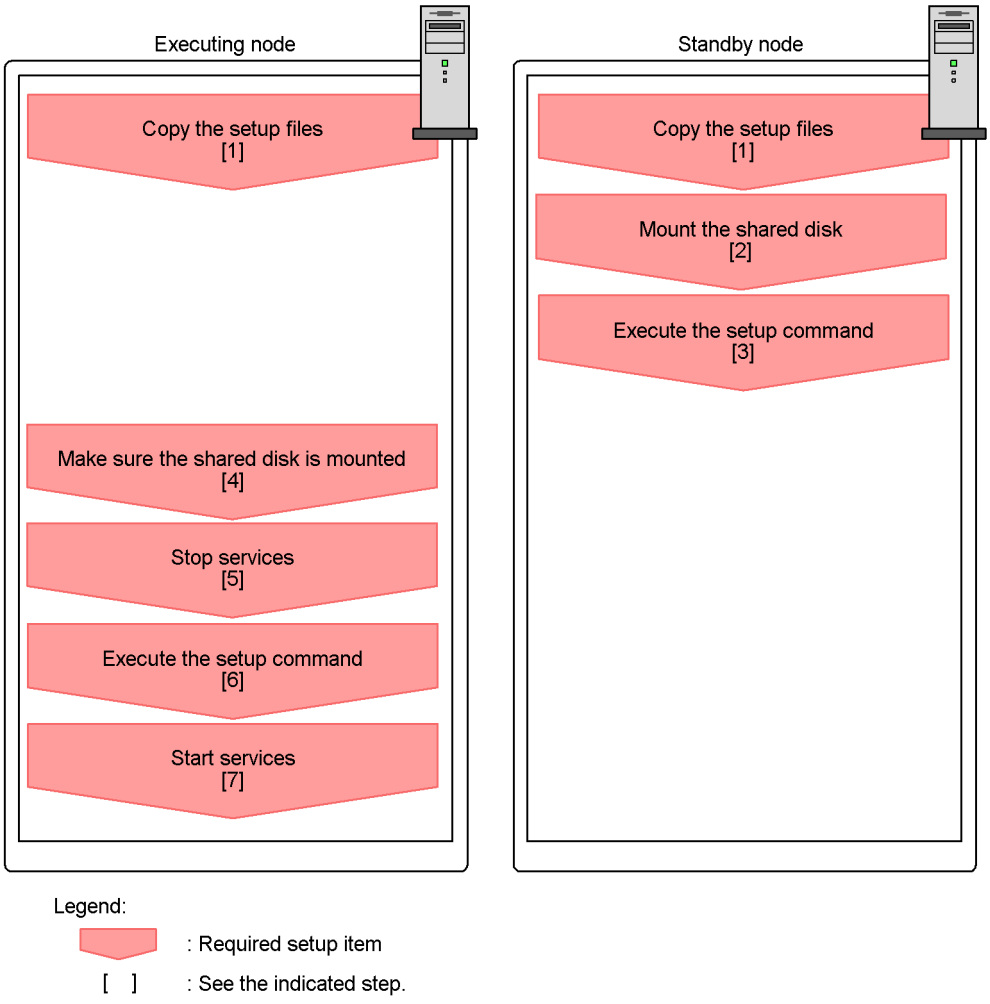
The process flow for performing an additional setup for the agent information of PFM - Agent or PFM - RM into PFM - Manager used on a logical host in a cluster system is described below.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM -

RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Perform the addition and setup of agent information on the standby node first. When the addition and setup are completed on the standby node, next perform setup on the executing node.

Figure 9-17: Process flow for performing an additional setup for PFM - Agent or PFM - RM information in PFM - Manager



Notes:

- If you add PFM - Agent or PFM - RM to the same host as PFM - Manager and PFM - Web Console, an additional setup is not required.
- If you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host, first set up the older version of PFM - Agent or PFM - RM, and then set up the newer version of PFM - Agent or PFM - RM.

The procedure for performing an additional setup for PFM - Agent or PFM - RM agent information is explained below.

To add and set up the PFM - Agent information in PFM - Manager:

The image 

means the procedure used on the executing node, and the image 

means the procedure used on the standby node.

1. Copying the setup files 

   Copy the PFM - Agent or PFM - RM setup files to the executing and standby nodes of PFM - Manager.

   For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

2. Executing the setup command 

   Execute the `jpcconf agent setup` command on the standby node to add and set up the new agent.

   Execute the command as follows:

   ```
   jpcconf agent setup -key xxxx
   ```

   xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

   For example, execute the following command to set up PFM - Agent for Oracle:

   ```
   jpcconf agent setup -key Oracle
   ```

   For details on the `jpcconf agent setup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

3. Making sure the shared disk is online Executing

   Make sure that the shared disk is online on the execution node. With the additional setup procedure, write the agent information to the shared disk. Use either operations from the cluster software or the volume manager to check if the shared disk is online.

4. Stopping services Executing

   Stop the Performance Management programs and services on the executing node. Use the cluster software to stop the programs and services.

5. Executing setup commands Executing

   Execute the `jpcconf agent setup` command on the executing node in the same manner as for the standby node in order to add and set up the new agent.

   ```
   jpcconf agent setup -key xxxx
   ```

   xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

   For example, execute the following command to set up PFM - Agent for Oracle:

   ```
   jpcconf agent setup -key Oracle
   ```

   For details on the `jpcconf agent setup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

6. Starting services Executing

   Start the Performance Management programs and services that were stopped on the executing node.

(3) Performing an additional setup for PFM - Agent or PFM - RM in PFM - Web Console

Perform an additional setup for PFM - Agent or PFM - RM information in instances of PFM - Web Console that are used on a logical host in a cluster system.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the

release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

For details on the additional setup procedure, see *9.2.3(3)(a) Performing an additional setup for PFM - Agent or PFM - RM information*.

(4) Checking PFM - Agent or PFM - RM that was added and set up

Check PFM - Agent or PFM - RM that was added and set up.

To check the added PFM - Agent:

1. Start the services on the PFM - Agent or PFM - RM nodes.

   Start the Performance Management programs and services on the nodes of the newly added PFM - Agent or PFM - RM.

2. Check if PFM - Agent or PFM - RM has been added correctly.

   Execute the `jpctool service list` command to check if PFM - Manager has been connected correctly.

   Execute the command as follows:

   ```
   jpctool service list -id *
   ```

   For details on the `jpctool service list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

9.3.2 Deleting PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be deleted when a monitored system is removed from the entire system due to changes in the system configuration.

Delete PFM - Agent or PFM - RM from the Performance Management system used by the logical host. The programs must be deleted from both the PFM - Manager and PFM - Web Console hosts.

Note:

Stop all Performance Management programs and services on the node from which PFM - Agent or PFM - RM will be deleted.

If the instance of PFM - Agent or PFM - RM that will be deleted is on the same node as PFM - Manager, it is necessary to first use the `jpctool service delete` command to delete the agent information, and then restart PFM - Manager.

(1) Deleting PFM - Agent or PFM - RM from PFM - Manager

To delete PFM -Agent from PFM - Manager:

1. Delete the agent information.

   Delete the agent information managed by PFM - Manager.

   Execute the command as follows:

   `jpctool service delete -id` *xxxx* `-host` *host-name* `-lhost` *logical-host-name*

   xxxx indicates the service ID for each PFM - Agent or PFM - RM.

   For example, execute the following command to delete the agent information for PFM - Agent for Oracle in the logical host environment with the host name `jp1` and the logical host name `jp1-ha1`.

   ```
   jpctool service delete -id O* -host jp1 -lhost jp1-ha1
   ```

   For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Perform unsetup and uninstall PFM - Agent or PFM - RM.

   Perform unsetup and uninstall PFM - Agent or PFM - RM. For details on how to perform unsetup and how to uninstall PFM - Agents or PFM - RM, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

   If the instance of PFM - Agent or PFM - RM that will be deleted is on the same node as PFM - Manager, it is necessary to restart PFM - Manager after the unsetup and uninstallation have been performed. Go to step 3.

3. Restart PFM - Manager.

   Restart PFM - Manager.

(2) Deleting PFM - Agent or PFM - RM from PFM - Web Console

To delete PFM - Agent from PFM - Web Console:

1. Restart PFM - Web Console on the executing node.

   Apply the changes made by the deleted PFM - Agent or PFM - RM information to PFM - Web Console.

   After performing unsetup and uninstalling PFM - Agent or PFM - RM, restart PFM - Web Console on the executing node.

   Reference note:

This restart is not required on the standby node since PFM - Web Console restarts when a failover occurs.

2. Delete the alarm definition information and report definition information.

   Delete the unnecessary alarm definition information and report definition information as necessary.

   For details on deleting alarm definition information, see *6.4.9(2) Deleting an alarm* or *6.7.6 Deleting an alarm*. For details on deleting report definition information, see *5.3.12(2) Deleting a report* or *5.5.2 Deleting an unnecessary report*.

9.3.3 Changing logical host names after starting operation

This subsection describes the procedures (performed on the Performance Management system) necessary for changing the host names of the PFM - Manager host, PFM - Agent host, or PFM - RM host after the Performance Management system has been configured.

To change a logical host name, you must first use the `jpcconf host hostname` command to change the monitoring host name.

If you execute the `jpcconf host hostname` command, all existing information, including definition and performance information, is inherited. For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

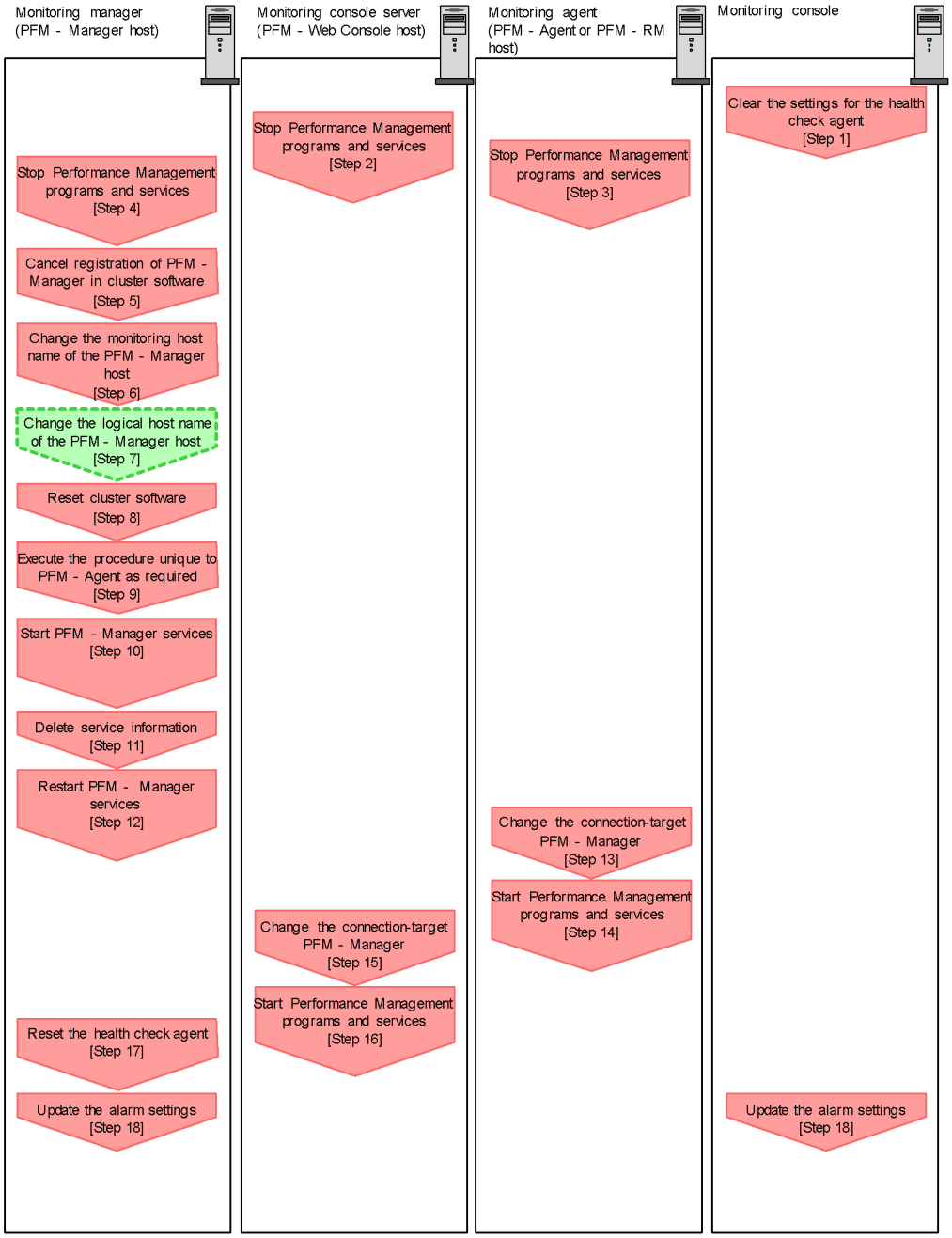
(1) Changing the PFM - Manager logical host name

You must work on the following hosts when changing the PFM - Manager logical host name:

- PFM - Manager host
- PFM - Web Console host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Figure 9-18: Process flow for changing the PFM - Manager host name



Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Clear the settings for the health check agent.

   If you are using the health check function, you can delete the agent definitions for the health check agent using your PFM - Web Console browser (by deleting the definitions from the management folder in the Agents tree and removing the association between the alarm tables and the definitions). For details on how to change the agent definition, see *6. Monitoring Operations with Alarms*.

2. Stop services on the PFM - Web Console host.

   On the PFM - Web Console host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcwstop` command.

3. Stop services on the PFM - Agent or PFM - RM host.

   On the PFM - Agent or PFM - RM host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcspm stop` command.

4. Stop services on the PFM - Manager host.

   Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

5. Cancel the registration of PFM - Manager from the cluster software.

   Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

6. Change the monitoring host name of PFM - Manager host.

   Execute the `jpcconf host hostname` command to change the monitoring host name.

   In the following example, the logical host name is changed from `lhostA` to `lhostB`.

   ```
   jpcconf host hostname -lhost lhostA -newhost lhostB -d
   d:\backup -dbconvert convert
   ```

   For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

Reference note:

The directory specified with the `-d` option of the `jpcconf host hostname` command requires disk space equal to the total size of the PFM - Agent and PFM - RM Store databases on the specified host.

For example, if PFM - Agent for Enterprise Applications and PFM - Agent for Oracle are located in the environment directory, the directory to be specified with the `-d` option will require disk space equal to the total size of the Store databases of the programs. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

7. Change the PFM - Manager logical host name.

   Change the PFM - Manager logical host name. Edit the settings in the `hosts` and `jpchosts` files, if necessary.

8. Reconfigure the cluster software

   For details, see *9.2.2(4) Cluster software setting procedure*.

9. Perform any PFM - Agent-specific steps, if necessary.

   If PFM - Agent has been installed on the PFM - Manager host, the PFM - Agent-specific procedure might be necessary. The following table describes whether the PFM - Agent-specific procedure is necessary.

   Table 9-4: Whether the PFM - Agent-specific procedure is necessary

Configuration		Necessity and reference
The version of PFM - Agent installed on the PFM - Manager host is 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The version of PFM - Agent installed on the PFM - Manager host is before 09-00.	The following PFM-Agent: • PFM - Agent for Enterprise Applications • PFM - Agent for Microsoft SQL Server	The Agent-specific procedure is necessary. For details, see *(4) Optional Agent-specific steps for host name changes*.
	Other than the above (including the case where PFM - RM is installed on the PFM - Manager host)	The Agent-specific procedure is not necessary.

If a PFM - Agent-specific step is to be performed, complete the reference step

shown in this table before proceeding to the next step.

10. Start services on the PFM - Manager host.

    Use the cluster software to start all PFM - Manager services.

11. Delete service information on the PFM - Manager host.

    Even though the PFM - Manager host name is changed, the service information of the Performance Management programs with the old host name remains the same. If you changed the PFM - Manager host name, you need to delete the old PFM - Manager service information. For example, to change the logical host name of the PFM - Manager host from `lhostA` to `lhostB`, execute the following command on the PFM - Manager host, and then delete all PFM - Manager service information from host `lhostA`.

    ```
    jpctool service delete -id P* -host lhostA -lhost lhostB
    jpctool service delete -id 0* -host lhostA -lhost lhostB
    ```

    For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

12. Restart services on the PFM - Manager host.

    Restart the PFM - Manager services using the cluster software to apply the deletion of the service information.

13. Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host.

    Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the logical host name. Use the `jpcconf mgrhost define` command to change the settings for PFM - Manager for the connection destination. For example, if the host name of PFM - Manager for the connection destination is changed to *host01*, specify and execute the command as follows:

    ```
    jpcconf mgrhost define -host lhostB
    ```

    For details on the `jpcconf mgrhost define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

14. Start services on the PFM - Agent or PFM - RM host.

    Start the Performance Management programs and services on the PFM - Agent or

PFM - RM host connected to PFM - Manager for which you have changed the logical host name. To start services, use `jpcspm start` command.

15. Change PFM - Manager for the connection destination on the PFM - Web Console host.

    Change the settings for PFM - Manager for the connection destination on the PFM - Web Console host connected to PFM - Manager for which you have changed the logical host name. Change the information in the Windows initialization file (`config.xml`) to change the settings for PFM - Manager for the connection destination. For details, see the chapter describing installation and setup (in Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

16. Start services on the PFM - Web Console host.

    Start the Performance Management programs and services on the PFM - Agent host connected to PFM - Manager for which you have changed the logical host name. To start services, use the `jpcwstart` command.

17. Reconfigure the definition for the health check agent.

    If you have been using the health check function, reconfigure the definition (that has been cleared in step 1) of the health check agent after changing the host name.

18. Update the alarm settings.

    In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

    - The action handler of the PFM - Manager host is specified for the action handler that executes actions.

      Edit the alarm to set `PH1`<*new-pfm-manager-host-name*> for the action handler that executes actions.

    - JP1 events are issued by actions.

      Set the JP1 event settings in the action again.

    For details on how to edit alarms, see *6. Monitoring Operations with Alarms*.

19. Update the JP1 system event settings.

    If either of the following conditions is met, use your PFM - Web Console browser to update the JP1 system event settings:

    - The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
    - The old host name is specified as the name of the monitoring console host for JP1 system events.

20. Check whether the JP1 system event settings are properly updated.

    Check the following items after changing the logical host name:

    - Collection of performance data

      Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).

    - Execution of the `jpctool db dump` command

      Make sure that there is no problem in outputting the collected performance data.

    - The report definitions and alarm definitions

      Make sure that there are no problems with the report definitions and alarm definitions created from the browser.

    - The actions

      Make sure that there is no problem in executing the created actions.

21. Log on to the network management product (NNM) again if it is linked for operation monitoring.

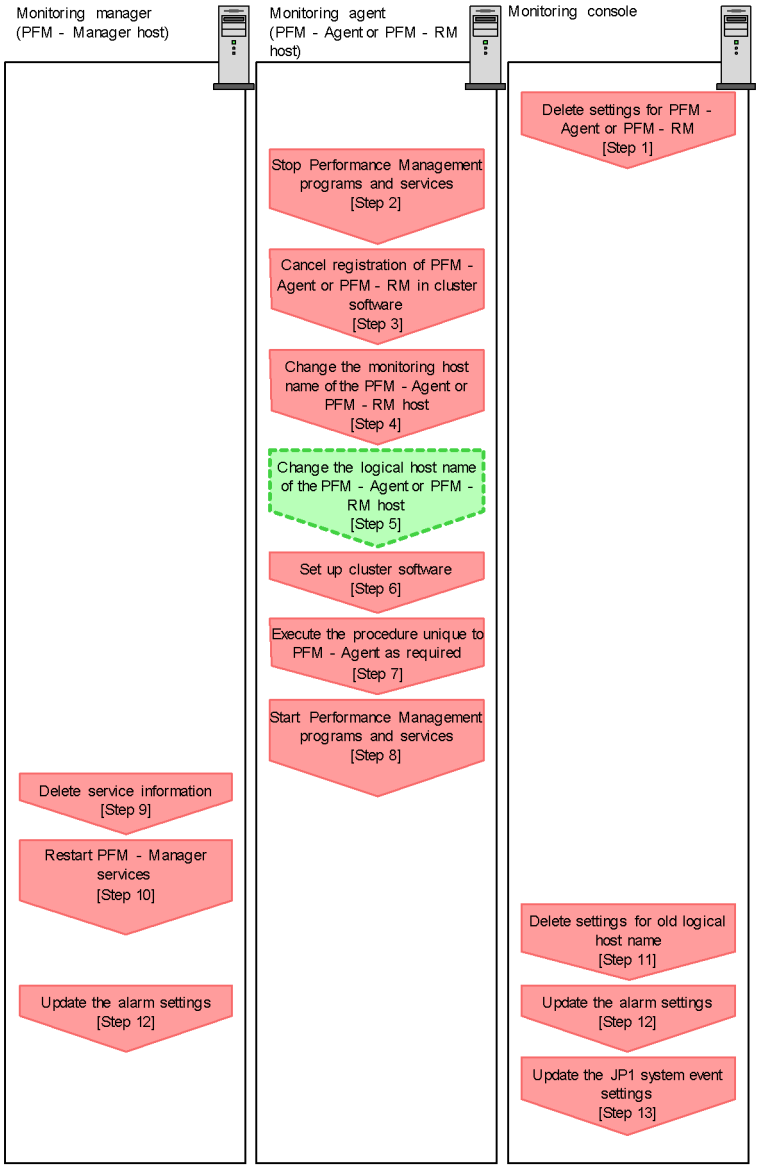
(2) Changing the PFM - Agent or PFM - RM logical host name

You must work on the following hosts when changing the PFM - Manager or PFM - RM logical host name:

- PFM - Manager host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Figure 9-19: The process flow for changing the host name.



Legend:

Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Delete the PFM - Agent or PFM - RM information.

Use the PFM - Web Console browser to delete the agent definitions from the PFM - Agent or PFM - RM host whose logical host name will be changed (by deleting the definitions from the management folder in the Agents tree and removing the association between the alarm tables and the definitions).

For details on how to change agent definitions, see *3. Monitoring Agents* or *6. Monitoring Operations with Alarms*.

2. Stop the services on the PFM - Agent or PFM - RM host.

   Stop all Performance Management programs and services on the PFM - Agent or PFM - RM host for which you intend to change the logical host name. Use operations from the cluster software to stop Performance Management programs and the services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

3. Unregister PFM - Agent or PFM - RM from the cluster software.

   Delete the settings related to PFM - Agent or PFM - RM on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

4. Change the monitoring host name for the PFM - Agent or PFM - RM host.

   Execute the `jpcconf host hostname` command to change the monitoring host name.

   In the following example, the logical host name is changed from `lhostA` to `lhostB`.

   ```
   jpcconf host hostname -lhost lhostA -newhost lhostB -d
   d:\backup -dbconvert convert
   ```

   For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

Reference note:

The directory specified with the `-d` option of the `jpcconf host hostname` command requires disk space equal to the total size of the PFM - Agent and PFM - RM Store databases on the specified host.

For example, if PFM - Agent for Enterprise Applications and PFM - Agent for Oracle are located in the environment directory, the directory to be specified with the `-d` option will require disk space equal to the total size of the Store databases of the programs. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

5. Change the PFM - Agent or PFM - RM logical host name.

   Change the PFM - Agent or PFM - RM logical host name. Edit the settings in the `hosts` and `jpchosts` files, if necessary.

6. Configure the cluster software.

   For details, see *9.2.2(4) Cluster software setting procedure*.

7. Perform any PFM - Agent-specific steps, if necessary.

   The following table describes whether the PFM - Agent-specific procedure is necessary.

   Table 9-5: Whether the PFM - Agent-specific procedure is necessary

Configuration		Necessity and reference
The monitoring host name to be changed is PFM - Agent version 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary, depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The monitoring host name to be changed is PFM - Agent for versions earlier than 09-00.	The following PFM-Agent: • PFM - Agent for Enterprise Applications • PFM - Agent for Microsoft SQL Server	The Agent-specific procedure is necessary. For details, see *(4) Optional Agent-specific steps for host name changes*.
	Other than the above (including the case where the monitoring host name to be changed is PFM - RM)	The Agent-specific procedure is not necessary.

   If a PFM - Agent-specific step is to be performed, complete the reference step shown in this table before proceeding to the next step.

8. Start services on the PFM - Agent or PFM - RM host.

   Start Performance Management programs and services from the cluster software on the PFM - Agent or PFM - RM host for which you have changed the logical host name.

9. Delete service information on the PFM - Manager host.

   Even though the PFM - Agent or PFM - RM host name is changed, the service information of Performance Management programs to which the old host name is added remains the same. If you changed the PFM - Agent or PFM - RM host name, you need to delete the old PFM - Agent or PFM - RM service information.

For example, to delete the information on the Agent Store service of PFM - Agent for Oracle on the `lhostB`, execute the following command on the PFM - Manager host:

```
jpctool service delete -id OS* -host lhostB
```

For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

10. Restart services on the PFM - Manager host.

    Restart the PFM - Manager services using the cluster software to apply the changes made by the deleted service information.

11. Delete the PFM - Agent or PFM - RM settings for the old logical host name.

    Use the PFM - Web Console browser to delete the agent definition of the PFM - Agent or PFM - RM host for which you changed the logical host name. After that, set the new definition for the agent. For details on how to change agent definitions, see *3. Monitoring Agents*.

12. Update the alarm settings.

    In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

    - When the action handler of the PFM - Agent or PFM - RM host is specified for the action handler that executes actions.

      Edit the alarm to set `PH1`<*new-pfm-agent-or-pfm-rm-host-name*> for the action handler that executes actions.

    - When JP1 events are issued by actions.

      Set the JP1 event settings in the action again.

    For details on how to edit alarms, see *6. Monitoring Operations with Alarms*.

13. Update the JP1 system event settings.

    If either of the following conditions is met, use your PFM - Web Console browser to update the JP1 system event settings:

    - The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
    - The old host name is specified as the name of the monitoring console host for JP1 system events.

14. Check whether the JP1 system event settings are properly updated.

Check the following items after changed the settings:

- Collection of the performance data

  Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).

- Execution of the `jpctool db dump` command

  Make sure that there is no problem in outputting the collected performance data.

- The report definitions and alarm definitions

  Make sure that there are no problems with the report definitions and alarm definitions created from the browser.

- The actions

  Make sure that there is no problem in executing the created actions.

(3) Changing the PFM - Web Console logical host name

To change the PFM - Web Console logical host name:

1. Stop services on the PFM - Web Console host.

   Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

2. Cancel the registration of PFM - Web Console from the cluster software.

   Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

3. Edit the PFM - Web Console host information in the Windows initialization file (config.xml) to refer to the new logical host name.

   This step is necessary when the logical host name has been set for the `ownHost` parameter in the `<vsa> - <vserver-connection>` tag of the Windows initialization file (`config.xml`).

   For details on how to edit the host information, see *9.2.3(3)(c) Setting up PFM - Web Console (logical host)* and *9.2.3(3)(e) Copying the Windows initialization file (config.xml) to the executing node*.

4. If the integrated management product (JP1/IM) is linked for operation monitoring, change the host name specified in each applicable definition file or in the property value for each service.

The location of the host name setting depends on the type of JP1 event that is used.

- If a JP1 user event is used:

  Change the host name in the definition files for the tool launcher and for opening monitor windows. For details, see *10.3.2(3) Editing and copying the definition files for linkage*.

- If a JP1 system event is used:

  Change the host name in the Monitoring Console Host property value for each service. For details, see *10.3.2(1) Configuring so that JP1 events are issued*.

For details on an integrated management product (JP1/IM), see *10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring*.

5. If the network management product (NNM) is linked for operation monitoring, change the host name in the definition file.

   Change the PFM - Web Console host name specified in the NNM linkage definition file (`jpcnnm.ini`) to a new host name.

   For details, see *11.2.3(3) Modifying the NNM linkage definition file*.

6. Change the PFM - Web Console logical host name.
7. Reconfigure the cluster software.

   For details on the setting procedure, see *9.2.3(4) Cluster software setting procedure*.

8. Start services on the PFM - Web Console host.

   Use operations from the cluster software to starts the PFM - Web Console services.

9. If the integrated management product (JP1/IM) is linked, restart the product (JP1/IM).

(4) Optional Agent-specific steps for host name changes

This subsection describes the PFM - Agent-specific steps necessary to perform the following operations for each product:

- Changing the PFM - Manager logical host name
- Changing the PFM - Agent or PFM - RM logical host name

For details on when it is necessary to perform these steps, see *(1) Changing the PFM - Manager logical host name* and *(2) Changing the PFM - Agent or PFM - RM logical host name*.

(a) In PFM - Agent for Enterprise Applications

Execute the `jpcconf inst setup` command for all created instance environments. For example, if an instance environment `o246bci_SD5_00` exists in PFM - Agent for Enterprise Applications, execute the following command:

```
jpcconf inst setup -key agtm -inst o246bci_SD5_00 -lhost
jp1-halr3
```

The `jpcconf inst setup` command is an interactive command that returns a command prompt when executed. At the ASHOST prompt, enter the new host name, and press the **Enter** key when the other prompts come up. If you press the **Enter** key at a prompt without entering a value, the existing value is assumed.

(b) In PFM - Agent for Microsoft SQL Server

Execute the `jpcconf inst setup` command for all created instance environments. For example, if an instance environment `default` exists in PFM - Agent for Microsoft SQL Server, execute the following command:

```
jpcconf inst setup -key agtq -inst default -lhost jp1-halSQL
```

The `jpcconf inst setup` command is an interactive command that returns a command prompt when executed. At the `SQL_HOST` prompt, enter the new host name, and press the **Enter** key when the other prompts come up. If you press the **Enter** key at a prompt without entering a value, the existing value is assumed.

9.4 Configuration of a cluster system (in UNIX)

This section describes the operations for setting up a Performance Management system in a cluster system. The following topics are described in this section:

- PFM - Manager installation and setup
- PFM - Web Console installation and setup
- PFM - Manager unsetup and uninstallation
- PFM - Web Console unsetup and uninstallation

9.4.1 Before installation and setup

This subsection describes the items to check before installing and setting up Performance Management in a cluster system.

(1) Prerequisite conditions

The prerequisite conditions for using Performance Management in a cluster system are described below.

(a) Cluster system

Make sure that the following conditions are satisfied:

- The cluster system is controlled by cluster software.
- Settings are made so that the starting and stopping of Performance Management used on a logical host are controlled by cluster software.

(b) Shared disk

Make sure that the following conditions are satisfied:

- Each logical host has a shared disk, and the disk can be taken over from the executing node by the standby node.
- Shared disks are physically connected to each node via Fibre Channel or SCSI. Configurations in which the shared disk is a network drive or disk replicated over a network is used are not supported.
- When a failover occurs, if some processes are still using the shared disks, make sure it is still possible to force shared disks offline via cluster software or by other means and perform a failover.
- If multiple Performance Management programs are executed on a single logical host, make sure the directory names for the shared disks are the same. For Store databases, make sure the storage destination can be changed to allow storage in a different directory on the same shared disk.

(c) Logical host name, logical IP address

Make sure that the following conditions are satisfied:

- There is a logical host name and corresponding logical IP address for each logical host, and switching from the executing node to the standby node can be performed.
- The logical host and logical IP address are set in the `hosts` file and on the name server.
- If using a DNS, a logical host name is specified without a domain name, instead of by using a FQDN.
- Each physical host name and logical host name is unique within the system.

Notes regarding logical host names:

- Do not use a physical host name (a host name displayed using the `hostname` command) for a logical host name. Otherwise, normal communication processing might be prevented.
- Logical host names must consist of from 1 to 32 bytes alphanumeric characters.
- `localhost`, an IP adress, or a string that begins with a hyphen (`-`) cannot be used for a logical host name.

(d) Other prerequisite conditions

Make sure that the following conditions are satisfied:

- Kernel parameters have been optimized.

(2) Checking the setup environment

In addition to the environment information normally required to set up Performance Management, the following information is required to set up Performance Management used on a logical host.

Table 9-6: Information required to set up PFM - Manager to be used on a logical host (in UNIX)

Item	Example
Logical host name	`jp1-ha1`
Logical IP address	`172.16.92.100`
Shared disk	`/jp1`

If multiple instances of Performance Management use a single logical host, each instance uses the directory of the same shared disk.

(3) Notes about upgrading when a logical host is used

To upgrade PFM - Manager on a logical host, you must place a shared disk online on either an executing or a standby node.

However, there is no need to place a shared disk online to upgrade PFM - Web Console in a cluster environment.

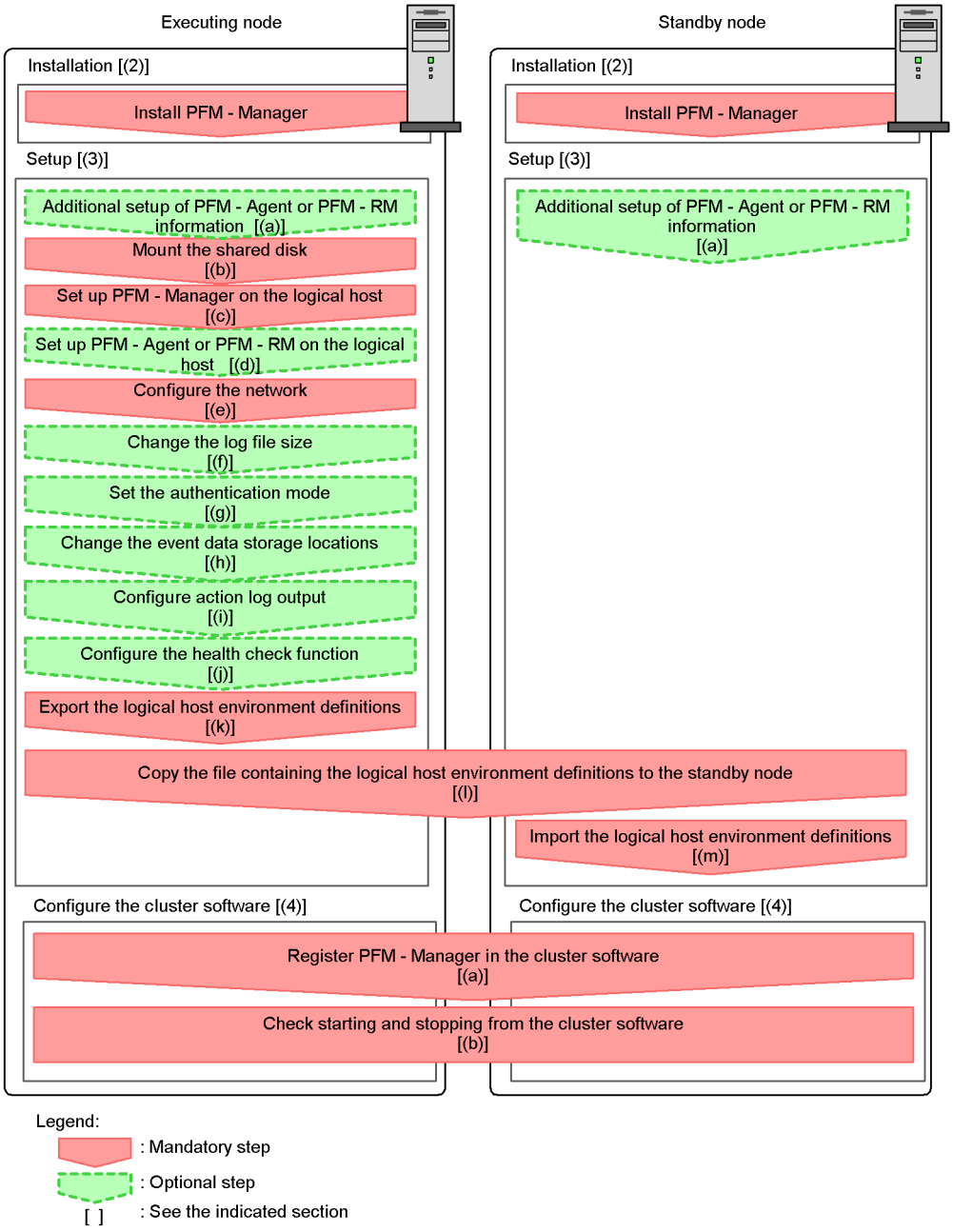
9.4.2 Installing and setting up PFM - Manager

This subsection describes the methods for installing and setting up PFM - Manager in a cluster system.

(1) Process flow for installation and setup

The following figure shows the process flow for installation and setup of PFM - Manager used on a logical host.

Figure 9-20: Process flow for installation and setup of PFM - Manager used on a logical host (in UNIX)



Notes:

- When PFM - Manager in a logical host environment is set up, PFM - Manager for the physical host environment can no longer be executed. However, the Action Handler service can still be executed, because it uses PFM - Agent or PFM - RM in the physical host environment.

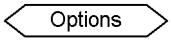
  When unsetup is performed on PFM - Manager in a logical host environment, PFM - Manager in the physical host environment can once again be executed.

- When PFM - Manager in a logical host environment is set up, the definitions for PFM - Manager in the physical host environment are inherited by the logical host environment. However, the content of the Store database is not inherited. If unsetup is performed on PFM - Manager in the logical host environment, the definitions for the logical host environment and the Store database are deleted, and therefore switching to the physical host environment is not possible.
- Do not manually set `JPC_HOSTNAME` as an environment variable because it is used for Performance Management as an environment variable. If you specify this setting, Performance Management will not run correctly.
- For PFM - Manager of the version 09-00 or later, when you set up a new instance of PFM - Manager in a logical host environment, the settings of the health check function in the physical host environment are inherited by the logical host environment. You must modify the settings of the health check function, if necessary.
- In a logical host environment, the function for setting monitoring-host names cannot be used. The `jpccomm.ini` file on a logical host is ignored and the host name for the logical host is used.

The installation and setup procedures for PFM - Manager and the setting procedures for the cluster software are explained below.

In the procedure explanation, the image 

indicates items to be performed on the executing node, and the image 

indicates items to be performed on the standby node. In addition, the image 

indicates setup items that are either required depending on the environment or can be performed if you want to set a value other than the default settings.

(2) Installation procedure 

Perform a new installation of PFM - Manager on the executing node and the standby node. The installation procedure is the same as for a non-cluster system. For details,

see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

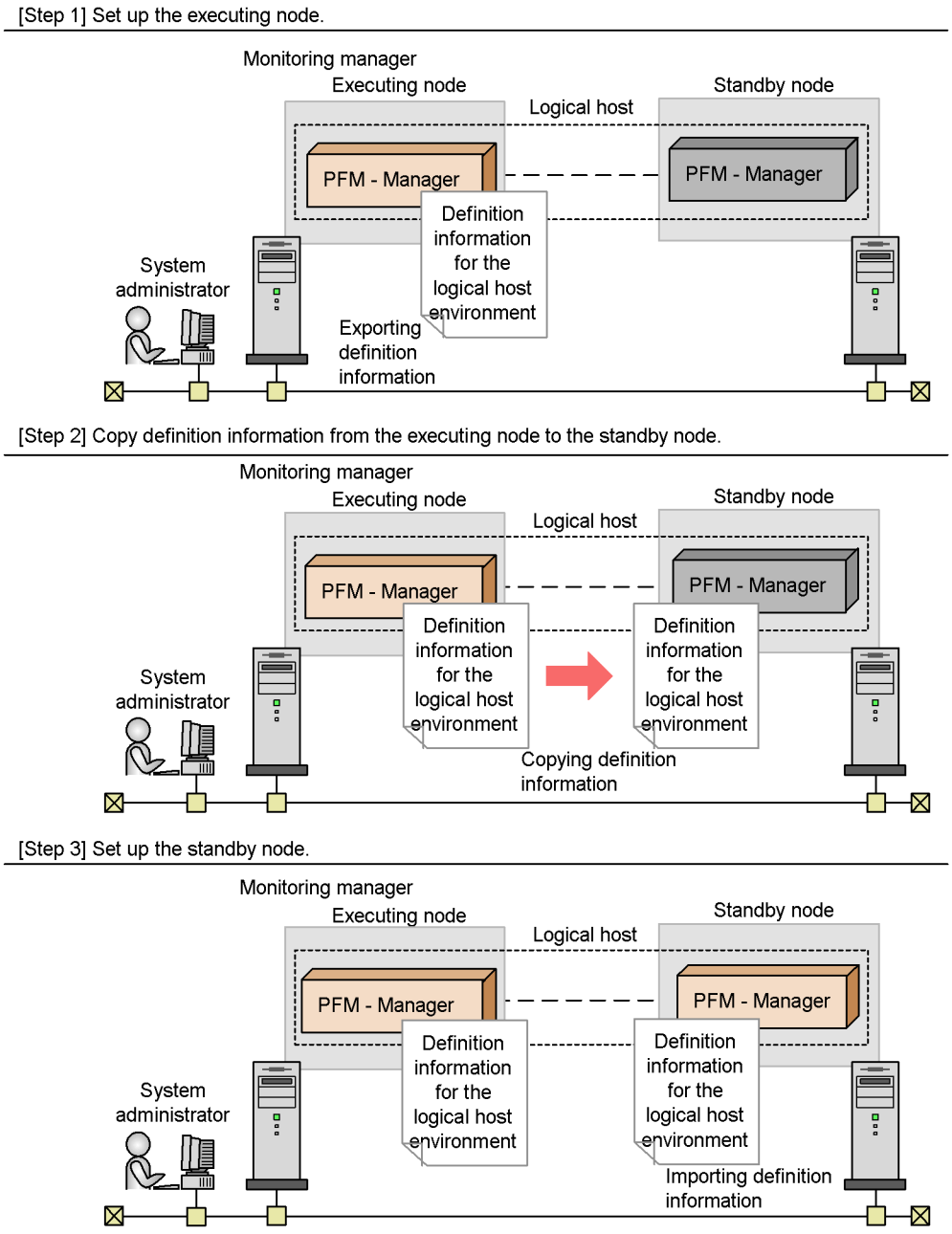
Note:

The installation destination is the local disk. Do not install PFM - Manager on the shared disk.

(3) Setup procedure

Perform PFM - Manager setup on the executing node first. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the setup content from the executing node to the standby node.

Figure 9-21: Method for applying the content set up on the executing node to the standby node



Each setup procedure is explained below.

(a) Performing an additional setup for PFM - Agent or PFM - RM information

Executing | Standby | Options

To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Manager for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

The setup procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

Note:

If you add another PFM - Agent or PFM - RM to the same host as PFM - Manager, an additional setup is not required.

(b) Making sure the shared disk is mounted

Executing

Make sure that the shared disk is mounted. If the shared disk is not mounted, execute the `mount` command to mount the file system.

Note:

If setup is performed without mounting the shared disk, files might be created on the local disk.

(c) Setting up a logical host for PFM - Manager

Executing

Set up the logical host environment for PFM - Manager on the executing node. Before performing setup, stop all the Performance Management programs and services throughout the entire system.

To set up a logical host for PFM - Manager:

1. Create a logical host environment.

   Execute the `jpcconf ha setup` command to create a logical host environment for PFM - Manager.

   Use `-lhost` to specify the logical host name. For DNS operation, specify a logical host name that does not include a domain name. Specify the `-d`

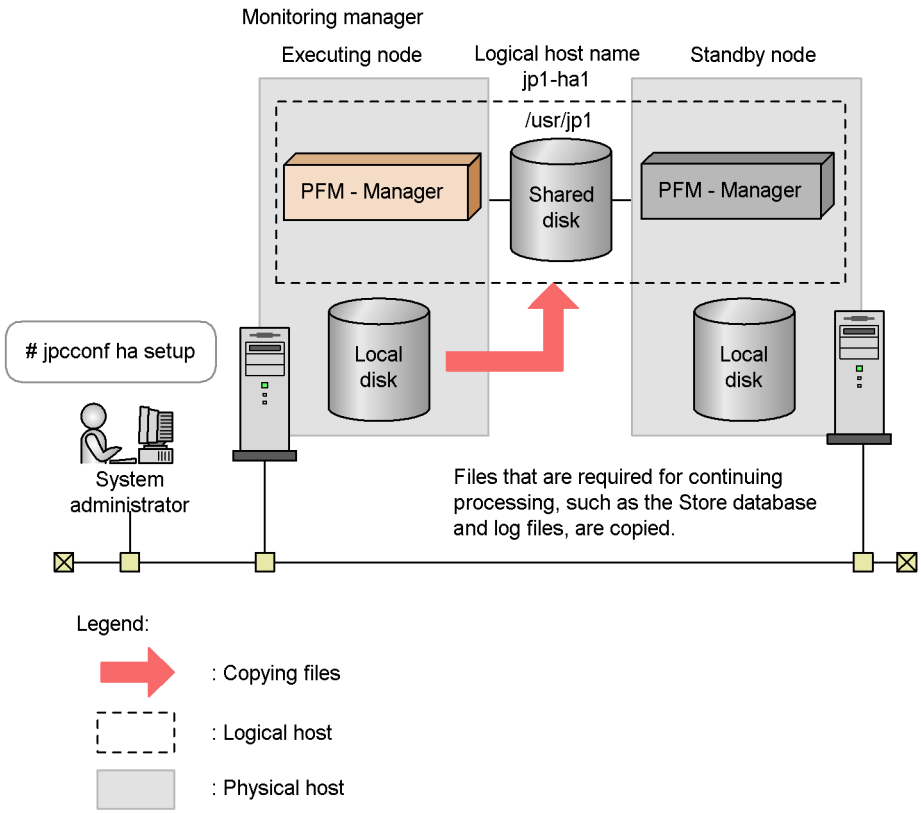
environment directory name for the directory name of the shared disk.

For example, execute the following command to set up a logical host with `jp1-ha1` as the logical host name and `/usr/jp1` as the environment directory.

```
jpcconf ha setup -key Manager -lhost jp1-ha1 -d /usr/jp1
```

When this command is executed, the `jp1pc` directory is created under `/usr/jp1`, and the files required in the logical host environment are copied to the environment directory. The following figure shows an example.

Figure 9-22: Execution example of the jpcconf ha setup command



When the command is executed, the required data is copied from the local disk of the executing node to the shared disk, and the settings required for use on the logical host are performed.

For details on the `jpcconf ha setup` command, see the chapters that describes commands in the manual *Job Management Partner 1/Performance Management*

Reference.

2. Check the settings for the logical host environment.

   Execute the `jpcconf ha list` command to check the settings for the logical host, and make sure that the logical host environment that has been created is correct.

   ```
   jpcconf ha list -key all
   ```

   An example of executing this command is as follows:

```
C:\>jpchasetup list all

Logical Host Name  Key      Environment Directory                 [Instance Name]
-----------------  -------- ------------------------------------- ---------------------------
jp1-ha1            mgr      "/usr/jp1/jp1pc"

KAVE05136-I  The logical host startup information listing ended normally.
```

   For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(d) Performing a setup for a logical host of PFM - Agent or PFM - RM

Executing | Options

This procedure is required only when there is a PFM - Agent or PFM - RM to set up in the same logical host in addition to PFM - Manager.

For details on the setup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

(e) Specifying network settings

Executing

To use the logical host names for communications between PFM - Manager and PFM - Web Console, add the following line to the *environment-directory*`/jp1pc/mgr/viewsvr/jpcvsvr.ini` file.

`java.rmi.server.hostname=`*logical-host-name*

For details on host names used for communications between PFM - Manager and PFM - Web Console, see the sections that describe port numbers in an appendix of the manual *Job Management Partner 1/Performance Management Reference*.

In addition, use the following procedure when changing IP addresses and port numbers according to the network configuration.

- Setting the IP address Options

  To set the IP addresses, directly edit the content of the `jpchosts` file. If you have edited the `jpchosts` file, copy the file from the executing node to the standby node.

  For details on setting IP addresses, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Setting port numbers Options

  This procedure is necessary only when running Performance Management in a network environment with a firewall.

  For Performance Management communications via a firewall, use the `jpcconf port define port` command to set a port number.

  For example, execute the following command to set all port numbers for services that exist on the host with the logical host name `jp1-ha1` specified in the fixed values.

  ```
  jpcconf port define -key all -lhost jp1-ha1
  ```

  When this command is executed, definitions of the port number and service name (TCP service name beginning with `jp1pc` by default) for Performance Management are added to the services file.

  For details on setting port numbers, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

  For details on the `jpcconf port define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(f) Changing the log file size Options

The operating status of Performance Management is output to a dedicated log file called the *common message log*. By default, the common message log uses two 2,048-KB files. This setting is required only when if you want change this file size.

For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(g) Specifying settings for the authentication mode

Options

This setting is required only if you want to change the authentication mode of Performance Management from PFM authentication mode to JP1 authentication mode.

For details, see *2. Managing User Accounts*.

(h) Changing the storage locations of event data

Options

The settings below are required if you want to change the storage destination, backup destination, or export destination of the event data managed by PFM - Manager.

By default, event data is stored in the following locations:

- Data storage folder: *environment-directory*`/jp1pc/mgr/store/`
- Backup folder: *environment-directory*`/jp1pc/mgr/store/backup/`
- Export folder: *environment-directory*`/jp1pc/mgr/store/dump/`

For details on how to changea destination, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(i) Specifying settings for action log output

Options

This setting is required if you want to output an action log when an alarm is issued. An action log is log information output in conjunction with the alarm function, when an aspect of the system (such as the system load) exceeds a threshold. For details on how to set this option, see the section describing action log output in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(j) Configuring the health check function

Executing Options

To configure the health check function:

1. Check the settings of the health check function.

   Execute the following command on the PFM - Manager host on the executing node to display the setting of the health check function.

   ```
   jpcconf hc display
   ```

   When the command is executed, the setting for the health check function appears as follows:

   - If the health check function is enabled: `available`

- If the health check function is disabled: `unavailable`

For details on the `jpcconf hc display` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Change the setting of the health check function.

   Execute the following command on the PFM - Manager host on the executing node to set up the health check function, if necessary.

   - To enable the health check function: `jpcconf hc enable`
   - To disable the health check function: `jpcconf hc disable`

   For details on the `jpcconf hc enable` and `jpcconf hc disable` commands, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

(k) Exporting the logical host environment definitions

Executing

When a logical host environment for PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file. To set up a different instance of Performance Management on the same logical host, perform an export after all setup procedures are completed.

To export the environment definitions:

1. Execute the `jpcconf ha export` command.

   Export the logical host environment definitions to the desired file.

   For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file.

   ```
   jpcconf ha export -f lhostexp.conf
   ```

   If the health check function is enabled for the PFM - Manager in the logical host environment you are exporting, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be exported.

   For details on the `jpcconf ha export` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(l) Copying the file containing the logical host environment definitions to the standby node

Executing Standby

Copy the file that has been exported in step (f) from the executing node to the standby

node, so that it will be applied on the standby node.

Next, unmount the file system to complete the work. If this shared disk will continue to be used, it is not necessary to unmount the file system.

Note:

Even if the shared disk is unmounted, if there is a `jp1pc` directory and associated files in the specified environment directory, setup is performed without mounting the shared disk. If that is the case, use the following procedure:

1. Use the `tar` command to archive the `jp1pc` directories in the environment directory specified on the local disk.
2. Mount the shared disk.
3. If the specified environment directory does not exist on the shared disk, create an environment directory.
4. Expand the `tar` file in the environment directory on the shared disk.
5. Unmount the shared disk.
6. Delete the `jp1pc` directory and associated files in the environment directory specified on the local disk.

(m) Importing the file containing the logical host environment definitions

Standby

Import the export file copied from the executing node into the standby node.

To import the exported file containing the logical host environment definitions:

1. Execute the `jpcconf ha import` command.

   Import the logical host environment definitions into the standby node.

   For example, execute the following command if the export file name is `lhostexp.conf`.

   ```
   jpcconf ha import -f lhostexp.conf
   ```

   When the `jpcconf ha import` command is executed, the environment settings for the standby node are changed to the same environment as for the executing node. Therefore, settings are made to use PFM - Manager on a logical host.

   If the health check function is enabled for the PFM - Manager in the logical host environment you are importing, the health check agent will be set up on the logical host. In this case, information relating to the health check agent will be imported.

For details on the `jpcconf ha import` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Check the settings for the logical host environment.

   Execute the `jpcconf ha list` command in the same manner as for the executing node to check the settings of the logical host.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

   For details on the `jpcconf ha listt` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Cluster software setting procedure

Cluster software settings are required for both the executing node and the standby node.

The procedure is as follows:

(a) Registering PFM - Manager in the cluster software

To use PFM - Manager on a logical host, register it in the cluster software, and set the cluster software to control the starting and stopping of PFM - Manager.

For details on how to register PFM - Agents or PFM - RM in the cluster software, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

Generally, the following four command items are required when registering an application in the UNIX cluster software: *Start*, *Stop*, *Monitor operations*, and *Forced stop*.

The following table lists and describes the settings in PFM - Manager.

Table 9-7: Control commands for PFM - Manager registered in the cluster software

Command	Description
Start	Execute the following commands in order, and then start PFM - Manager: `/opt/jp1pc/tools/jpcspm start -key Manager -lhost` *logical-host-name* `/opt/jp1pc/tools/jpcspm start -key AH -lhost` *logical-host-name* Perform this action after a condition has been reached in which the shared disk and logical IP address can be used.
Stop	Execute the following commands in order, and then stop PFM - Manager: `/opt/jp1pc/tools/jpcspm stop -key AH -lhost` *logical-host-name* `/opt/jp1pc/tools/jpcspm stop -key Manager -lhost` *logical-host-name* Perform this action before a condition is reached in which the shared disk and logical IP address cannot be used. When a service is stopped due to a problem, the return value for the `jpcspm stop` command is `3`. If this is the case, it can be considered a normal termination since the services have been stopped. For the cluster software that determines execution results by return values, the recovery value can be set to `0`.
Monitor operations	Use the `ps` command to check if the following process is running. `ps -ef | grep "`*process-name logical-host-name*`" | grep -v "grep process monitored"` For details on process names, see *9.6.1(3) Service names*. Hitachi recommends that you prepare a command for suppressing operation monitoring (for example, a command to stop monitoring when there is a file that is under maintenance) in anticipation of a temporary stop in Performance Management due to maintenance during the operation.
Forced stop	Execute the following command when a forced stop is required: `/opt/jp1pc/tools/jpcspm stop -key all -lhost` *logical-host-name* `-kill immediate` Only `all` can be set to the service key for the first argument. Note: If this command is executed, SIGKILL is sent to perform a forced stop of all Performance Management processes in the specified logical host environment. At this time, the forced stop is performed on Performance Management not for each service, but for each logical host. Set this item to perform a forced stop only when the system cannot be stopped by executing a normal stop command.

Notes:

- Do not make automatic startup settings for OS startups, since the starting and stopping of the Performance Management registered in the cluster are controlled by the cluster.
- If the cluster software uses command return values to determine execution results, specify settings so that the command return values for Performance Management are converted to the values that can be correctly interpreted by the cluster software. For details on the command return values for Performance Management, check the reference documentation for each command.
- Before using the `ps` command for monitoring operations, execute the `ps` command to confirm that a character string that is a combination of the logical host name and the instance name is correctly displayed. If part of the character string is not displayed, shorten the instance name.

(b) Checking starting and stopping from the cluster software

Executing

Standby

Check whether the cluster software is operating correctly by using it to issue start and stop requests to PFM - Manager or PFM - Web Console on each node.

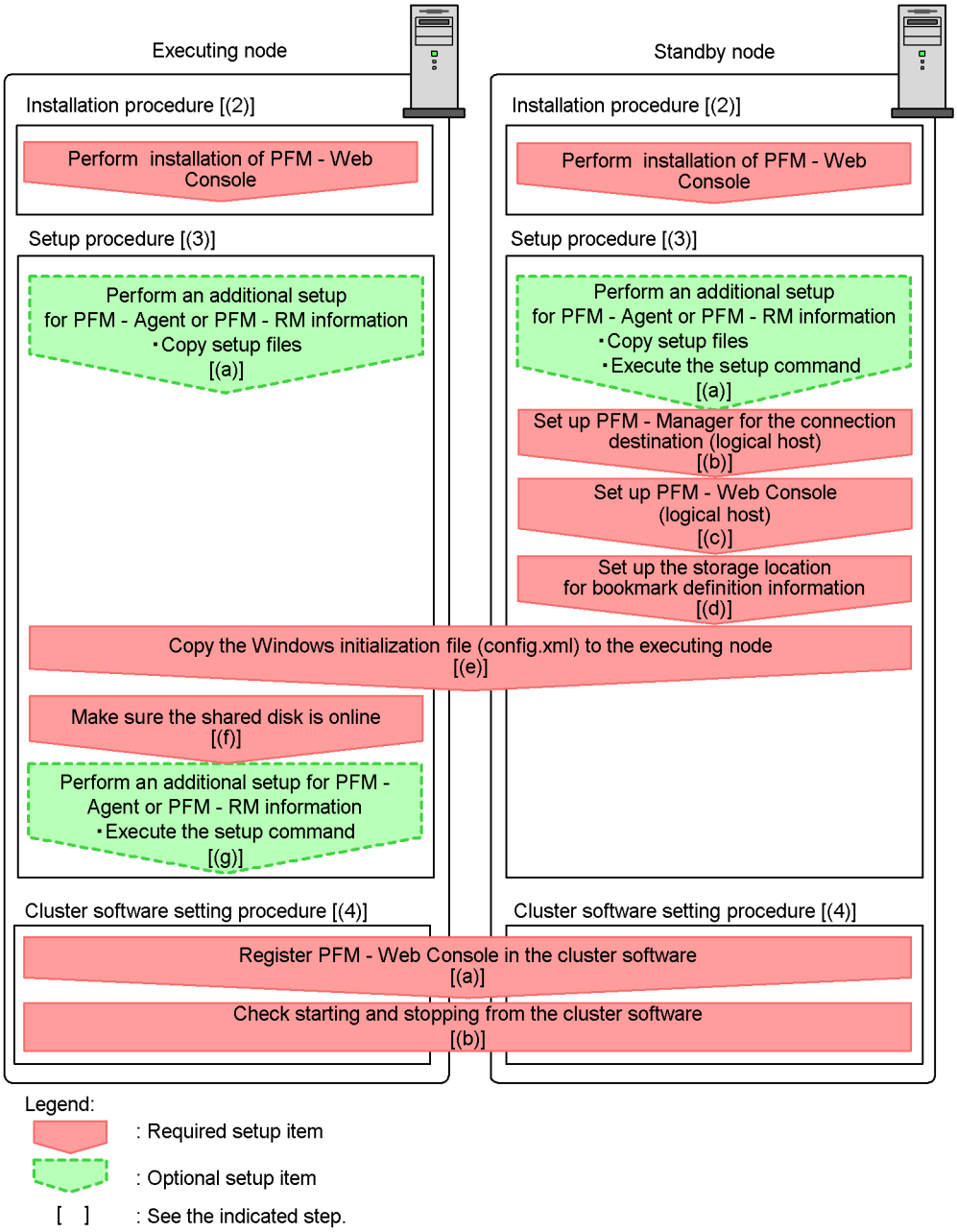
9.4.3 Installing and setting up PFM - Web Console

This subsection describes the methods for installing and setting up PFM - Web Console in a cluster system.

(1) Process flow for installation and setup

The following figure shows the process flow for installation and setup of PFM - Web Console used on a logical host.

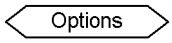
Figure 9-23: Process flow for installation and setup of PFM - Web Console used on a logical host



The installation and setup procedures for PFM - Web Console and the setup procedures for the cluster software are explained below.

In the procedure explanation, the image 

indicates the tasks to be performed on the executing node, and the image 

indicates the tasks to be performed on the standby node. In addition, the image 

indicates the setup items required for specific environments, and optional setup items for when you want to change the default settings.

(2) Installation procedure 

Perform a new installation of PFM - Web Console on the executing node and the standby node. The installation procedure is the same as for a non-cluster system.

For details on the installation procedure, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Notes:

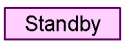
- Install PFM - Web Console on the local disk, not the shared disk.
- Install each PFM - Web Console for both the executing node and the standby node in a location with the same path.

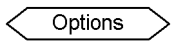
(3) Setup procedure

When using PFM - Web Console on a logical host, the environment configurations on the executing node and the standby node have to be the same.

Each of the setup types for PFM - Web Console is explained below.

(a) Performing an additional setup for PFM - Agent or PFM - RM information 





To perform integrated management of PFM - Agent or PFM - RM in a cluster system, register the agent information of PFM - Agent or PFM - RM in PFM - Web Console for the executing node and the standby node.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Notes:

- You do not need to register PFM - Agent or PFM - RM when you add the same version of PFM - Agent or PFM - RM with the same product ID to a Performance Management system in which the PFM - Agent or PFM - RM information has been already registered.
- Set up the latest version of PFM - Agent or PFM - RM if you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host.

To perform an additional setup of agent information in PFM - Web Console, see the process flow shown in Figure 9-23.

To register the agent information in PFM - Web Console:

1. Copy the setup files. Executing Standby

   Copy the PFM - Agent or PFM - RM setup file to the following locations on the PFM - Web Console executing node and standby node.

   ```
   /opt/jp1pcwebcon/setup
   ```

   The files to copy and the procedure for copying the files are the same as when performing an additional setup for PFM - Manager. For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

2. Execute the setup command on the standby node. Standby

   Execute the `jpcwagtsetup` command on the standby node to register the agent information.

   Execute the command as follows:

   ```
   jpcwagtsetup
   ```

   For details on the `jpcwagtsetup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

Supplemental information:

When you register the agent information of PFM - Agent or PFM - RM in PFM - Web Console, you must restart PFM - Web Console. However, because PFM - Web Console restarts on the standby node when a failover occurs, you do not need to restart PFM - Web Console on the standby node after step 2.

(b) Setting up PFM - Manager for the connection destination

Standby

On the standby node, set the IP address or host name for the PFM - Manager that serves as the connection destination for PFM - Web Console in the initialization file (`config.xml`). If the PFM - Manager that serves as the connection destination is running on a cluster system, set the logical IP address or the logical host name.

To set up PFM - Manager for the connection destination:

1. Open the initialization file (`config.xml`).

   Use a text editor or XML editor to open the `/opt/jp1pcwebcon/conf/config.xml` file.

2. Set the IP address or host name for the PFM - Manager host serving as the connection destination.

   Enter the following tag immediately after the `<vserver-connection>` tag within the `<vsa>` tag:

   ```
   <param name="host" value="IP-address-or-host-name"/>
   ```

   For example, if the IP address of the PFM - Manager host is *10.210.24.56*, perform the following settings:

   ```
   <vsa>
   <vserver-connection>
   <param name="host" value="10.210.24.56"/>
   <!-- The host computer name to which PFM View Server uses.
   Specifiable values: 1024 to 65535
   Default: 22286
   -->
   <param name="port" value="22286"/>
   </vserver-connection>
   ```

3. Save the initialization file (`config.xml`) you edited in step 2.

Note:

If areas other than those specified are changed in the initialization file (`config.xml`), PFM - Web Console might not operate correctly.

(c) Setting up PFM - Web Console (logical host)

Standby

Set the logical IP address or logical host name for PFM - Web Console in the initialization file (`config.xml`) on the standby node.

To set a logical host for PFM - Web Console:

1. Open the initialization file (config.xml).

   Use a text editor or XML editor to open the /opt/jp1pcwebcon/conf/config.xml file.

2. Set the logical IP address or logical host name for the PFM - Web Console host.

   Enter the following tag in the <vserver-connection> tag within the <vsa> tag:

   <param name="ownHost" value="*logical-IP-address-or-logical-host-name*"/>

   For example, if the logical IP address of the PFM - Web Console host is *10.210.26.18*, make the following settings:

```
    <vsa>
        <vserver-connection>
            <param name="host" value="10.210.24.56"/>
            <!-- The host computer name to which PFM View
Server uses.
                 Specifiable values: 1024 to 65535
                 Default           : 22286
            -->
            <param name="port" value="22286"/>
            <param name="ownHost" value="10.210.26.18"/>

       </vserver-connection>
```

3. Save the initialization file (config.xml) you edited in step 2.

Note:

If areas other than those specified are changed in the initialization file (config.xml), PFM - Web Console might not operate correctly.

(d) Setting up the storage location for bookmark definition information

Standby

Set the storage directory for bookmark definition information in the initialization file (config.xml) on the standby node. Specify an installation directory on the shared disk to ensure that bookmark definition information is inherited when a failover occurs.

To set the storage location for bookmark definition information:

1. Open the initialization file (config.xml).

Use a text editor or XML editor to open the `/opt/jp1pcwebcon/conf/config.xml` file.

2. Set the directory for storing the bookmark definition information.

   Set the storage directory in the `<bookmark>` tag immediately after the `<format>` tag within the `<vsa>` tag in the initialization file (`config.xml`).

   The directory you set will be created automatically when the PFM - Web Console service starts.

   For example, use the following setting to make *environment-directory*`/jp1pcwebcon/common/bookmarks` the storage directory.

```
</format>

<bookmark>
<!-- The directory where bookmark repository is stored.
Default : <install directory>/bookmarks -->
<param name="bookmarkRepository" value="environment-directory/
jp1pcwebcon/common/bookmarks"/>
</bookmark>

</vsa>
```

3. Save the initialization file (`config.xml`) you edited in step 2.

Note:

If areas other than those specified are changed in the initialization file (`config.xml`), PFM - Web Console might not operate correctly.

(e) Copying the initialization file (config.xml) to the executing node

Standby Executing

Copy the initialization file (`config.xml`) edited in (b), (c), and (d) to the executing node.

Copy the file to the following location on the executing node:

`/opt/jp1pcwebcon/conf`

(f) Making sure the shared disk is online

Executing

Make sure that the shared disk is online on the execution node. If the shared disk is not online, use the cluster software and the volume manager to bring it online.

(g) Performing an additional setup for PFM - Agent or PFM - RM information

Executing | Options

Use the setup file copied in (a) to perform an additional setup of the agent information for PFM - Agent or PFM - RM on the execution node.

To add the PFM - Agent information:

1. Stop the PFM - Web Console service on the executing node.

   Use the `jpcwstop` command to stop the services if the PFM - Web Console services are not registered with the cluster software. To perform a forced stop, execute the `jpcwstop` command with the `-immediate` option.

   When making changes to the Performance Management configuration such as adding PFM - Agent or PFM - RM after the services are registered with the cluster software, use the cluster software to stop the services. For details on changing the configuration of the cluster system, see *9.5 Changing the cluster system configuration (in UNIX)*.

2. Execute the setup command on the executing node.

   Execute the command as follows:

   ```
   jpcwagtsetup
   ```

   For details on the `jpcwagtsetup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

3. Start the PFM - Web Console service on the executing node.

   Start the PFM - Web Console service that you stopped in step 1.

(4) Configuring the cluster software

Set up PFM - Web Console in the cluster software. Perform this task on both the executing node and the standby node.

The procedure is as follows:

(a) Registering PFM - Web Console with the cluster software

Executing | Standby

If you intend to use PFM - Web Console in a logical host environment, register PFM - Web Console with the cluster software. Also, set up the environment so that PFM - Web Console is started and stopped based on instructions from the cluster software.

Generally, the following four command items are required when registering an

application in the cluster software: *Start*, *Stop*, *Monitor operations*, and *Forced stop*.

The following table lists and describes the settings for PFM - Web Console.

Table 9-8: Control commands for PFM - Web Console registered in the cluster software

Item	Explanation
Start	Execute the following command to start PFM - Web Console: `/opt/jp1pcwebcon/tools/jpcwstart`
Stop	Execute the following command to stop PFM - Web Console: `/opt/jp1pcwebcon/tools/jpcwstop`
Forced stop	Execute the following command to perform a forced stop of PFM - Web Console: `/opt/jp1pcwebcon/tools/jpcwstop -immediate`
Monitor operations	Use the `ps` command to check if the following process is running. `ps -ef | grep "`*process-name*`" | grep -v "grep` *process-monitored*`"` For details on process names, see *9.6.1(3) Service names*.

Note

- Do not configure PFM - Web Console to start automatically when the OS starts. When PFM - Web Console is registered in the cluster system, it is started and stopped by the cluster software.
- If the cluster software uses command return values to determine execution results, specify settings so that the command return values from PFM - Web Console are converted to the values that can be correctly interpreted by the cluster software. For details on the command return values for PFM - Web Console, check the reference documentation for each command.
- If you execute a `jpcwstop` command while PFM - Web Console is being used, it might delay the stop processing.

  To successfully register the `jpcwstop` command in the cluster software, create a script to wait for several minutes if a value of 4 is returned by the command, and then to execute the `jpcwstop` command again to register the command.

(b) Checking starting and stopping from the cluster software

Executing

Standby

Check whether the cluster software is operating correctly by using it to issue start and stop requests to PFM - Manager on each node.

9.4.4 Installing an upgrade for PFM - Agent or PFM - RM

To install an upgrade for PFM - Agent or PFM - RM in a physical host environment where PFM - Agent, PFM - RM, or PFM - Manager is running in a logical host environment:

1. Use the cluster software to stop all PFM services on each logical host.
2. Use the `jpcspm stop -key all` command to stop all PFM services on both the executing and standby physical hosts.
3. Install PFM - Agent or PFM - RM on each applicable executing host by overwriting the previous installation.
4. Install PFM - Agent or PFM - RM on each applicable standby host by overwriting the previous installation.
5. Set up Performance Management so that it can run.
6. Use the cluster software to start all PFM services on each logical host.
7. Use the cluster software to start all PFM services on both the executing and standby physical hosts.

For details on PFM - Agent-specific or PFM - RM-specific considerations, see the corresponding PFM - Agent or PFM - RM manual and the *Release Notes*.

9.4.5 Unsetup and uninstallation of PFM - Manager

This subsection describes the methods for performing unsetup and uninstallation of PFM - Manager in a cluster system.

(1) Before unsetup and uninstallation

The following describes notes on performing unsetup and uninstallation of PFM - Manager:

Notes regarding the order of unsetup:

PFM - Manager is required to execute PFM - Agent or PFM - RM. Therefore, when performing unsetup on PFM - Manager, it is necessary to consider its relationship with PFM - Agent or PFM - RM in the system and determine the work order for unsetup. The work order when unsetup is required is the same as the order for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Notes on stopping of services:

Stop all Performance Management programs and services running on the executing nodes and standby nodes on which unsetup is to be performed. Also, stop all PFM - Agent and PFM - RM services across the Performance

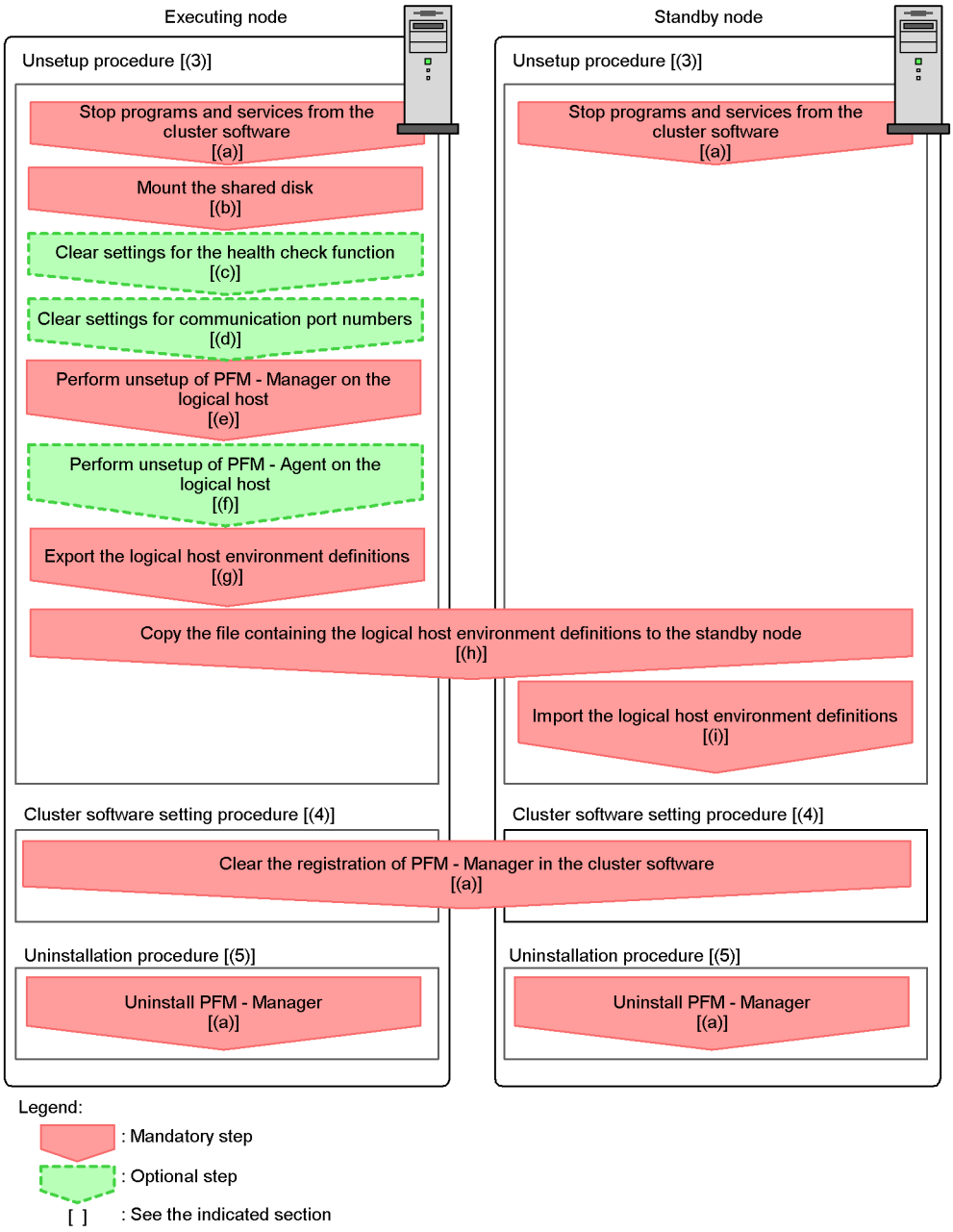
Management system connected to the instance of PFM - Manager that will be unsetup. For details on how to stop services, see *1. Starting and Stopping Performance Management*.

(2) Process flow for unsetup and uninstallation

The process flow for unsetup and uninstallation for PFM - Manager used on a logical host is explained below.

The following figure shows the process flow for uninstallation and unsetup.

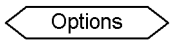
Figure 9-24: Process flow for unsetup and uninstallation of PFM - Manager used on a logical host (in UNIX)



Next, the unsetup procedures, procedures for clearing cluster software settings, and uninstallation procedures for PFM - Manager and the setting procedures for cluster software are explained below.

In the procedure explanation, the image 

indicates the items to be performed on the executing node, and the image 

indicates the items to be performed on the standby node. In addition, the image 

indicates the setup items required depending on the environment, and the optional setup items for when changing the default settings.

(3) Unsetup procedure

First, perform unsetup on the executing node. Next, export the logical host environment definitions for the executing node to a file. Finally, import the file containing the environment definitions to the standby node to apply the unsetup content from the executing node to the standby node.

The procedure is as follows:

(a) Stopping from the cluster software 

Use operations from the cluster software to stop Performance Management programs and services running on the executing node and the standby node. For details on how to stop programs and services, see the cluster software documentation.

(b) Making sure the shared disk is mounted 

Make sure that the shared disk is mounted. If the shared disk is not mounted, execute the `mount` command to mount it on the file system.

Note:

Even if the shared disk is unmounted, if there is a `jp1pc` directory and associated files in the environment directory of the logical host that is to be unsetup, setup is performed without mounting the shared disk. If that is the case, use the following procedure:

1. Use the `tar` command to archive the `jp1pc` directories in the environment directory of the logical host that is to be unsetup on the local disk.
2. Mount the shared disk.
3. If there is no environment directory of the logical host that is to be unsetup on the shared disk, create an environment directory.
4. Expand the `tar` file in the environment directory of the logical host that is to be unsetup on the shared disk.

5. Unmount the shared disk.
6. Delete the `jp1pc` directory and its associated files in the environment directory of the logical host that is to be unsetup on the local disk.

(c) Clearing settings for the health check function

Executing

Execute the following command on the PFM - Manager host on the executing node to clear the settings for the health check function.

```
jpcconf hc disable
```

For details on the `jpcconf hc disable` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(d) Clearing settings for communication port numbers

Executing Standby

This procedure is required only when port numbers have been set using the `jpcconf port define` command during the setup in an environment with a firewall.

To clear settings for communication port numbers:

1. Clear the settings for communication port numbers.

   Execute the `jpcconf port define` command to clear the settings for communication port numbers.

   For example, execute the following command to clear all the settings for port numbers for services that exist on the host with the logical host name `jp1-ha1`.

   ```
   jpcconf port define -key all -lhost jp1-ha1
   ```

   The `jpcconf port define` command is used to set the port numbers that are used for communications by PFM - Manager on the logical host or by other Performance Management programs. When entering a port number, a value of `0` will clear the setting. In addition, when this command is executed, the port numbers and service names (service names starting with `jp1pc` by default) for Performance Management defined in the services file are deleted

   For details on the `jpcconf port define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(e) Performing unsetup of a logical host for PFM - Manager

Executing

To perform unsetup of a logical host for PFM - Manager:

1. Check the logical host settings.

   Check the current settings before performing unsetup on the logical host environment. Check the logical host name and shared disk path.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

   An example of executing this command is as follows:

   ```
   C:\>jpchasetup list all

   Logical Host Name  Key      Environment Directory                  [Instance Name]
   -----------------  -------- -------------------------------------- ---------------------------
   jp1-ha1            mgr      "/usr/jp1/jp1pc"

   KAVE05136-I  The logical host startup information listing ended normally.
   ```

   For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Delete the logical host environment for PFM - Manager.

   When the `jpcconf ha unsetup` command is executed, the settings for starting PFM - Manager on the logical host are deleted. In addition, the files for the logical host on shared disks are also deleted. Execute the command as follows:

   ```
   jpcconf ha unsetup -key Manager -lhost jp1-ha1
   ```

   For details on the `jpcconf ha unsetup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

   Note:

   If the shared disk is offline, only the logical host settings will be deleted. The directories and files on the shared disk will not be deleted.

3. Check the logical host settings.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

Make sure that PFM - Manager has been deleted from the logical host environment.

For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(f) Performing unsetup for a logical host of PFM - Agent or PFM - RM

Executing Standby

This procedure is required only when there is PFM - Agent or PFM - RM on the same logical host from which unsetup will also be performed for PFM - Manager.

Perform unsetup of PFM - Agent or PFM - RM. For details on the unsetup procedure, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

(g) Exporting the logical host environment definitions

Executing

When a logical host environment to perform unsetup of PFM - Manager is created on the executing node, apply the settings information for the executing node to the standby node. First, export the logical host environment definitions for the executing node to a file.

Note:

To perform unsetup of a different instance of Performance Management from the same logical host, perform the export after all unsetup procedures are completed

To export the environment definitions:

1. Export the logical host environment definitions.

   For example, execute the following command to export the logical host environment definitions to the `lhostexp.conf` file. The export file allows an arbitrary file name.

   ```
   jpcconf ha export -f lhostexp.conf
   ```

   For details on the `jpcconf ha export` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(h) Copying the file containing the logical host environment definitions to the standby node

Executing Standby

Copy the file that has been exported in step (f) from the executing node to the standby node, so that it will be applied on the standby node.

Next, unmount the file system to complete the work. If this shared disk will continue to be used, it is not necessary to unmount the file system.

(i) Importing the file containing the logical host environment definitions

Standby

Import the export file copied from the executing node to the standby node, so that it will be applied to the standby node

Use the `jpcconf ha import` command to apply the Performance Management settings for the logical host created on the executing node to the standby node. If multiple instances of Performance Management have been set up on a single logical host, import all of the instances as one group.

To import the export file containing the logical host environment definitions:

1. Import the logical host environment definitions.

   Use the `jpcconf ha import` command to import the exported file of the logical host environment definitions copied from the executing node to the standby node.

   For example, execute the following command if the export file name is `lhostexp.conf`.

   ```
   jpcconf ha import -f lhostexp.conf
   ```

   When the command is executed, the environment settings for the standby node are changed to the same environment settings specified for the executing node that has been exported. Therefore, the settings for running PFM - Manager on a logical host are deleted. If you perform unsetup of Performance Management on another logical host, the relevant settings are also deleted.

   For details on the `jpcconf ha import` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Check the settings for the logical host environment.

   Execute the `jpcconf ha list` command in the same manner as for the executing node, to check the settings of the logical host.

   Execute the command as follows:

   ```
   jpcconf ha list -key all
   ```

   For details on the `jpcconf ha list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Cluster software setting procedure

(a) Clearing the registration of PFM - Manager in the cluster software

Executing Standby

Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

(5) Uninstallation procedure Executing Standby

(a) Performing uninstallation of PFM - Manager

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Notes:

- When performing uninstallation of PFM - Manager, stop all Performance Management programs and services on the node where uninstallation is to be performed.
- If uninstallation is performed on Performance Management without deleting the logical host environment, the environment directory might remain. When this happens, delete the environment directory.

9.4.6 Unsetup and uninstallation of PFM - Web Console

The procedures for performing unsetup and uninstallation of PFM - Web Console are explained below.

(1) Process flow for unsetup and uninstallation

The process flow for unsetup and uninstallation of PFM - Web Console on a logical host in a cluster system is explained below.

The following figure shows the process flow for unsetup and uninstallation.

Figure 9-25: Process flow for unsetup and uninstallation of PFM - Web Console used on a logical host (in UNIX)

The unsetup procedures, procedures for clearing cluster software settings, and uninstallation procedures are explained below.

The image Executing indicates the steps to be performed on the executing node, and the image Standby indicates the items to be performed on the standby node.

(2) Unsetup procedure

The unsetup procedure for PFM - Web Console is as follows:

(a) Stopping from the cluster software Executing Standby

Use the cluster software to stop all Performance Management programs and services active on the executing node and standby node. For details on how to stop programs

and services, see the cluster software documentation.

(b) Making sure the shared disk is online Executing

Make sure that the shared disk is online. If the shared disk is not online, use the cluster software and the volume manager to bring it online.

(3) Configuring the cluster software

(a) Unregister PFM - Web Console with the cluster software Executing Standby

Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

(4) Uninstallation procedure

(a) Uninstalling PFM - Web Console Executing Standby

Uninstallation is performed separately for the executing node and the standby node. The uninstallation procedure for PFM - Web Console is the same as for a non-cluster system. For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

Note:

If the storage directory for the bookmark definition information has been changed from the default setting, it will not be deleted when you uninstall PFM - Web Console. You need to delete it manually after performing the uninstallation.

9.5 Changing the cluster system configuration (in UNIX)

After a system is configured and the operation started, as the business expands and processed data volume increases, the system's cluster configuration might need to be changed with the addition of servers or introduction of new applications.

For this reason, the following the Performance Management configuration changes need to be studied in response to changes in the cluster configuration of the monitoring target system:

- Addition of PFM - Agent or PFM - RM due to the addition of a monitored system
- Removal of PFM - Agent or PFM - RM due to the removal of a monitored system

This section describes the procedures for making changes to the Performance Management configuration when using a cluster system on a logical host.

9.5.1 Adding PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be added in order to monitor the performance of servers or applications that are newly added to a system.

When you add PFM - Agent or PFM - RM with a new product ID that has not previously been used in the Performance Management system, you need to set up the agent information in PFM - Manager and PFM - Web Console.

For details on product IDs, see the appropriate PFM - Agent or PFM - RM manual.

Point:

Agent information is used by PFM - Manager and PFM - Web Console to manage and display PFM - Agent or PFM - RM.

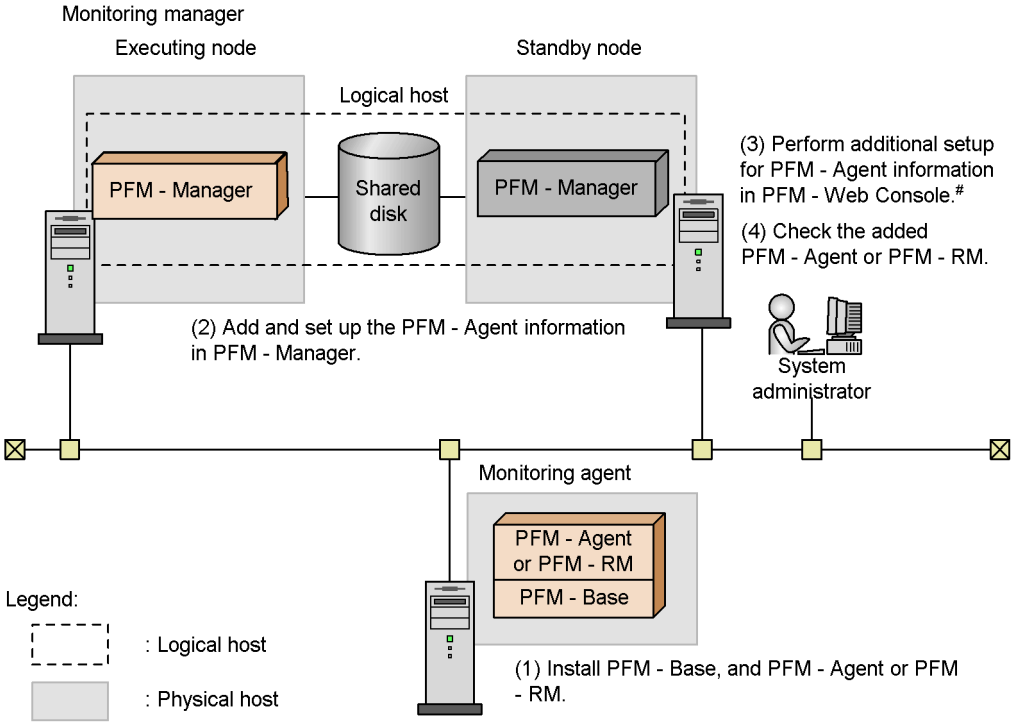
Notes:

- Stop PFM - Manager and all Performance Management programs and services on that node before adding PFM - Agent or PFM - RM. For details on how to stop services, see *1. Starting and Stopping Performance Management*.
- It is also necessary to stop PFM - Manager used on a logical host while work is being performed. An error might occur if you execute the `jpcconf agent setup` command or the `jpcwagtsetup` command to add PFM - Agent or PFM - RM before the Performance Management programs and services are completely stopped. In such cases, first make sure that all services have completely stopped, and then re-execute the `jpcconf agent setup` command or the `jpcwagtsetup` command.

The following figure shows the process flow for adding PFM - Agent or PFM - RM to

a Performance Management system in a logical host environment.

Figure 9-26: Process flow for adding PFM - Agent or PFM - RM to a Performance Management system in a logical host environment



The procedure is as follows:

(1) Installing PFM - Base and either PFM - Agent or PFM - RM

Perform a new installation of PFM - Base and either PFM - Agent or PFM - RM on the host where Performance Management will be used to monitor performances.

For details on how to install, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

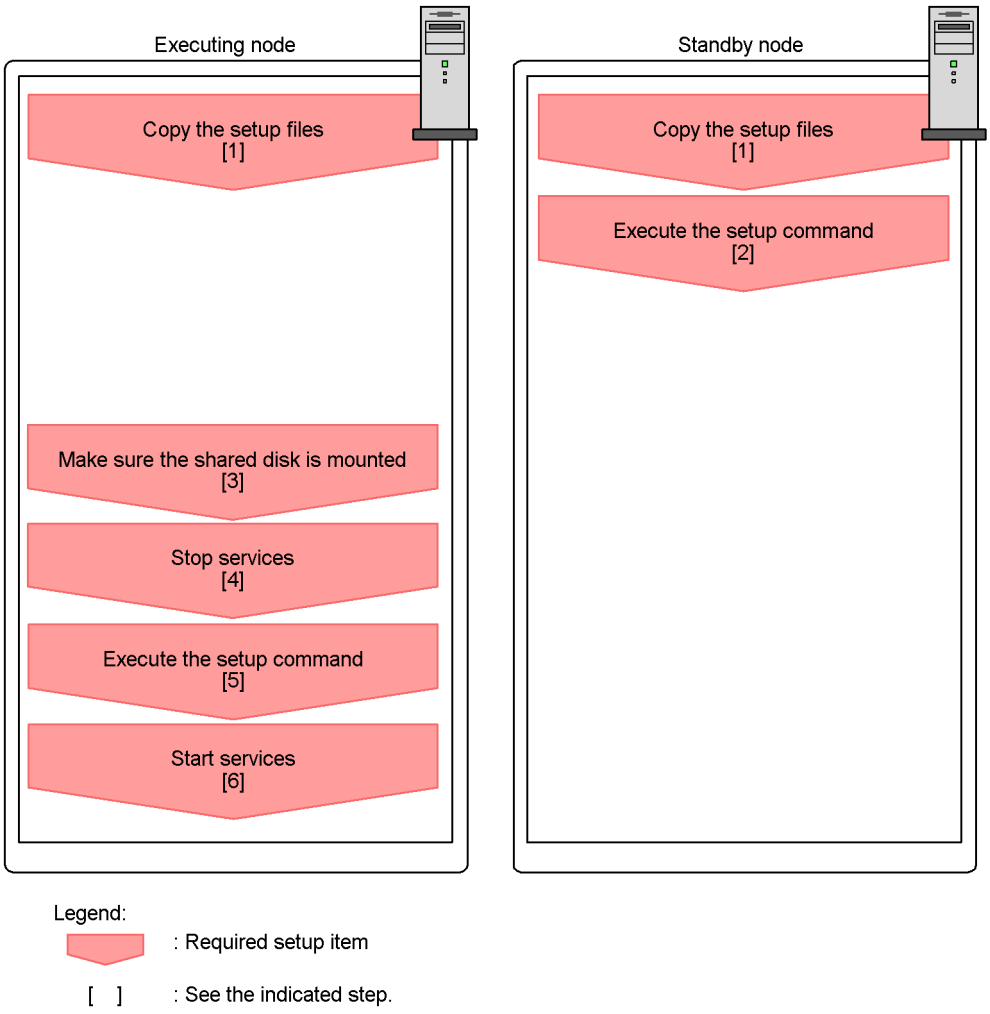
(2) Adding and setting up the PFM - Agent or PFM - RM information in PFM - Manager

The process flow for adding and setting up the agent information of PFM - Agent or PFM - RM into PFM - Manager used on a logical host in a cluster system is described below.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

Perform the addition and setup of the agent information on the standby node first. When the addition and setup are completed on the standby node, next perform setup on the executing node.

Figure 9-27: Process flow for adding and setting up PFM - Agent or PFM - RM into PFM - Manager



Notes:

- If you add another PFM - Agent or PFM - RM to the same host as PFM - Manager, an additional setup is not required.
- If you install a different version of PFM - Agent or PFM - RM with the same product ID on a different host, first set up the older version of PFM - Agent or PFM - RM, and then set up the newer version of PFM - Agent or PFM - RM.

The procedure for adding and setting up agent information for PFM - Agent or PFM - RM is explained below.

The image Executing indicates a procedure used on the executing node, and the image Standby indicates a procedure used on the standby node.

1. Copying the setup files Executing Standby

   Copy the PFM - Agent or PFM - RM setup files to the executing and standby nodes of PFM - Manager.

   For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

2. Executing the setup command Standby

   Execute the `jpcconf agent setup` command on the standby node, and then perform additional setup for the new agent.

   Execute the following command:

   ```
   jpcconf agent setup -key xxxx
   ```

   xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

   For example, execute the following command to set up PFM - Agent for Oracle:

   ```
   jpcconf agent setup -key Oracle
   ```

   For details on the `jpcconf agent setup` command, see the chapter that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

3. Making sure the shared disk is mounted Executing

   Make sure that the shared disk has been mounted on the executing node. Write the agent information to the shared disk with the additional setup procedure. Use the cluster software or the volume manager to check that the shared disk has been mounted.

4. Stopping services Executing

   Stop the Performance Management programs and services on the executing node.

Use the cluster software to stop the programs and services.

5. Executing setup commands Executing

   Execute the `jpcconf agent setup` command on the executing node in the same manner as for the standby mode in order to add and set up the new agent.

   ```
   jpcconf agent setup -key xxxx
   ```

   xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

   For example, execute the following command to set up PFM - Agent for Oracle:

   ```
   jpcconf agent setup -key Oracle
   ```

   For details on the `jpcconf agent setup` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

6. Starting services Executing

   Start the Performance Management programs and services that were stopped on the executing node.

(3) Adding and setting up PFM - Agent or PFM - RM in PFM - Web Console

Perform additional setup for PFM - Agent or PFM - RM information in PFM - Web Consoles that are used on a logical host in a cluster system.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent, or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

For details on the additional setup procedure, see *9.2.3(3)(a) Performing an additional setup for PFM - Agent or PFM - RM information* .

(4) Checking PFM - Agent or PFM - RM added and set up

Check PFM - Agent or PFM - RM that was added and set up.

1. Start the services in the nodes of PFM - Agent or PFM - RM.

   Start the Performance Management programs and services in the nodes of the newly added PFM - Agent or PFM - RM.

2. Check if PFM - Agent or PFM - RM has been added correctly.

   Execute the `jpctool service list` command to check if PFM - Manager has been connected correctly.

   Execute the command as follows:

   ```
   jpctool service list -id "*"
   ```

   For details on the `jpctool service list` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

9.5.2 Deleting PFM - Agent or PFM - RM

PFM - Agent or PFM - RM might be deleted when a monitored system is removed from the entire system due to changes in the system configuration.

Delete PFM - Agent or PFM - RM from the Performance Management system used in the logical host. Deletion needs to be performed on both the PFM - Manager host and the PFM - Web Console host.

Notes:

- Stop all Performance Management programs and services in the node from which PFM - Agent or PFM - RM will be deleted.
- If PFM - Agent or PFM - RM to be deleted is in the same node as PFM - Manager, it is necessary to first use the `jpctool service delete` command to delete the agent information, and then restart PFM - Manager.

(1) Deleting PFM - Agent or PFM - RM from PFM - Manager

To delete PFM -Agent from PFM - Manager:

1. Delete the agent information.

   Delete the agent information managed by PFM - Manager.

   Execute the command as follows:

   `jpctool service delete -id` *xxxx* `-host` *host-name* `-lhost` *logical-host-name*

   xxxx indicates the service ID for each PFM - Agent or PFM - RM.

   For example, execute the following command to delete the agent information for PFM - Agent for Oracle in the logical host environment with the host name `jp1` and the logical host name `jp1-ha1`.

```
jpctool service delete -id "O*" -host jp1 -lhost jp1-ha1
```

For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

2. Perform unsetup and uninstall PFM - Agent or PFM - RM.

   Perform unsetup and uninstall PFM - Agent or PFM - RM. For details on how to perform unsetup and how to uninstall PFM - Agents or PFM - RM, see the chapters that describe operations on cluster systems in the appropriate PFM - Agent or PFM - RM manual.

   If the PFM - Agent or PFM - RM to be deleted is in the same node as PFM - Manager, it is necessary to restart PFM - Manager after unsetup and uninstallation have been performed. Go to step 3.

3. Restart PFM - Manager.

   Restart PFM - Manager.

(2) Deleting PFM - Agent or PFM - RM from PFM - Web Console

To delete PFM - Agent from PFM - Web Console:

1. Restart PFM - Web Console on the executing node.

   Apply the changes made by the deleted PFM - Agent or PFM - RM information to PFM - Web Console.

   After performing unsetup and uninstalling PFM - Agent or PFM - RM, restart PFM - Web Console on the executing node.

   Reference note:

   > This restart is not required on the standby node since PFM - Web Console restarts when a failover occurs.

2. Delete the alarm definition information and report definition information.

   Delete the unnecessary alarm definition information and report definition information as necessary.

   For details on deleting alarm definition information, see *6.4.9(2) Deleting an alarm* or *6.7.6 Deleting an alarm*. For details on deleting report definition information, see *5.3.12(2) Deleting a report* or *5.5.2 Deleting an unnecessary report*.

9.5.3 Changing logical host names after starting operation

This subsection describes the procedures (performed on the Performance Management system) necessary for changing the logical host names of the PFM - Manager host,

PFM - Agent host, or PFM - RM host after the Performance Management system is configured.

To change a logical host name, you must first use the `jpcconf host hostname` command to change the monitoring host name.

If you execute the `jpcconf host hostname` command, all existing information, including definition and performance information, is inherited. For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

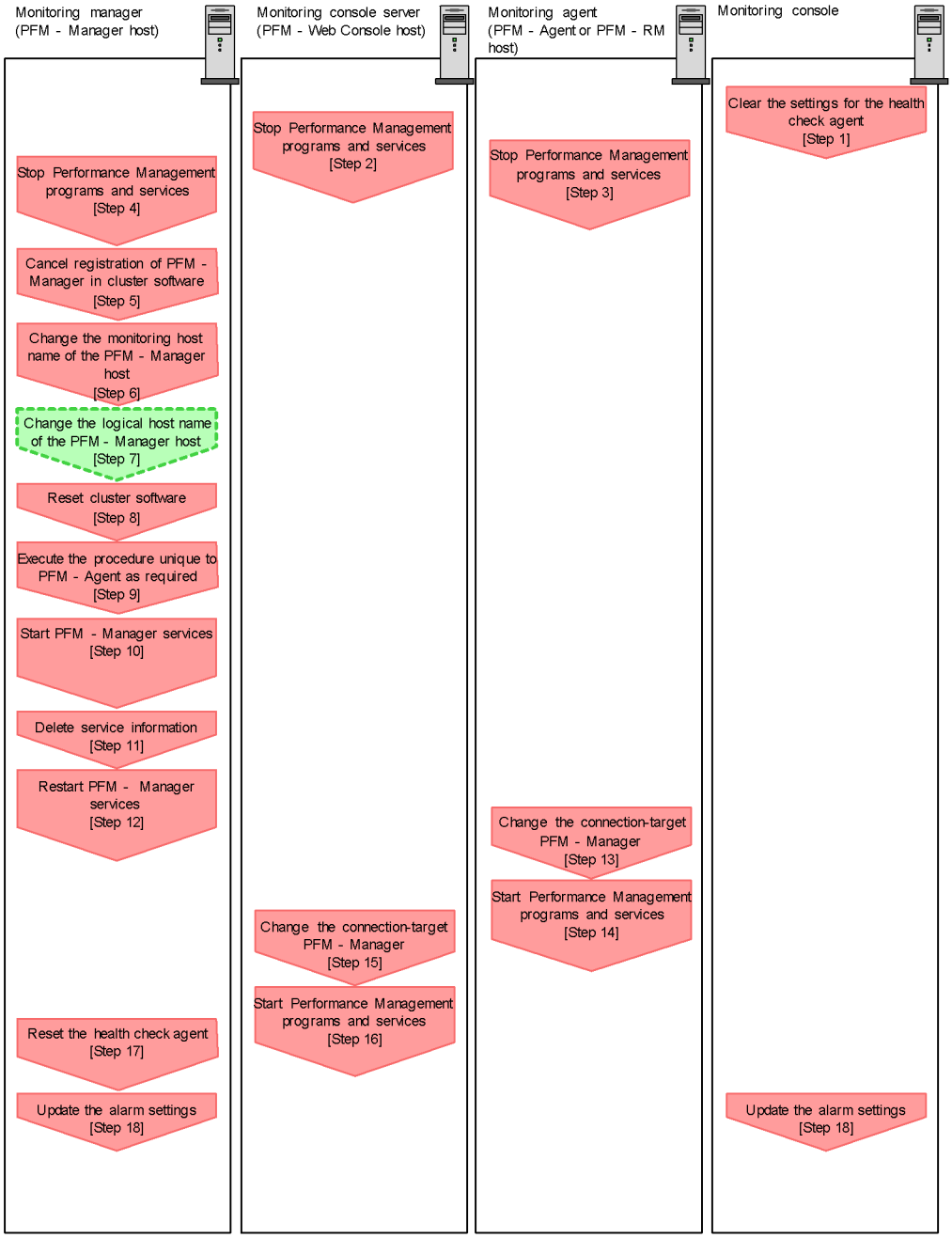
(1) Changing the PFM - Manager logical host name

You must work on the following hosts when changing the PFM - Manager logical host name:

- PFM - Manager host
- PFM - Web Console host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Figure 9-28: Process flow for changing the PFM - Manager host name



Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Clear the setting for the health check agent.

   If you are using the health check function, you can delete the agent definitions for the health check agent using your PFM - Web Console (by deleting the definitions from the management folder in the Agents tree and removing the association between the alarm tables and the definitions). For details on how to change the agent definition, see *6. Monitoring Operations with Alarms*.

2. Stop services on the PFM - Web Console host.

   On the PFM - Web Console host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcwstop` command.

3. Stop services on the PFM - Agent or PFM - RM host.

   On the PFM - Agent or PFM - RM host connected to PFM - Manager for which you intend to change the host name, stop all Performance Management programs and services. To stop services, use the `jpcspm stop` command.

4. Stop services on the PFM - Manager host.

   Use operations from the cluster software to stop Performance Management programs and services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

5. Cancel the registration of PFM - Manager from the cluster software.

   Delete the settings related to PFM - Manager on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

6. Change the monitoring host name of PFM - Manager host.

   Execute the `jpcconf host hostname` command to change the monitoring host name.

   In the following example, the logical host name is changed from `lhostA` to `lhostB`.

   ```
   jpcconf host hostname -lhost lhostA -newhost lhostB -d
   d:\backup -dbconvert convert
   ```

   For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

Reference note:

The directory specified with the `-d` option of the `jpcconf host hostname` command requires disk space equal to the total size of the PFM - Agent and PFM - RM Store databases on the specified host.

For example, if PFM - Agent for Enterprise Applications and PFM - Agent for Oracle are located in the environment directory, the directory to be specified with the `-d` option will require disk space equal to the total size of the Store databases of the programs. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

7. Change the PFM - Manager logical host name.

   Change the PFM - Manager logical host name. Edit the settings in the `hosts` and `jpchosts` files, if necessary.

8. Reconfigure the cluster software.

   For details, see *9.4.2(4) Cluster software setting procedure*.

9. Perform any PFM - Agent-specific steps, if necessary.

   If PFM - Agent has been installed on the PFM - Manager host, the PFM - Agent-specific procedure might be necessary. The following table describes whether the PFM - Agent-specific procedure is necessary.

   Table 9-9: PFM - Agent-specific procedure is necessary or not

Configuration		Necessity and reference
The version of PFM - Agent installed on the PFM - Manager host is 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The version of PFM - Agent installed on the PFM - Manager host is before 09-00.	The following PFM-Agent: • PFM - Agent for Enterprise Applications • PFM - Agent for Microsoft SQL Server	The Agent-specific procedure is necessary. For details, see *(4) Optional Agent-specific steps for host name changes*.
	Other than the above (including the case where PFM - RM is installed on the PFM - Manager host)	The Agent-specific procedure is not necessary.

If a PFM - Agent-specific step is to be performed, complete the reference step

shown in this table before proceeding to the next step.

10. Start services on the PFM - Manager host.

    Use the cluster software to start all PFM - Manager services.

11. Delete service information on the PFM - Manager host.

    Even though the PFM - Manager host name is changed, the service information of the Performance Management programs with the old host name remains the same. If you changed the PFM - Manager host name, you need to delete the old PFM - Manager service information. For example, to change the logical host name of the PFM - Manager host from `lhostA` to `lhostB`, execute the following command on the PFM - Manager host, and then delete all PFM - Manager service information from host `lhostA`.

    ```
    jpctool service delete -id "P*" -host lhostA -lhost lhostB
    jpctool service delete -id "0*" -host lhostA -lhost lhostB
    ```

    For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

12. Restart services on the PFM - Manager host.

    Restart the PFM - Manager services using the cluster software to apply the changes made by the deleted service information.

13. Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host.

    Change the settings for PFM - Manager for the connection destination on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the logical host name. Use the `jpcconf mgrhost define` command to change the settings for PFM - Manager for the connection destination. For example, if the host name of PFM - Manager for the connection destination will be changed to *lhostB*, specify and execute the command as follows:

    ```
    jpcconf mgrhost define -host lhostB
    ```

    For details on the `jpcconf mgrhost define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

14. Start services on the PFM - Agent or PFM - RM host.

    Start the Performance Management programs and services on the PFM - Agent or PFM - RM host connected to PFM - Manager for which you have changed the

logical host name. To start services, use `jpcspm start` command.

15. Change PFM - Manager for the connection destination on the PFM - Web Console host.

    Change the settings for PFM - Manager for the connection destination on the PFM - Web Console host connected to PFM - Manager for which you have changed the logical host name. Change the information in the Windows initialization file (`config.xml`) to change the settings for PFM - Manager for the connection destination. For details, see the chapter describing installation and setup (in UNIX) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

16. Start services on the PFM - Web Console host.

    Start the Performance Management programs and services on the PFM - Web Console host connected to PFM - Manager for which you have changed the logical host name. To start services, use the `jpcwstart` command.

17. Reconfigure the definition for the health check agent.

    If you have been using the health check function, reconfigure the definition (that has been cleared at step 1) of the health check agent after changing the host name.

18. Update the alarm settings.

    In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

    - The action handler of the PFM - Manager host is specified for the action handler that executes actions.

      Edit the alarm to set `PH1`<*new-pfm-manager-host-name*> for the action handler that executes actions.

    - JP1 events are issued by actions.

      Set the JP1 event settings in the action again.

    For details on how to edit alarms, see *6. Monitoring Operations with Alarms*.

19. Update the JP1 system event settings.

    If either of the following conditions is met, use the PFM - Web Console browser to update the JP1 system event settings:

    - The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
    - The old host name is specified as the name of the monitoring console host for JP1 system events.

20. Check whether the JP1 system event settings are properly updated.

Check the following items after changing the logical host name:

- Collection of performance data

  Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).

- Execution of the `jpctool db dump` command

  Make sure that there is no problem in outputting the collected performance data.

- The report definitions and alarm definitions

  Make sure that there are no problems with the report definitions and alarm definitions created from the browser.

- The actions

  Make sure that there is no problem in executing the created actions.

21. Log on to the network management product (NNM) again if it is linked for operation monitoring.

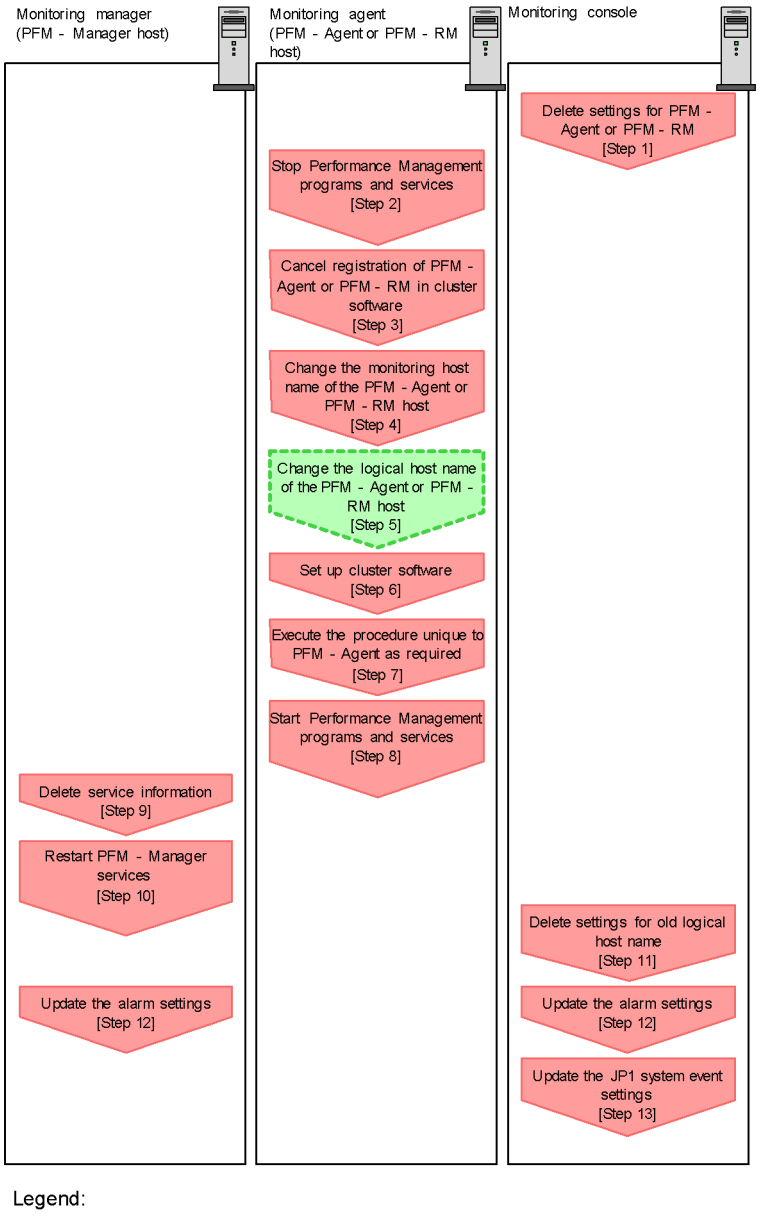
(2) Changing the PFM - Agent or PFM - RM logical host name

You must work on the following hosts when changing the PFM - Agent or PFM - RM logical host name:

- PFM - Manager host
- PFM - Agent or PFM - RM host
- Monitoring console

The following figure shows the process flow for changing the host name.

Figure 9-29: Process flow for changing the PFM - Agent or PFM - RM monitoring host name



Use the following procedure to set the display conditions (Each step corresponds to the step number in the figure above):

1. Delete the PFM - Agent or PFM - RM information.

   Use your PFM - Web Console browser to delete the agent definitions from the PFM - Agent or PFM - RM host whose logical host name is to be changed (by deleting the definitions from the management folder in the Agents tree and disassociating any alarm tables from them).

   For details on how to change the agent definition, see *3. Monitoring Agents* or *6. Monitoring Operations with Alarms*.

2. Stop the services on the PFM - Agent or PFM - RM host.

   Stop all Performance Management programs and services on the PFM - Agent or PFM - RM host for which you intend to change the logical host name. Use operations from the cluster software to stop Performance Management programs and services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

3. Unregister PFM - Agent or PFM - RM from the cluster software.

   Delete the settings related to PFM - Agent or PFM - RM on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

4. Change the monitoring host name for the PFM - Agent or PFM - RM host.

   Execute the `jpcconf host hostname` command to change the monitoring host name.

   In the following example, the logical host name is changed from `lhostA` to `lhostB`.

   ```
   jpcconf host hostname -lhost lhostA -newhost lhostB -d
   d:\backup -dbconvert convert
   ```

   For details on the `jpcconf host hostname` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

Reference note:

The directory specified with the `-d` option of the `jpcconf host hostname` command requires disk space equal to the total size of the PFM - Agent and PFM - RM Store databases on the specified host.

For example, if PFM - Agent for Enterprise Applications and PFM - Agent for Oracle are located in the environment directory, the directory to be specified with the `-d` option will require disk space equal to the total size of the Store databases of the programs. You do not need to include the size of the Store database for the PFM - Manager Master Store service in the total size.

5. Change the PFM - Agent or PFM - RM logical host name.

   Change the PFM - Agent or PFM - RM logical host name. Edit the settings in the `hosts` and `jpchosts` files, if necessary.

6. Configure the cluster software.

   For details, see *9.4.2(4) Cluster software setting procedure*.

7. Perform any PFM - Agent-specific steps, if necessary.

   The following table describes whether the PFM - Agent-specific procedure is necessary.

   Table 9-10: Whether the PFM - Agent-specific procedure is necessary

Configuration		Necessity and reference
The monitoring host name to be changed is PFM - Agent version 09-00 or later.		Whether the PFM - Agent-specific procedure is necessary depends on PFM - Agent. For details on the PFM - Agent-specific procedure, see the chapters describing installation and setup in the PFM - Agent manuals.
The monitoring host name to be changed is PFM - Agent for versions earlier than 09-00.	The following PFM-Agent: • PFM - Agent for Enterprise Applications • PFM - Agent for Microsoft SQL Server	The Agent-specific procedure is necessary. For details, see *(4) Optional Agent-specific steps for host name changes*.
	Other than the above (including the case where the monitoring host name to be changed is PFM - RM)	Agent-specific procedure is not necessary.

   If a PFM - Agent-specific step is to be performed, complete the reference step shown in this table before proceeding to the next step.

8. Start services on the PFM - Agent or PFM - RM host.

   Start Performance Management programs and services from the cluster software on the PFM - Agent or PFM - RM host for which you have changed the logical host name.

9. Delete service information on the PFM - Manager host.

   Even though the PFM - Agent or PFM - RM host name is changed, the service information of Performance Management programs to which the old host name is added remains the same. If you changed the PFM - Agent or PFM - RM host name, you need to delete the old PFM - Agent or PFM - RM service information. For example, to delete the information on the Agent Store service of PFM - Agent for Oracle on the `lhostB`, execute the following command on the PFM - Manager host:

   ```
   jpctool service delete -id "OS*" -host lhostB
   ```

   For details on the `jpctool service delete` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

10. Restart services on the PFM - Manager host.

    Restart the PFM - Manager services using the cluster software to apply the changes made by the deleted service information.

11. Delete the PFM - Agent or PFM - RM settings for the old logical host name.

    Use the PFM - Web Console browser to delete the agent definition of the PFM - Agent or PFM - RM host for which you changed the logical host name. After that, set the new definition for the agent.

    For details on how to change the agent definition, see *3. Monitoring Agents*.

12. Update the alarm settings.

    In the following cases, you must update the alarm settings by using the `jpctool alarm` command of the PFM - Manager host or the monitoring console.

    - When the action handler of the PFM - Agent or PFM - RM host is specified for the action handler that executes actions.

      Edit the alarm to set `PH1`<*new-pfm-agent-or-pfm-rm-host-name*> for the action handler that executes actions.

    - When JP1 events are issued by actions.

      Set the JP1 event settings in the action again.

    For details on how to edit alarms, see *6. Monitoring Operations with Alarms*.

13. Update the JP1 system event settings.

    If either of the following conditions is met, use your PFM - Web Console browser to update the JP1 system event settings:

    - The old host name is specified as the name of the event server that connects to JP1 Base for JP1 system events.
    - The old host name is specified as the name of the monitoring console host for JP1 system events.

14. Check whether the JP1 system event settings are properly updated.

    Check the following items after changed the settings:

    - Collection of the performance data

      Make sure that the performance data can be collected for a period at least twice as long as the time period specified as the collection interval (**Collection Interval**).

    - Execution of the `jpctool db dump` command

      Make sure that there is no problem in outputting the collected performance data.

    - The report definitions and alarm definitions

      Make sure that there are no problem with the report definitions and alarm definitions created by the browser.

    - The actions

      Make sure that there is no problem in executing the created actions.

(3) Changing the PFM - Web Console logical host name

To change the PFM - Web Console logical host name:

1. Stop services on the PFM - Web Console host.

   Use operations from the cluster software to stop Performance Management programs and services running on the executing and standby nodes. For details on how to stop programs and services, see the cluster software documentation.

2. Cancel the registration of PFM - Web Console from the cluster software.

   Delete the settings related to PFM - Web Console on the logical host from the cluster software. For details on how to delete settings, see the cluster software documentation.

3. Edit the PFM - Web Console host information in the initialization file (`config.xml`) to refer to the new logical host name.

   This step is necessary when the logical host name has been set for the `ownHost`

parameter in the <vsa> - <vserver-connection> tag of the Windows initialization file (config.xml).

For details on the procedure, see *9.4.3(3)(c) Setting up PFM - Web Console (logical host)* and *9.4.3(3)(e) Copying the initialization file (config.xml) to the executing node*.

4. If the integrated management product (JP1/IM) is linked for operation monitoring, change the host name specified in each applicable definition file or in the property value for each service.

   The location of the host name setting depends on the type of JP1 event that is used.

   - If a JP1 user event is used:

     Change the host name in the definition files for the tool launcher and for opening monitor windows. For details, see *10.3.2(3) Editing and copying the definition files for linkage*.

   - If a JP1 system event is used:

     Change the host name in the Monitoring Console Host property value for each service. For details, see *10.3.2(1) Configuring so that JP1 events are issued*.

   For details on an integrated management product (JP1/IM), see *10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring*.

5. If the network management product (NNM) is linked for operation monitoring, change the host name in the definition file.

   Change the PFM - Web Console host name specified in the NNM linkage definition file (jpcnnm.ini) to a new host name.

   For details, see *11.2.3(3) Modifying the NNM linkage definition file*.

6. Change the PFM - Web Console logical host name.

7. Reconfigure the cluster software.

   For details on the setting procedure, see *9.4.3(4) Configuring the cluster software*.

8. Start services on the PFM - Web Console host.

   Use operations from the cluster software to starts the PFM - Web Console services.

9. If the integrated management product (JP1/IM) is linked, restart the product (JP1/IM).

(4) Optional Agent-specific steps for host name changes

This subsection describes the PFM - Agent-specific steps necessary to perform the following operations for each product:

- Changing the PFM - Manager logical host name
- Changing the PFM - Agent or PFM - RM logical host name

For details on when it is necessary to perform these steps, see *(1) Changing the PFM - Manager logical host name* and *(2) Changing the PFM - Agent or PFM - RM logical host name*.

(a) In PFM - Agent for Enterprise Applications

Execute the `jpcconf inst setup` command for all created instance environments. For example, if an instance environment `o246bci_SD5_00` exists in PFM - Agent for Enterprise Applications, execute the following command:

```
jpcconf inst setup -key agtm -inst o246bci_SD5_00 -lhost
jp1-halr3
```

The `jpcconf inst setup` command is an interactive command that returns a command prompt when executed. At the `ASHOST` prompt, enter the new host name, and press the **Enter** key when the other prompts come up. If you press the **Enter** key at a prompt without entering a value, the existing value is assumed.

(b) In PFM - Agent for Microsoft SQL Server

Execute the `jpcconf inst setup` command for all created instance environments. For example, if an instance environment `default` exists in PFM - Agent for Microsoft SQL Server, execute the following command:

```
jpcconf inst setup -key agtq -inst default -lhost jp1-halSQL
```

The `jpcconf inst setup` command is an interactive command that returns a command prompt when executed. At the `SQL_HOST` prompt, enter the new host name, and press the **Enter** key when the other prompts come up. If you press the **Enter** key at a prompt without entering a value, the existing value is assumed.

9.6 Cluster system operations

This section describes operations necessary to use Performance Management on a logical host in a cluster system. Operations necessary for using Performance Management on a logical host in a cluster system include:

- Starting and stopping Performance Management
- Managing user accounts
- Managing monitoring agents in an integrated manner
- Collecting and managing the operation management data
- Creating operation management reports
- Performing realtime operation monitoring by alarms
- Performing backup and restore
- Performing the required operation when a failover occurs

9.6.1 Starting and stopping Performance Management in a cluster system

This section describes starting up and stopping Performance Management on a logical host in a cluster system.

The order to start up and stop Performance Management is the same as for non-cluster systems. For details, see *1. Starting and Stopping Performance Management*.

(1) Starting up Performance Management

This section describes starting up Performance Management on a logical host in a cluster system.

(a) Starting services manually

To start up Performance Management used on a logical host, use the cluster software to start up the logical host on which Performance Management has been registered.

Note:

If you start up Performance Management using a method other than the cluster software, there might be a difference between the actual Performance Management status and the status controlled by the cluster software, causing an error to be assessed.

(b) Starting services automatically

If you wish to automatically start up Performance Management used on a logical host when starting up the cluster system, set the system so that the cluster software automatically starts up the logical host on which Performance Management has been registered.

(2) Stopping Performance Management

This subsection describes stopping Performance Management on a logical host in a cluster system.

(a) Stopping services manually

Use the cluster software to stop the logical host on which Performance Management has been registered to stop Performance Management used on a logical host.

Note:

- If you stop Performance Management using a method other the cluster software, such as by using the `jpcspm stop` command, there might be a difference between the actual Performance Management status and the status controlled by the cluster software, causing an error to be assessed.
- Use the cluster software to stop Performance Management if, when changing Performance Management settings, you want to only stop Performance Management without stopping resources such as the shared disk and logical IP address. If the cluster software does not have the ability to stop Performance Management only, temporarily suppress monitoring of Performance Management actions, and then use the `jpcspm stop` command to manually stop Performance Management. In such cases, you need to prepare a mechanism to suppress monitoring of actions when you register Performance Management in the cluster,

(b) Stopping services automatically

If you wish to automatically stop Performance Management used on a logical host when stopping the cluster system, set the system so that the cluster software automatically stops the logical host on which Performance Management has been registered.

Point:

Methods to stop Performance Management include stopping the logical host and then stopping the node, or performing failovers for the logical host to another node and then stopping the node.

(3) Service names

Performance Management on a logical host has the following service names (in Windows) or process names (in UNIX or Linux), and they are different from cases in which Performance Management is run in a non-cluster system.

Notes about the current directory when a logical host is used:

When PFM - Manager is used on a logical host, the current directory of the services is the directory on the shared disk on which you configured the environment.

For that reason, the services directory name displayed in the window of PFM - Web Console is not the installation directory but is instead the directory on the shared disk.

The following table lists Windows service names or process names on the physical host and logical host. INST means the instance name and LHOST means the logical host name.

Table 9-11: Service names on physical and logical hosts (in Windows)

Performance Management service name	Windows service name on physical host	Windows service name on logical host
Action Handler	PFM - Action Handler	PFM - Action Handler [*LHOST*]
Agent Collector and Remote Monitor Collector (for a single instance)	PFM - Agent Collector for *xxxx*#	PFM - Agent Collector for *xxxx*# [*LHOST*]
Agent Collector and Remote Monitor Collector (for multi-instances)	PFM - Agent Collector for *xxxx*# *INST*	PFM - Agent Collector for *xxxx*# *INST* [*LHOST*]
Agent Collector (for health check agent)	PFM - Agent for HealthCheck	PFM - Agent for HealthCheck [*LHOST*]
Agent Store and Remote Monitor Store (for a single instance)	PFM - Agent Store for *xxxx*#	PFM - Agent Store for *xxxx*# [*LHOST*]
Agent Store and Remote Monitor Store (for multi-instances)	PFM - Agent Store for *xxxx*# *INST*	PFM - Agent Store for *xxxx*# *INST* [*LHOST*]
Agent Store (for health check agent)	PFM - Agent Store for HealthCheck	PFM - Agent Store for HealthCheck [*LHOST*]
Correlator	PFM - Correlator	PFM - Correlator [*LHOST*]
Master Manager	PFM - Master Manager	PFM - Master Manager [*LHOST*]

Performance Management service name	Windows service name on physical host	Windows service name on logical host
Master Store	PFM - Master Store	PFM - Master Store [*LHOST*]
Name Server	PFM - Name Server	PFM - Name Server [*LHOST*]
Trap Generator	PFM - Trap Generator	PFM - Trap Generator [*LHOST*]
Web Console	PFM - Web Console	PFM - Web Console
Web Service	PFM - Web Service	PFM - Web Service
View Server	PFM - View Server	PFM - View Server [*LHOST*]

#

xxxx indicates the name of the monitored program for each PFM - Agent or PFM - RM.

Table 9-12: Process names on physical and logical hosts (in UNIX)

Performance Management service name	Process name on physical host	Process name on logical host
Action Handler	jpcah	jpcah *LHOST*
Agent Collector and Remote Monitor Collector (for a single instance)	jpcagt*X*#	jpcagt*X*# *LHOST*
Agent Collector and Remote Monitor Collector (for multi-instances)	jpcagt*X*#*_INST*	jpcagt*X*#*_INST LHOST*
Agent Collector (for health check agent)	jpcagt0	jpcagt0 *LHOST*
Agent Store and Remote Monitor Store (for a single instance)	agt*X*#/jpcsto	agt*X*#/jpcsto *LHOST*
Agent Store and Remote Monitor Store (for multi-instances)	agt*X*#/jpcsto*_INST*	agt*X*#/jpcsto*_INST LHOST*
Agent Store (for health check agent)	agt0/jpcsto	agt0/jpcsto *LHOST*
Correlator	jpcep	jpcep *LHOST*

Performance Management service name	Process name on physical host	Process name on logical host
Master Manager	jpcmm	jpcmm *LHOST*
Master Store	mgr/jpcsto	mgr/jpcsto *LHOST*
Name Server	jpcnsvr	jpcnsvr *LHOST*
Trap Generator	jpctrap	jpctrap *LHOST*
View Server	jpcvsvr	jpcvsvr *LHOST*

#

X indicates the product ID of each PFM - Agent or PFM - RM.

Table 9-13: Process names on physical and logical hosts

Performance Management service name	Process name on physical host	Process name on logical host
Web Console	cjstartweb# PFMWebConsole	Same as on physical host
Web Service	httpsd# -R /opt/jp1pcwebcon/CPSB/httpsd/libexec	Same as on physical host
	cprfd# -PRFID PFMWebCon -CTMID PFMWebCon	Same as on physical host

#

When you display process information using the `ps` command, process names might appear with their absolute paths in the command column, or might appear with different options from those shown above. Check how the process name appears in your environment before using it.

9.6.2 Managing user accounts in a cluster system

The system administrator logs on to the system from the window of PFM - Web Console and manages user accounts.

(1) Logging on to PFM - Web Console

The procedure for logging on to PFM - Web Console is the same as that for a non-cluster system. However, enter the following URL in the browser to display the PFM Web Console login window:

`http://`*PFM - Web Console-installation-server-name*`:20358/PFMWebConsole/login.do`

For the *server-name*, specify the logical IP address or logical host name of the PFM - Web Console host.

For details on the logon procedure, see *1.5.1 Logging on to PFM - Web Console*.

PFM - Web Console is connected using the logical IP address of the node that runs PFM - Manager when used on a logical host.

(2) Managing user accounts

The managing of Performance Management user accounts is the same as with a non-cluster system. For details, see *2. Managing User Accounts*.

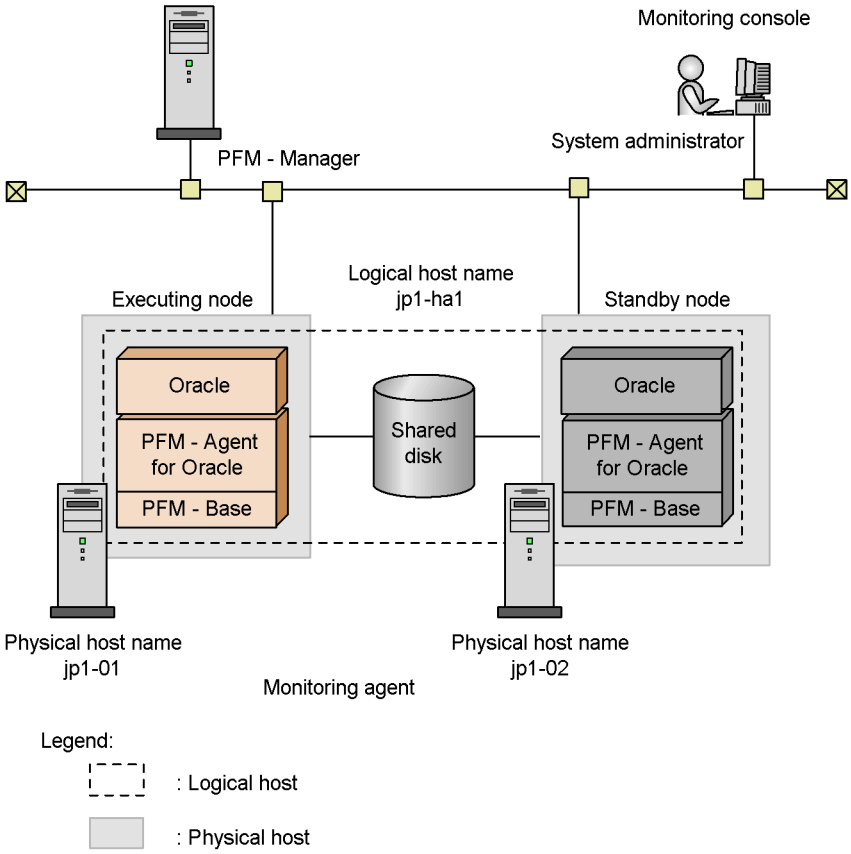
9.6.3 Managing agents in an integrated manner in a cluster system

Only one agent with the logical host name is displayed in the window of PFM - Web Console when PFM - Agent or PFM - RM runs on a logical host in a cluster system. An agent using an executing node or standby node name is not displayed.

The agent that runs on the executing node is operated when you operate the agent displayed as the logical host name.

For example, when Oracle with a cluster configuration that runs in an environment having the same logical host name `jp1-ha1` is monitored by PFM - Agent for Oracle that runs in the environment having the same logical host name `jp1-ha1`, the operations are as shown in the following figure. An agent that runs on the logical host environment is displayed using the logical host name. You are automatically connected to PFM - Agent for Oracle that runs on the executing node when you operate this agent.

Figure 9-30: Example of monitoring Oracle by PFM - Agent for Oracle in a cluster configuration



Point:

The agent with the physical host name is displayed in the window of PFM - Web Console when PFM - Agent or PFM - RM runs on a non-cluster system.

9.6.4 Collecting and managing the operation management data in a cluster system

The collection and management of operation management data is the same as with a non-cluster system. For details, see the chapter describing Performance Management functionality in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

9.6.5 Creating operation management reports in a cluster system

Reports are created in a cluster system in the same manner as with a non-cluster

system. For details, see *5. Creation of Reports for Operation Analysis*.

9.6.6 Performing realtime operation monitoring by alarms in a cluster system

Alarms need to be set in order to notify users when an error occurs in a monitoring target system. Note that the method of setting alarms is different from that for a non-cluster system when a logical host is used in a cluster system.

Notes about the nodes that executes actions:

- If `LOCAL` is set for **Command Execution Action Handler**, actions are executed on the node on which PFM - Agent or PFM - RM that performs alarm monitoring operates. For example, when an alarm occurs with PFM - Agent or PFM - RM used on a logical host, actions are executed on the executing node on which PFM - Agent or PFM - RM runs.
- When Performance Management runs on a logical host, if you specify the logical host name or `LOCAL` for **Command Execution Action Handler**, commands are executed on the node on which Performance Management operates. For that reason, you need to configure the environment in such a way that commands can be executed in the same way on both the executing and standby nodes.
- Also, if the Action Handler service runs on a logical host, the current directory is as described below. The environment directory means the environment directory name specified with the `jpcconf ha setup` command.

  environment-directory`\jp1pc\bin\action`
- When Performance Management is running on a cluster system and a JP1 event is issued as an alarm action, the JP1 event is registered in the event server of JP1/Base on a physical host as standard behavior.

  When Performance Management and JP1/Base are operated on the same logical host, use the `-r` *logical-host-name* option to additionally specify the logical host name as the event server name in the message text (JP1 event attribute to be passed to the `jpcimevt` command) field where the JP1 event is registered.

  You cannot specify the event server name of JP1/Base that runs on a different logical host.

  For details on the alarm setting procedure, see *6.4 Setting alarms by using the browser*.

9.6.7 Performing backup and restore in a cluster system

You need to back up the data periodically in case of problems when Performance

Management runs on a logical host in a cluster system.

The following information needs to be backed up:

- Definition information required to operate Performance Management

  Report definition information

  Alarm table definition information

  Service definition information

- Operation monitoring data collected by Performance Management

  Performance data

  Event data

In addition to the above, the bookmark definition information that is set in PFM - Web Console also needs to be backed up. Note that the information that needs to be backed up is the same as with a non-cluster system.

For details on how to perform backup and restore, see *8. Backing Up and Restoring Data*.

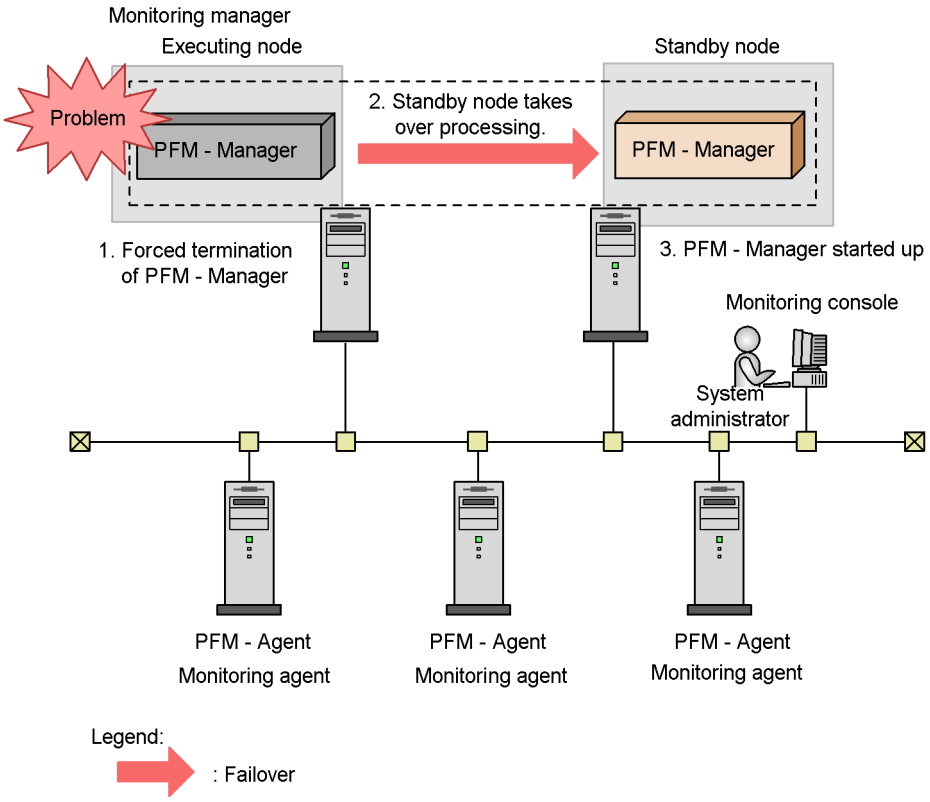
9.6.8 Performing the required operation when a failover occurs in a cluster system

When a failure occurs on the executing node, the cluster software executes a failover and the standby node takes over the processing. This subsection describes the operation when a failover occurs in PFM - Manager and in PFM - Agent or PFM - RM, respectively.

(1) Flow of processing for a failover when a failure occurs in PFM - Manager

The following figure shows the system processing when a failure occurs in PFM - Manager during the operation and a failover occurs.

Figure 9-31: Flow of processing when a failover occurs on the PFM - Manager host



The flow of system processing is as follows:

1. The cluster software forces PFM - Manager to terminate when a failover occurs.
2. The cluster software directs the standby node to take over the PFM - Manager processing from the executing node.
3. The cluster software starts up PFM - Manager on the standby node.

(a) Operation on PFM - Web Console

The KAVJS0012-E message is displayed if you are performing operations from a PFM - Web Console window when a failover occurs in PFM - Manager.

To connect to the failover destination PFM - Manager:

1. Log out from the window of PFM - Web Console.

   Click the **Logout** menu in the Main window.

2. Log on in the window of PFM - Web Console.

   Log on from the window of PFM - Web Console again after the failover destination PFM - Manager starts up.

Note:

If a failover occurs while you are working with the bookmarks, the information that was not correctly written in the bookmarks definition information is lost. Correct the bookmark definition if the bookmarks cannot be operated properly.

(b) Operations using PFM - Agent or PFM - RM

You do not need to perform special operations in PFM - Agent or PFM - RM when a failover occurs in PFM - Manager during operation. The performance data continues to be collected in PFM - Agent or PFM - RM during a failover of PFM - Manager.

(2) Effects when PFM - Manager stops

Stopping PFM - Manager affects the entire Performance Management system.

PFM - Manager performs integrated management of the agent information for each node where PFM - Agent or PFM - RM runs. Also, PFM - Agent or PFM - RM controls alarm event reports sent when a performance value exceeds a threshold value during monitoring and execution of actions triggered by an alarm event. For that reason, stopping PFM - Manager affects the Performance Management system in the areas listed in the following table.

Table 9-14: Effects on PFM - Web Console when PFM - Manager stops

Effect	Solution
• An alarm flashing in red in the window of PFM - Web Console returns to green immediately after PFM - Manager restarts or when a failover occurs, and then starts flashing in red again. When PFM - Manager stops, the KAVJS0012-E message occurs and no further operations can be performed.	Start up PFM - Manager, and then log on again.
• You cannot log on to Performance Management when you attempt to log on from the window of PFM - Web Console if PFM - Manager has stopped.	Start up PFM - Manager, and then log on again.

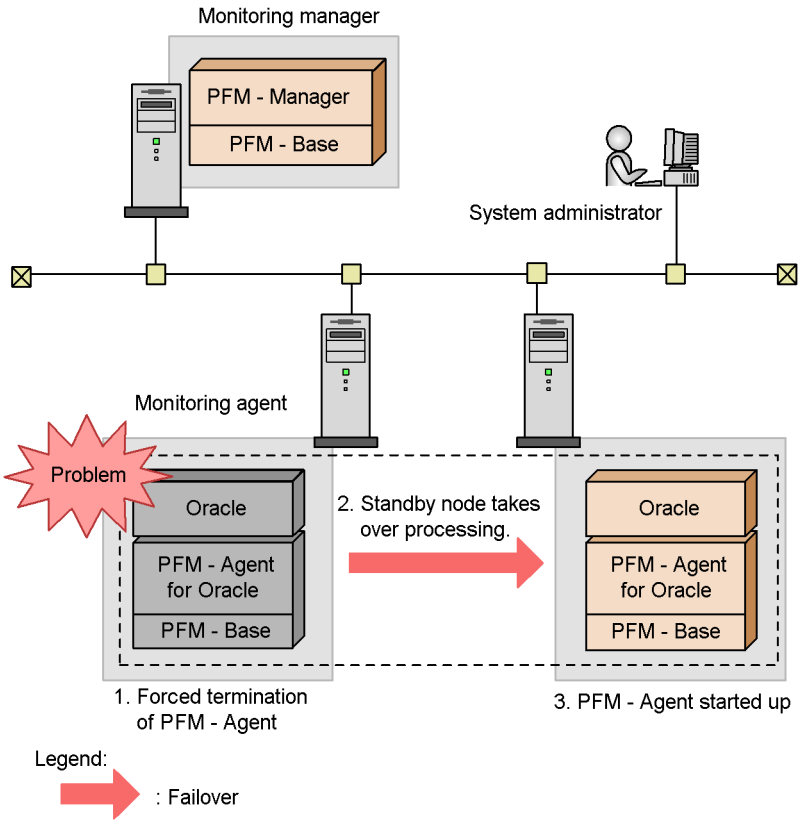
Table 9-15: Effects on PFM - Agent or PFM - RM when PFM - Manager stops

Effect	Solution
• The Performance data continues to be collected. • Since the alarm event that occurred cannot be reported to PFM - Manager, the alarm event is retained for each alarm definition and the report is retried until PFM - Manager starts up. The oldest alarm event is overwritten when more than three alarm events are retained. If PFM - Agent or PFM - RM is stopped, all retained alarm events are deleted. • When PFM - Manager restarts, the alarm status that has already been reported to PFM - Manager is reset at once. Then PFM - Manager checks the status of PFM - Agent or PFM - RM and updates the alarm status. • When you attempt to stop PFM - Agent or PFM - RM, it takes time because the attempt to stop the program is not sent to PFM - Manager.	Start up PFM - Manager. You can continue using the PFM - Agent or PFM - RM that is running without any changes. However, since an alarm might not be reported as expected, check the `KAVE00024-I` message output to the common message log of PFM - Agent or PFM - RM after PFM - Manager recovers.

(3) Flow of processing for a failover when a failure occurs in PFM - Agent or PFM - RM

The following figure shows processing when a failure occurs in PFM - Agent or PFM - RM during operation.

Figure 9-32: Flow of processing when a failover occurs in PFM - Agent or PFM - RM



The flow of system processing is as follows:

1. The cluster software forces PFM - Agent or PFM - RM to terminate when a failover occurs.
2. The cluster software directs the standby node to take over the PFM - Agent or PFM - RM processing from the executing node.
3. The cluster software starts up PFM - Agent or PFM - RM on the standby node.

(a) Operations in the window of PFM - Web Console

A message appears, according to the status, if you operate in the window of PFM - Web Console during a PFM - Agent or PFM - RM failover. In such cases, wait until the failover completes and the operation starts.

If you operate in the window of PFM - Web Console after the PFM - Agent or PFM - RM failover, you will be connected to and operate PFM - Agent or PFM - RM that is

started up on the failover destination node.

9.7 Failure recovery in a cluster system

When a failure occurs on the executing node, the cluster software executes a failover and the standby node takes over the processing. When a failover takes place, processing that was being executed by the executing node stops.

The system administrator identifies the cause of the failure that occurred on the executing node. After removing the cause of the failure, you need to switch the processing to the executing node to recover from the failure.

Collect and analyze the following log information to identify the cause of the failure:

- Performance Management log information

  This information is the same as that collected in a non-cluster system. Collected information includes:

  - System log
  - Common message log
  - Operation status log
  - Trace log

- Cluster software and OS log information

  Hitachi recommends that you collect the cluster software log information as well as logs output by the OS itself.

For details on the Performance Management log information, see *14.3 Log information*.

(1) Collecting the log information in a cluster system

Pay attention to the following items when you collect the Performance Management log information in a cluster system:

- The common message log and trace log are output to the shared disk when Performance Management is used on a logical host.

  Log information before and after the failover is recorded in the same log file since the log file on the shared disk is inherited together with the system when a failover takes place.

- If Performance Management is used on a logical host, it is necessary to refer to the information from around the time when a failure occurs. For this reason, you need to extract the log information on both the executing node that stopped the processing due to the failover and the failover destination standby node.

For details on how to extract the Performance Management log information, see *14.5*

Data collection procedure.

9.8 Notes on cluster systems

Note the following items when you use Performance Management in a cluster system.

(1) Notes on failover occurrence detection

It is difficult for Performance Management to detect failovers on PFM - Manager, PFM - Agent, or PFM - RM nodes. To detect the occurrence of a failover, you need to utilize methods such as using cluster software management tools, SNMP traps issued by the cluster software, or message monitoring of log files. For details on message monitoring of log files, see *13.5 Detecting problems by linking with the integrated system monitoring product*.

(2) Notes on starting and stopping Performance Management

Use the cluster software to start and stop Performance Management that is used on a logical host registered in the cluster software. If you start up or stop Performance Management using a method other than the operating cluster software, such as by using the `jpcspm start` or `jpcspm stop` command, there might be a difference between the actual Performance Management status and the status controlled by the cluster software, causing an error to be assessed.

(3) Notes on setting Status Server services

One host can run only one Status Server service. For that reason, the Status Server service on a physical host manages the status of the physical host and logical host services. You need to set the Status Server service not to perform a failover or run constantly.

(4) Notes on command execution

Only the executing node can execute the following PFM - Web Console commands when Performance Management is used on a logical host:

- `jpcaspsv` command
- `jpcasrec` command
- `jpcmkkey` command
- `jpcrdef` command
- `jpcrpt` command

Both the executing node and standby node can execute the `jpcwras` and `jpcwagtsetup` commands. These two commands act for the physical host that executes the commands.

(5) Notes on networks

Performance Management on a physical host cannot operate if it cannot communicate

using the physical IP address that corresponds to the physical host name (in the Windows system, the host name displayed when the `hostname` command is executed, and in the UNIX system, the host name displayed when the `uname -n` command is executed).

(6) Notes on using JP1 authentication mode

To use JP1 authentication mode in an environment using PFM - Manager on a cluster system, JP1/Base must also be used on the cluster system. The JP1/Base version must be 08-00 or later.

Chapter

10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring

This chapter describes operation monitoring by linking Performance Management with the integrated management product JP1/IM. The chapter covers the setup procedure for linking Performance Management with JP1/IM, and how to perform operation monitoring of the target system by using Performance Management from JP1/IM.

10.1 Overview of linking with the integrated management product JP1/IM for operation monitoring
10.2 Considerations for linking with JP1/IM
10.3 Setting up the linkage with JP1/IM
10.4 Operating the linkage with JP1/IM
10.5 List of JP1 event attributes

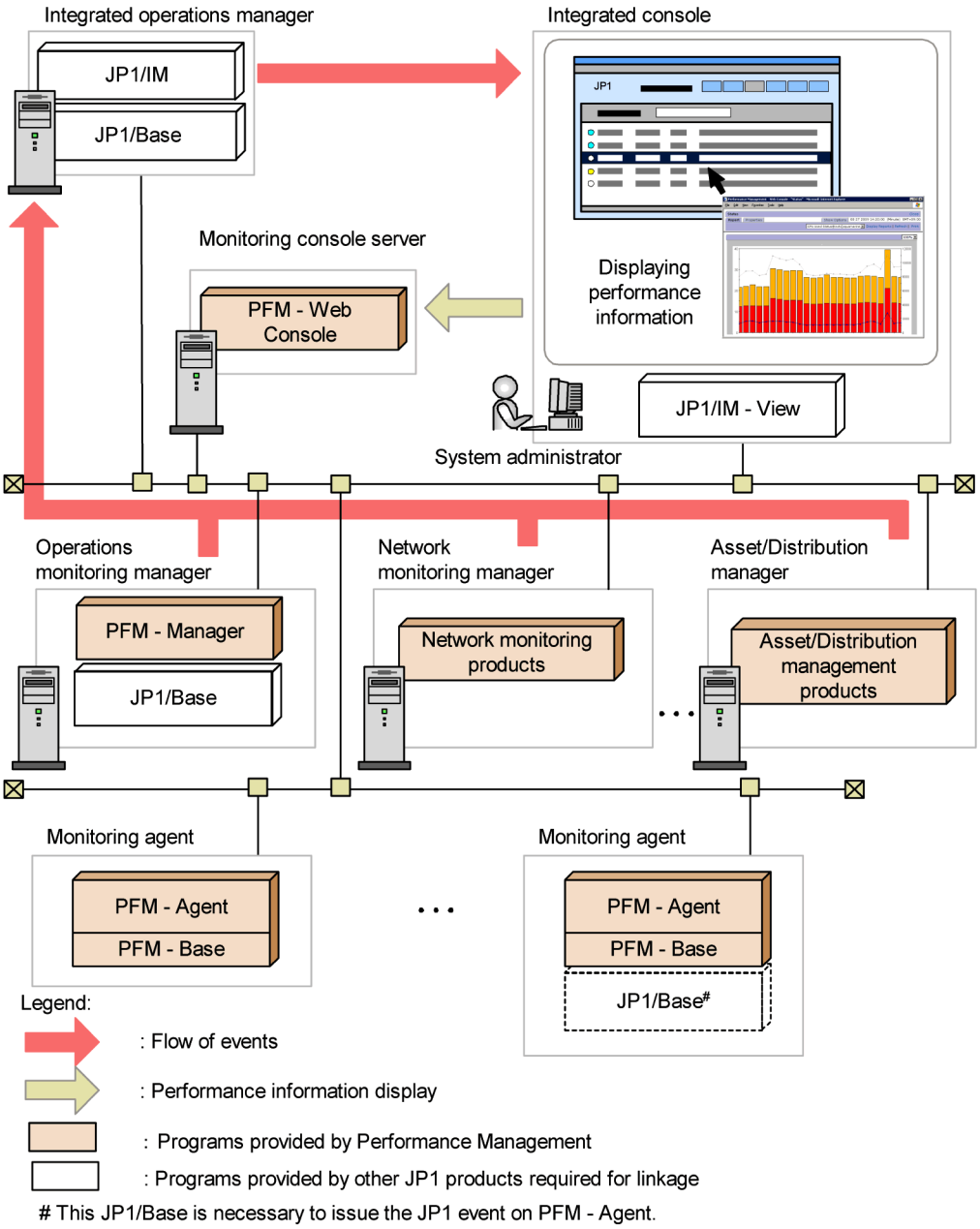
10.1 Overview of linking with the integrated management product JP1/IM for operation monitoring

Performance Management enables you to monitor operations by linking with the integrated management product JP1/IM.

You can set up Performance Management so that a JP1 event is issued when a monitored program exceeds a threshold and an alarm event occurs, when the status of Performance Management services changes, or when the status of an agent changes. Therefore, you can monitor errors that occur in Performance Management by using JP1 events from JP1/IM. Linkage with JP1/IM also enables you to monitor Performance Management and other JP1 programs on the same display and to view operation reports on Performance Management if any problems occur. Moreover, you can log on to Performance Management as a JP1 user.

The following figure shows an example of operation monitoring by using Performance Management linked with JP1/IM.

Figure 10-1: Example of operation monitoring by Performance Management linked with JP1/IM



Reference note: What is *JP1/IM*?

JP1/IM is a product that provides integrated operations management of the JP1 series. It provides the functionality to perform integrated management of entire enterprise information systems. With JP1/IM, monitoring is possible with the *integrated console* function and with the *integrated scope* function that allows the entire system to be visualized from a business standpoint. The integrated scope includes a visual monitoring window that allows the entire enterprise system to be visualized from a business standpoint, thereby allowing for the intuitive monitoring of large-scale, complex systems.

JP1/IM provides two methods for monitoring Performance Management. You can select the method that best matches the item being monitored and your goals. Their respective features are as follows:

- Monitoring by using the integrated console

  A console window is used for monitoring JP1 events occurring in the system subject to monitoring (monitoring agent). This method enables JP1 event filtering, and event searches.

- Monitoring by using the integrated scope

  A visual-display window is used for monitoring JP1 events occurring in the monitoring agent. For example, you can effectively visualize the entire system by grouping events by operation or organization, or by grouping by business units across the country or data center layout.

10.1.1 Monitoring by using integrated console

The Event Console window in JP1/IM's integrated console can list JP1 events issued from Performance Management.

You can use a displayed JP1 event to display a window of PFM - Web Console (browser) from which you can identify the cause of the JP1 event. Moreover, you can use the browser to check the contents of alarm definitions and, if a report is associated with the alarm, you can view the alarm report. You can set the console to display only specified JP1 events by changing the display conditions for the event console. When a JP1 event is issued due to an alarm event occurring in Performance Management or a Performance Management service status change, the JP1 event is sent to JP1/IM via JP1/Base, and then is displayed in the Event Console window.

10.1.2 Monitoring by using integrated scope

This method enables grouping of systems and monitoring from a tree- or map-type window.

You can display icons on the Monitoring tree window that indicate the operating statuses of the monitoring agents and can check the statuses by checking the color of the icons. In JP1/IM, a monitoring target is called a *monitored object*.

Point:

The name of the icon indicating the operating status of the monitored agent is made up of the agent name and the instance name for PFM - Agent or PFM - RM and is displayed in the following format: *agent-name_instance-name* `Monitoring (PFM)`. For example, when the program is monitoring PFM - Agent for Oracle whose instance name is `InstA`, `Oracle_InstA Monitoring (PFM)` is displayed.

When a JP1 event is issued in Performance Management, the color of the icon for PFM - Agent or PFM - RM changes to a color that indicates the error status. This helps to easily identify agents with problems.

Note

To use the JP1/IM integrated scope to automatically generate a Monitoring tree, JP1/Base must be running on the PFM - Agent or PFM -RM host that is to be added to the tree.

For details, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, *Job Management Partner 1/ Integrated Management - Manager Configuration Guide*, and the manual *Job Management Partner 1/Integrated Management - Manager Command and Defined file Reference*.

10.1.3 Linkage of Performance Management and JP1/IM

You can set up Performance Management so that a JP1 event detected by JP1/IM triggers display of a report in a window of PFM - Web Console. You can also set it up to enable a window of PFM - Web Console to be displayed from the integrated management menu in JP1/IM.

The following describes linked functions for Performance Management and JP1/IM:

- Displaying a report from JP1/IM

  From a JP1 event displayed in the Event Console window of the JP1/IM integrated console, you can display a report previously associated with an alarm in the window of PFM - Web Console.

- Starting the window of PFM - Web Console from the Tool Launcher window of JP1/IM

  You can display the window of PFM - Web Console from the Tool Launcher window of JP1/IM to perform performance monitoring.

10.2 Considerations for linking with JP1/IM

This section explains about JP events issued from Performance Management to JP1/IM.

10.2.1 JP1 event types

There are two types of JP1 events: *JP1 system events* and *JP1 user events*. The main differences are as follows:

Table 10-1: Differences between JP1 system events and JP1 user events

Item		JP1 system event	JP1 user event
Event ID		A numerical value from 00004800 to 00004850 is output (fixed number).	Any numerical value can be output.#1
Issued event	Occurrence of alarm events	Yes	Yes
	Status change of agents	Yes	No
	Status change of Performance Management services	Yes	No
	Events for operations#2	Yes	No

Legend:

Yes: Events are issued

No: Events are not issued

#1

Any value can be specified when setting up a JP1 user event.

#2

This is an event generated by PFM - Agent or PFM - RM.

Compared to the JP1 user event type, the JP1 system event type covers a larger range of events. Also, when setting up JP1 system events to be issued, you do not need to edit or copy any definition files required by JP1/IM - Manager. We recommend that you use the JP1 system event type if you are using PFM - Manager 09-00 or later.

The JP1 user event type includes events that are equivalent to conventional Performance Management JP1 events (PFM - Manager versions earlier than 08-11).

You should consider these factors when determining which JP1 event type to use.

10.2.2 Prerequisite conditions for issuing JP1 events

The prerequisite conditions depend on the types of issued JP1 events. The following table describes the prerequisite conditions for issuing JP1 events.

Table 10-2: Prerequisite conditions for issuing JP1 events

Required programs	Version	
	JP1 system event	JP1 user event
PFM - Manager	09-00 or later	08-00 or later
PFM - Base	09-00 or later	08-00 or later
PFM - Agent	08-00 or later#	06-70 or later
PFM - RM	09-00 or later	09-00 or later
PFM - Web Console	08-00 or later	08-00 or later
JP1/IM - Manager	09-00 or later	08-00 or later
JP1/IM - View	09-00 or later	08-00 or later
JP1/Base	09-00 or later	06-00 or later

#

Version 09-00 or later is required to issue events for operations.

For details on the system configuration for issuing JP1 events, see *10.3.1 Installation*.

10.3 Setting up the linkage with JP1/IM

This section describes the installation and setup procedures for setting up an environment for linking with JP1/IM.

10.3.1 Installation

The following prerequisite conditions for linking with JP1/IM must be satisfied:.

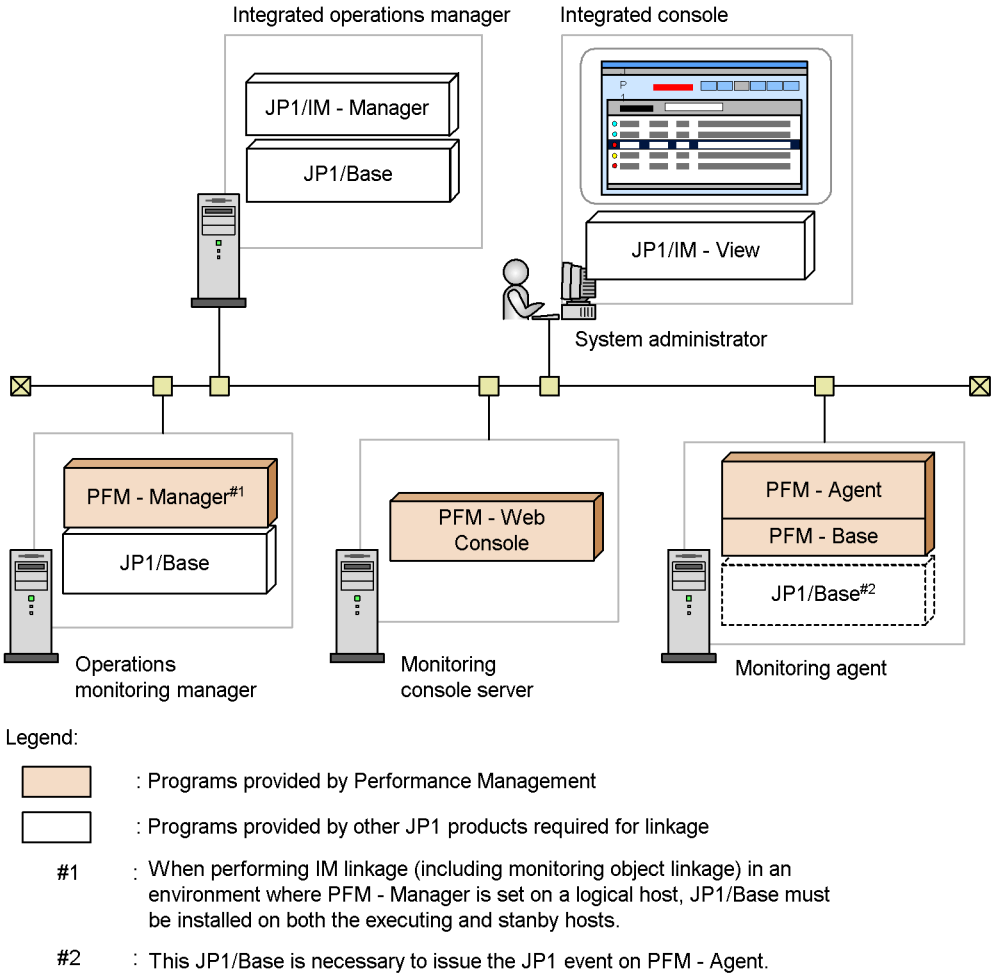
- The PFM - Manager host must have JP1/Base installed in order to log on to Performance Management as a JP1 user. Perform user management with JP1/Base.
- JP1/Base on the PFM - Manager host must be configured as an object to be managed by JP1/IM - Manager.
- To start PFM - Web Console from JP1/IM View, the JP1/IM - View host must have a browser installed.
- Performance Management 08-00 or later and an earlier version of Performance Management cannot be set up at the same time when establishing linkage with JP1/IM.

Note:

If Performance Management earlier than 08-00 is used for setting up the JP1/IM linkage function, you need to perform unsetup of the JP1/IM linkage function of the earlier version (previous to 08-00) and then set up the JP1/IM linkage function using version 08-00 or later again.

The following figure shows the installation configuration:

Figure 10-2: JP1/IM installation configuration for linkage with JP1/IM



10.3.2 Setup

This section describes the setup procedure for linking with JP1/IM.

If the name of the Performance Management monitoring host differs from its actual host name, the monitoring host name must be added to the JP1/IM host information file (`jcs_hosts`). After editing the file, use the following procedure to apply the changes:

1. Import the host information.

   `jcshostsimport -o` (*host-information-file*)

2. Reload JP1/IM.

```
jco_spmd_reload
```

For details on the host information file and JP1/IM commands, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* or the manual *Job Management Partner 1/Integrated Management - Command and Definition File Reference*.

The following table shows the process flow for setup. The required steps depend on the JP1 event type used and the extent of linkage between Performance Management and JP1/IM.

Table 10-3: Process flow for setup

Setup procedure	Refer to:	Necessity for setup	
		JP1 system event	JP1 user event
Configuration for issuing JP1 events In the PFM - Web Console browser, set up the configuration so that JP1 events are issued when a monitored event occurs in JP1/IM.	*10.3.2(1)*	Required	Required
Defining alarm events and reports Define alarm events to be monitored in JP1/IM and operation reports in the PFM - Web Console browser.	*10.3.2(2)*	Required	Required
Setting for linking with JP1/IM integrated console Edit the definition files required in JP1/IM - Manager, and then store them under a directory for JP1/IM.	*10.3.2(3)(a)*	None required#1	Required
Setting for linking with the Tool Launcher window of JP1/IM#2 Edit the definition files required in JP1/IM - View, and then store them under a directory for JP1/IM.	*10.3.2(3)(b)*	Required if linking	Required if linking
Setting for linking with the integrated scope of JP1/IM#3 Execute the command for linkage with the monitored object (`jpcconf im` command).	*10.3.2(4)*	Required if linking	Required if linking
Specifying whether the messages of JP1 user events are enclosed in quotes In UNIX, specify whether JP1 user event messages are enclosed in quotes.	*10.3.2(5)*	Unavailable	Optional (Set if not using quotation mark)

#1

For a JP1 system event, you do not need to edit or copy the definition file, even when linking with JP1/IM integrated console.

#2

Before Performance Management can be configured to link with the JP1/IM Tool Launcher, you must complete the configuration for linking with the JP1/IM integrated console.

#3

Before Performance Management can be configured to link with the JP1/IM integrated scope, you must complete the configuration for linking with the JP1/IM integrated console.

Note:

Linkage with the system-monitored object for Performance Management in JP1/IM is required in order to enable monitoring with the integrated scope. For details on settings and operations of JP1/IM, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* and *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

This subsection describes the setup procedures for linking with JP1/IM.

(1) Configuring so that JP1 events are issued

To configure so that JP1 events are issued:

1. From the monitoring console browser, log on to PFM - Web Console.

   Log on to a user account that has administrator user permissions.

   The main window of PFM - Web Console appears. You must have administrator user permissions to use the Services window.

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

   The Services window appears.

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

   The selected service is marked with a checkmark.

   The following table lists the events that trigger JP1 system events and the properties to be set for each target service.

Table 10-4: Events that trigger JP1 system events and properties to be set for each target service

Event	Target service	Properties to be set
Occurrence of alarm events	Action Handler service • Action Handler	Master Manager, Agent Collector, Remote Monitor Collector, or Action Handler[#1]
Occurrence of events related to the status change and operation of Performance Management services	PFM - Manager service • Name Server • Master Manager • Master Store • Correlator • Trap Generator • View Server	Master Manager
	PFM - Agent and PFM - RM services • Agent Collector and Remote Monitor Collector • Agent Store or Remote Monitor Store These services are used instance by instance (for multi-instance agents).	Agent Collector and Remote Monitor Collector
	Action Handler service • Action Handler	Master Manager, Agent Collector, Remote Monitor Collector, or Action Handler[#1]
	Status Server service[#2] • Status Server	Master Manager, Agent Collector, Remote Monitor Collector, or Action Handler[#1]

#1

Use the same value for the listed services on the same host.

#2

The Status Server service does not appear as a service on a logical host.

4. Select the **JP1 Event Configurations** node.

   At the bottom of the information frame, the properties of the **JP1 Event Configurations** node are displayed.

5. For JP1 system events, set the properties as follows.

   This step is not required for JP1 user events. Go to step 6.

   Target service: `Yes`

   JP1 Event Send Host

   Specify the name of an event server connected to JP1/Base using 255 or less

alphanumeric characters. You can only specify an event server running on the same logical or physical host as the Performance Management service that issues the JP1 events. You cannot specify an IP address. Any preceding or trailing spaces in the specified value are ignored.

localhost indicates a physical host. If an out-of-range value is specified or if no value is specified, the event-issuing host is assumed to be a host (a physical host in a physical host environment or a logical host in an logical host environment) running Performance Management services that issue JP1 events.

The default value is blank.

Reference note:

Normally, you do not need to set this parameter. However, we recommend that you set this parameter in the following case:

- Performance Management services are running on host 1 (physical host), but you want to use JP1/Base running on host 2 (logical host) to issue JP1 events.

In this case, we recommend that you set **JP1 Event Send Host** to host 2 (the logical host).

The name of the event server in this parameter is different from the name set for the using the function for setting monitoring-host names. If you have already set a monitoring host name, you do not need to set this parameter.

Monitoring Console Host

To start the PFM - Web Console browser, specify the name of the PFM - Web Console host in the JP1/IM - Manager monitor startup function. Specify the name with 255 or less alphanumeric characters. You cannot specify an IP address. Any preceding or trailing spaces in the specified value are ignored.

If an out-of-range value is specified or if no value is specified, the name of the PFM - Manager for the connection destination of PFM - Web Console is assumed.

The default value is blank.

Monitoring Console Port

Specify the port number (http request port number) for the PFM - Web Console to be started. If no value is specified, the value `20358` is assumed.

The default value is blank.

6. Select the **Alarm** node under the **JP1 Event Configurations** node.

At the bottom of the information frame, the properties of the **Alarm** node are displayed.

7. Set the properties to the following:

   Specify a JP1 event type to be associated if an alarm event occurs.

   JP1 Event Mode

   To use a JP1 system event: `JP1 System Event`

   To use a JP1 user event: `JP1 User Event`

(2) Defining alarm events and reports

In the Alarms window of PFM - Web Console, set up the following items:

- Set up the issuing of a JP1 event as an action.

  This item sets up the issuing of a JP1 event as the action to be performed when an alarm is issued.

- Associate alarms with reports.

  This item enables reports to be displayed in the window of PFM - Web Console from the JP1/IM event console.

For details on the definition of alarms, see *6. Monitoring Operations with Alarms*.

The following procedure mainly describes operations for setting up JP1 events to be issued and for associating alarms with reports.

To set up JP1 events to be issued and associate alarms with reports:

1. Log on to PFM - Web Console as a user with administrator user permissions.
2. In the navigation frame of the Main window, select the **Alarms** tab.
3. In the navigation frame of the Alarms window, select the alarm definition for which you want to issue JP1 events.

   The selected alarm is marked with a checkmark.
4. Choose the **Edit** method in the method frame.

   The Edit > Main Information window appears in the information frame.
5. Click the **Next** button several times until the Edit > Action window appears.
6. Set **Actions to be executed**.

   In **Command**, select conditions (**Abnormal**, **Warning**, or **Normal**) of the alarm for which you want to issue JP1 events.
7. In **Report to be displayed**, click the **Browse** button to select the report to be associated with the alarm.

The selected alarm is marked with a checkmark.

8. Click the **Finish** button.
9. Click the **Next** button.

   The **Command Definition** area of the Edit > Action Definitions window appears.
10. Click the **JP1 Event Settings** button.

    The New Alarm > Action Definitions > JP1 Event Settings window appears.
11. Set the event ID and so on.

    For example, suppose you want to send the JP1 event under the following conditions:

    Conditions:

    - Set the event ID to `001`.
    - Set the message text to the content of the message text (`%MTS`), which you set in the **Message** of the New Alarm Table > Main Information dialog box.
    - Convert the alarm status to a severity-level JP1 event.

    Set as follows:

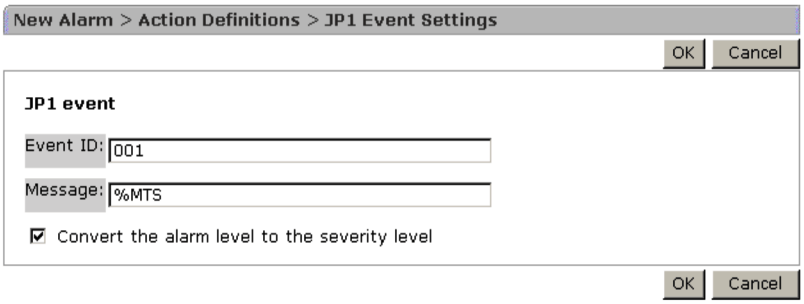
    Event ID: `001`

    Message: `%MTS`

    Convert the alarm level to the severity level: `Selected`

    The following figure shows a setting example of the New Alarm > Action Definitions > JP1 Event Settings window.

    Figure 10-3: New Alarm > Action Definitions > JP1 Event Settings window



Note:

Do not modify the attributes of the JP1 event if you want to link with the JP1/IM monitoring objects.

For a JP1 system event, the information set for **Event ID** is output as an event ID (JPC_USER_EVENTID) identifying an extended JP1 event attribute. For a JP1 user event, the information is output as an event ID for a basic JP1 event attribute.

For details on JP1 event types, see *10.2 Considerations for linking with JP1/IM*.

12. Click the **OK** button.

    The issuing of the JP1 event is defined as an alarm action, and the selected report is associated. For details on the issued JP1 events, see *10.5 List of JP1 event attributes*.

13. Select the Action Handler service of the host that issues the JP1 event.

    When you modify the **JP1 Event Settings**, the setting in **Action handler** is changed to the Action Handler service on the PFM - Manager host. If you want to issue the JP1 event on a host other than the PFM - Manager host, you must modify the setting in **Action handler**.

    Note 1

    To issue a JP1 event, JP1/Base must be installed on the same host as the Action Handler that issues the event.

    Note 2

    To issue a JP1 event during Performance Management monitoring using the JP1/IM integrated scope, you must select an Action Handler service running on the same host as PFM - Manager.

14. Click the **Finish** button.

(3) Editing and copying the definition files for linkage

In order to enable monitoring of JP1 events by using JP1/IM, you need to edit the JP1/IM definition files that are provided by Performance Management according to the environment and to copy the files to each of the corresponding JP1/IM directories.

Point:

- You might need to restart JP1/IM to enable the editing of definition files in JP1/IM. For details on restart timings of the definition files and timing when the definition files take effect, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, and the manual *Job Management Partner 1/Integrated Management - Manager Command and Defined file Reference*.

The JP1/IM definition file provided by Performance Management is stored in the following folder:

PFM-Web-Console-installation-folder\sample\imconf

The following lists JP1/IM definition files, items to edit, and copy destinations.

(a) Definition files required in JP1/IM - Manager

When you use monitoring with the integrated console to issue a JP1 user event, you must edit and copy the definition file required by JP1/IM - Manager. This is not necessary when you use monitoring with the integrated console to issue a JP1 system event.

- Definition file for the extended event attributes

This file defines the extended event attributes of JP1 events.

File name:

hitachi_jp1_pfmWebCon_attr_en.conf

Items to edit:

Change the order id value to the event ID set by the JP1 event-issuing command. To display reports from JP1/IM, you also need to set the specified event ID in the definition file for opening monitor windows.

For example, specify the following when the event ID is 00001234:

```
@define-block    type="event-attr-order-def";
block    platform="BASE",extended="false";
order id="00001234"
,attrs="_COMMON|E.JPC_AGENT|E.JPC_MGR|E.JPC_TIME|E.JPC_REPORTID";
@define-block-end;
```

Copy destination

Copy the edited definition file for the extended event attributes to the directory on the host that has JP1/IM - Manager installed as listed below:

For physical hosts:

- In Windows:

  installation-folder-for-jp1/im-manager\conf\console\attribute

- In UNIX:

  /etc/opt/jp1cons/conf/console/attribute

For logical hosts:

- In Windows:

  shared-folder\jp1cons\conf\console\attribute

- In UNIX:

  shared-directory/jp1cons/conf/console/attribute

For details, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, and the manual *Job Management Partner 1/Integrated Management - Manager Command and Defined file Reference*.

- Definition file for opening monitor windows

  This file defines settings for opening monitor windows. The definition file for opening monitor windows is used to open a monitor window, such as one for the event-issuing source, from the event console window of JP1/IM - View. You need to set up the file to display a PFM - Web Console report window from a JP1 event.

File name:

hitachi_jp1_pfmWebCon_mon_en.conf

Items to edit:

Change the value of the EVENT_ID to the event ID set with the JP1 event-issuing command. Also, change the PATH host name and port number to those of PFM - Web Console. Note that the specified event ID needs to be set in the definition file for the extended event attributes.

For example, if 00001234, PFM-WebCon, and 20358 are assigned to the event ID, host name, and port number respectively are specified as follows:

```
DEF_KEY PRODUCT_NAME=/PFM/ALARM_EVENT EVENT_ID=00001234 INTERFACE=PC_MONITOR

DEF_MTR_CALL NAME=PC_MONITOR EXEC_ID=default_browserPATH="http://PFM-WebCon:20358/
PFMWebConsole/  login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER$UR
LENC%&manager=%IM_EVC_PARAMETER_1$URLENC%&reportId=%IM_EVC_PARAMETER_2$URLENC%&nod
e=%IM_EVC_PARAMETER_3$URLENC%" PARAM=E.JPC_MGR,E.JPC_REPORTID,E.OBJECT_ID
```

Copy destination

Copy the edited definition file for opening monitor windows to the directory on the host that has JP1/IM - Manager installed as listed below:

For physical hosts:

- In Windows:

  installation-folder-for-jp1/im-manager\conf\console\monitor

- In UNIX:

  /etc/opt/jp1cons/conf/console/monitor

For logical hosts:

- In Windows:

  shared-folder\jp1cons\conf\console\monitor

- In UNIX:

  shared-directory/jp1cons/conf/console/monitor

For details, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, and the manual *Job Management Partner 1/Integrated Management - Manager Command and Defined file Reference*.

- Example: PFM - Web Console report windows are displayed for multiple PFM - Managers

  Note

  A PFM - Web Console instance is required for each PFM - Manager instance. For example, if there are two PFM - Manager instances, there must be two PFM - Web Console instances.

You need to use different event IDs to enable multiple PFM - Managers to be displayed by PFM - Web Console report windows.

For example, if 00000000 and 00001111 are assigned to the event IDs, specify the definition file for the extended event attributes and the definition file for opening monitor windows as follows:

Definition file for the extended event attributes:

```
@file type="extended-attributes-definition",                    version="0300";
@product name="/PFM/ALARM_EVENT";
@define-block     type="event-attr-def";
block     platform="BASE",          extended="false", lang="English";
attr      name="E.JPC_AGENT",   title="Agent host name";
attr      name="E.JPC_MGR",             title="Manager host name";
attr      name="E.JPC_TIME",            title="Alarm time";
attr      name="E.JPC_REPORTID",                title="Report ID";
@define-block-end;
@define-block     type="event-attr-group-def";
block     platform="BASE",          extended="false";
group name="_COMMON",           attrs="";
group name="_COMMON_START", attrs="";
group name="_COMMON_END",     attrs="";
@define-block-end;
@define-block     type="event-attr-order-def";
block     platform="BASE",          extended="false";
order id="00000000",  attrs="_COMMON|E.JPC_AGENT|E.JPC_MGR|E.JPC_TIME|E.JPC_REPORTID";
order id="00001111",  attrs="_COMMON|E.JPC_AGENT|E.JPC_MGR|E.JPC_TIME|E.JPC_REPORTID";
@define-block-end;
```

Definition file for opening monitor windows:

```
DESC_VERSION=0300

#PFM - View definition file for monitor window transitions

DEF_KEY PRODUCT_NAME=/PFM/ALARM_EVENT EVENT_ID=0000000 INTERFACE=PC_MONITOR1
DEF_KEY PRODUCT_NAME=/PFM/ALARM_EVENT EVENT_ID=0001111 INTERFACE=PC_MONITOR2

DEF_MTR_CALL NAME=PC_MONITOR1 EXEC_ID=default_browser PATH="http://PFM-Webcon1:8080/
PFMWebConsole/
login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER$URLE
NC%&manager=%IM_EVC_PARAMETER_1$URLENC%&reportid=%IM_EVC_PARAMETER_2$URLENC
%&node=%I
M_EVC_PARAMETER_3$URLENC%" PARAM=E.JPC_MGR,E.JPC_REPORTID,E.OBJECT_ID

DEF_MTR_CALL NAME=PC_MONITOR2 EXEC_ID=default_browser PATH="http://PFM-Webcon2:20358
/PFMWebConsole/
login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER$URL
ENC%&manager=%IM_EVC_PARAMETER_1$URLENC%&reportId=%IM_EVC_PARAMETER_2$URLEN
C%&node=
%IM_EVC_PARAMETER_3$URLENC%" PARAM=E.JPC_MGR,E.JPC_REPORTID,E.OBJECT_ID
```

In the example above, the event ID `00000000` corresponds to PFM - Web Console host name `PFM-Webcon1` and port number `8080`. Similarly, the event ID `00001111` corresponds to PFM - Web Console host name `PFM-Webcon2` and port number `20358`.

(b) Definition files required in JP1/IM - View

- Definition file for the tool launcher

This file defines the Tool Launcher window. The definition file for the tool launcher defines the tree structure and display items to be displayed in the Tool Launcher window in JP1/IM - View. You need to set the definition file for the tool launcher to enable the window of PFM - Web Console to be displayed from the Tool Launcher window.

File name

`hitachi_jp1_pfmWebCon_tree.conf`

Items to edit

Change the host name and port number of arguments to the host name and port number of PFM - Web Console.

If `PFM-WebCon` and `20358` are assigned to the host name and port number of PFM - Web Console respectively, specify as follows:

```
name="Server Availability Management (Administrator)";
execute_id="default_browser";arguments="http://PFM-WebCon:20358/WebConsole/
login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1USER$URLENC %"
;@define-block-end;
```

Copy destination

Copy the edited definition file for the tool launcher to the folder on the host that has JP1/IM - View installed, as follows:

installation-folder-for-jp1/im-view`\conf\function\ja`

- Example: Windows of PFM - Web Console are started respectively by differing hosts

You need to define blocks within the definition file for the tool launcher corresponding to respective PFM - Web Console to enable differing hosts to start windows of PFM - Web Console respectively. For details, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, and the manual *Job Management Partner 1/Integrated Management - Manager Command and Defined file Reference*.

The following provides an example of setting the definition file for the tool

launcher and an example of the Tool Launcher window display.

Example settings: Definition file for the tool launcher

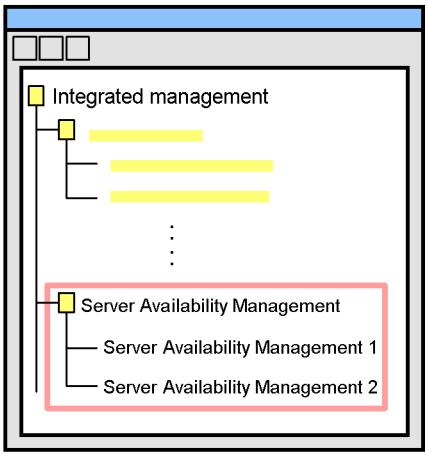
```
@file type="function-definition", version="0300";
#-------------------------------------------------------------------------------
@define-block type="function-tree-def";
id="jco_JP1_PC_manager1";
parent_id="jco_folder_ServerAvailability";
name="Server Availability Management 1";
execute_id="default_browser";
arguments="http://PFM-WebCon1:20358/PFMWebConsole/
login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1U
SER$URLENC%";
@define-block-end;
#-------------------------------------------------------------------------------
@define-block type="function-tree-def";
id="jco_JP1_PC_manager2";
parent_id="jco_folder_ServerAvailability";
name="Server Availability Management 2";
execute_id="default_browser";
arguments="http://PFM-WebCon2:32222/PFMWebConsole/
login.do?jp1token=%JCO_JP1TOKEN$ENC$URLENC%&userName=%JCO_JP1U
SER$URLENC%";
@define-block-end;
#-------------------------------------------------------------------------------
@define-block type="function-tree-def";
id="jco_folder_ServerAvailability";
parent_id="root";
name="Server Availability Management";
@define-block-end;
#-------------------------------------------------------------------------------
```

Setting of Server 1

Setting of Server 2

Setting of the server availablity management folder

Example of the Tool Launcher window



In the examples above, double-clicking **Server Availability Management 1** in

the Tool Launcher window connects the program to PFM - Web Console with the host name of *PFM - WebCon1* and port number *20358*, and then starts the corresponding window of PFM - Web Console. Similarly, double-clicking **Server Availability Management 2** in the Tool Launcher window connects the program to PFM - Web Console with the host name of *PFM - WebCon2* and port number *32222*, and then starts the corresponding window of PFM - Web Console.

(4) Executing the command for linkage with the monitored object

Execute the `jpcconf im` command on the PFM - Manager host to monitor the operating status of the system on Performance Management by using icons through linkage with the monitored object function of JP1/IM. This step is required for JP1/IM to collect definition information from Performance Management.

Execute the `jpcconf im` command on the PFM - Manager host as shown below to start linkage with JP1/IM:

```
jpcconf im enable
```

Execute the command as shown below to stop linkage with JP1/IM:

```
jpcconf im disable
```

If PFM - Manager is in a logical host environment, execute the command one time on both the active and standby nodes.

(5) Setting quotation marks enclosing a JP1 user event message

For UNIX, a JP1 user event message can be enclosed in double quotation marks (`"`). To enclose such a message in double quotation marks, directly edit the `jpccomm.ini` file, which is located on the host running the Action Handler server that executes the action. To specify whether the messages of JP1 user events are enclosed in quotes:

1. Stop the Action Handler service to be configured.

   For the logical host environment, stop the Action Handler services of the logical host.

2. Edit the `jpccomm.ini` file.

   The `jpccomm.ini` file is stored in the following locations:

   On physical hosts:

   `/opt/jp1pc/`

   On logical hosts:

   environment-directory`/jp1pc/`

   The following table describes the section name, label name, and range of setting

values that you can edit in the `jpccomm.ini` file.

Table 10-5: Setting item for specifying whether the messages of JP1 user events are enclosed in quotes

Section	Label name	Value range	Default value	Description
[Common Section]	JP1 Event Double Quote	0 | 1	1	Specify whether the messages of JP1 user events are enclosed in quotes. `0`: Do not enclose in quotes `1`: Enclose in quotes

This label is available only for UNIX. In Windows, the setting of the label is ignored.

3. Start the Action Handler service that has been configured.

10.3.3 Unsetup

Delete the definition files for linkage with JP1/IM to disable the linkage function.

Delete all definition files you have copied to the JP1/IM directory. For details on the trigger applied to JP1/IM for deletion of a definition file, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, and the manual *Job Management Partner 1/Integrated Management - Manager Command and Defined file Reference*.

10.4 Operating the linkage with JP1/IM

This section describes the procedure for monitoring Performance Management from JP1/IM. For details on settings and operations of JP1/IM, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* and *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

10.4.1 Procedure for alarm event monitoring via the JP1/IM integrated console

The Event Console window of JP1/IM's integrated console displays information based on JP1 events sent from JP1 series programs. The information displayed in the Event Console window includes the severity of JP1 events, event reception time, and messages. This window is for monitoring alarm events.

10.4.2 Procedure for monitoring via the integrated scope of JP1/IM

Once you have set up the function to monitor the status of Performance Management in the Monitoring tree window of the JP1/IM integrated scope, an icon representing status appears in the window. The color of the icon changes when an alarm event occurs. You can check a detailed description of events in the Event Console window.

10.4.3 Displaying a report from the integrated console of JP1/IM

You can display reports associated with JP1 events issued from Performance Management in the Event Console window in the JP1/IM integrated console.

To display a report, select a JP1 event for which you want to display a report in the Event Console window, and then click **Monitor**.

A report associated with the specified JP1 event is displayed in the window of PFM - Web Console.

10.4.4 Procedure for starting PFM - Web Console from the JP1/IM integrated management menu

To start the window of PFM - Web Console from the integrated management menu of JP1/IM, follow the procedure below:

1. From **Options**, choose **Tool Launcher** on the Event Console window in the integrated console of JP1/IM.

   The Tool Launcher window appears. It displays a tree of the programs managed by JP1/IM.

2. In the tree area, select the **Server Availability Management** folder.

   The menu within the folder is expanded.

3. From the menu, click the **Server Availability Management** menu command.

   The window that appears might vary depending on the Performance Management authentication mode.

   In PFM authentication mode:

   The Login window of PFM - Web Console appears.

   In JP1 authentication mode:

   The window of PFM - Web Console is started in order to perform user authentication automatically for previously logged-on JP1/IM users.

10.5 List of JP1 event attributes

This section describes the attributes and contents of JP1 events issued from Performance Management.

(1) When alarm events occurs

You can set up a configuration so that either JP1 system events or JP user events are issued when an alarm event occurs.

The following table lists the JP1 system events to be issued when an alarm event occurs.

Table 10-6: JP1 event attributes and contents

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	(Not applicable)	`00004840`
		Message	(Not applicable)	The value that has been specified in **Message** in the procedure for issuing JP1 events.
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Information Alarm status: `OK` (The alarm status is Normal (green).) • Warning Alarm status: `WARNING` (The alarm status is Warning (yellow).) • Error Alarm status: `EXCEPTION` (The alarm status is Abnormal (red).)
		User name	USER_NAME	• In Windows: `SYSTEM` • In UNIX: `root` (user name whose user ID is `0`)
		Product name	PRODUCT_NAME	`/HITACHI/JP1/PFM/ALARM_EVENT`
		Object type	OBJECT_TYPE	`ALARM`
		Object name	OBJECT_NAME	Alarm name

Attribute type		Item	Attribute name	Contents
		Registration type	ROOT_OBJECT_TYPE	ALARM_TABLE
		Registration name	ROOT_OBJECT_NAME	Alarm table name
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	NOTICE
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	• In PFM - Agent Host name of PFM - Agent where an alarm was issued • In PFM-RM (remote agent) Monitored host name of a remote agent where an alarm was issued • In PFM-RM (group agent) Primary host name of a group agent where an alarm was issued (*PFM-RM-host-name*)
		Date and time of alarm occurrence	JPC_TIME	Date and time when the alarm occurred
		Displayed report ID	JPC_REPORTID	Report definition ID to be displayed when a JP1 event is selected
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination
		Event ID	JPC_USER_EVENTID	The value that has been specified in **Event ID** in the procedure for issuing JP1 events when an alarm event occurs.

The following table lists the JP1 user events to be issued when an alarm event occurs.

Table 10-7: JP1 user events to be triggered by the occurrence of an alarm event

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	Event ID
		Message	(Not applicable)	The value that has been specified in **Message** in the procedure for issuing JP1 events.
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Information Alarm status: `OK` (The alarm status is Normal (green).) • Warning Alarm status: `WARNING` (The alarm status is Warning (yellow).) • Error Alarm status: `EXCEPTION` (The alarm status is Abnormal (red).)
		Product name	PRODUCT_NAME	`/PFM/ALARM_EVENT`
		Object type	OBJECT_TYPE	`ALARM`
		Object name	OBJECT_NAME	Alarm name
		Registration type	ROOT_OBJECT_TYPE	`ALARM_TABLE`
		Registration name	ROOT_OBJECT_NAME	Alarm table name
		Object ID	OBJECT_ID	Agent name
		Event type	OCCURENCE	`NOTICE`
	Specific information	Agent host name	JPC_AGENT	• In PFM - Agent Host name of PFM - Agent where an alarm was issued • In PFM-RM (remote agent) Monitored host name of a remote agent where an alarm was issued • In PFM-RM (group agent) Primary host name of a group agent where an alarm was issued (*PFM-RM-host-name*)
		Manager host name	JPC_MGR	PFM - Manager host name

Attribute type		Item	Attribute name	Content
		Date and time of alarm occurrence	JPC_TIME	Date and time when the alarm occurred
		Displayed report ID	JPC_REPORTID	Report definition ID to be displayed when a JP1 event is selected

(2) When Performance Management services start

When a Performance Management service starts, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 10-8: JP1 system events to be issued when Performance Management services start

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	`00004800`
		Message	(Not applicable)	KAVE00335-I message
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Information
		User name	USER_NAME	• In Windows: `SYSTEM` • In UNIX: `root` (user name whose user ID is `0`)
		Product name	PRODUCT_NAME	`/HITACHI/JP1/PFM`
		Object type	OBJECT_TYPE	`SERVICE`
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	`START`
		Starting time	START_TIME	The time when the service started (time when an event is issued)

Attribute type		Item	Attribute name	Content
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	The name of the PFM - Agent host or PFM - RM host which issued the event (this information is only displayed if the service that issued the event was either PFM - Agent or PFM - RM)
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

(3) When Performance Management services stop

When a Performance Management service stops, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 10-9: JP1 system events to be issued when Performance Management services stop

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	`00004810`
		Message	(Not applicable)	KAVE00336-I message (normal termination) KAVE00339-I message (abnormal termination)
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Information (normal termination) • Error (abnormal termination)
		User name	USER_NAME	• In Windows: `SYSTEM` • In UNIX: `root` (user name whose user ID is `0`)
		Product name	PRODUCT_NAME	`/HITACHI/JP1/PFM`

Attribute type		Item	Attribute name	Content
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	END
		Starting time	END_TIME	The time when the service stopped (time when an event is issued)
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	The name of the PFM - Agent host or PFM - RM host which issued the event (this information is only displayed if the service that issued the event was either PFM - Agent or PFM - RM)
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

(4) When the startup of Performance Management services fails

When a startup of Performance Management services fails, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 10-10: JP1 system events to be issued when the startup of Performance Management services fails

Attribute type	Item	Attribute name	Content
Basic attribute	Event ID	(Not applicable)	00004820
	Message	(Not applicable)	KAVE00337-E message

Attribute type		Item	Attribute name	Content
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Error
		User name	USER_NAME	• In Windows: `SYSTEM` • In UNIX: `root` (user name whose user ID is `0`)
		Product name	PRODUCT_NAME	`/HITACHI/JP1/PFM`
		Object type	OBJECT_TYPE	`SERVICE`
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	`NOTSTART`
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	The name of the PFM - Agent host or PFM - RM host which issued the event (this information is only displayed if the service that issued the event was either PFM - Agent or PFM - RM)
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

(5) When events for operation occur

When an event for operation occurs, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 10-11: JP1 system events to be issued when an event for operation occurs

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	`00004830`
		Message	(Not applicable)	Service-specific message#
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Information • Warning • Error
		User name	USER_NAME	• In Windows: `SYSTEM` • In UNIX: `root` (user name whose user ID is `0`)
		Product name	PRODUCT_NAME	`/HITACHI/JP1/PFM`
		Object type	OBJECT_TYPE	`SERVICE`
		Object name	OBJECT_NAME	Service ID
		Object ID	OBJECT_ID	Service ID
		Event type	OCCURENCE	`NOTICE`
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	The name of the PFM - Agent host or PFM - RM host which issued the event (this information is only displayed if the service that issued the event was either PFM - Agent or PFM - RM)
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

#

An applicable message from among the following is output:

- A PFM - Manager message listed in the manual *Job Management Partner 1/*

Performance Management Reference (for which a JP1 system event is specified as the destination in the destination list)

- A message listed in the appropriate PFM - Agent or PFM - RM manual (for which a JP1 system event is specified as the destination in the destination list)

(6) When agent statues are changed

If the status of an agent changes, a JP1 system event is issued. The following table lists the JP1 system events to be issued.

Table 10-12: JP1 system events issued when the status of an agent changes

Attribute type		Item	Attribute name	Content
Basic attribute		Event ID	(Not applicable)	00004850
		Message	(Not applicable)	One of the following is output: • Agent event [Status Change] • KAVE00217-I message (when the status of an agent monitored for alarms changes to Normal) • KAVE00218-W message (when the status of an agent monitored for alarms changes to Warning) • KAVE00219-E message (when the status of an agent monitored for alarms changes to Abnormal) • KAVE00333-E message (when the operating status of an agent changes to Busy or Abnormal End) • KAVE00334-I message (when the operating status of an agent recovers from Busy or Abnormal End)
Extended attribute	Common information	Severity	SEVERITY	Severity is set. • Information (when the status of an agent monitored for alarms changes to Normal) • Warning (when the status of an agent monitored for alarms changes to Warning) • Error (when the status of an agent monitored for alarms changes to Error or when the operating status of an agent recovers from Busy or Abnormal End)

Attribute type		Item	Attribute name	Content
		User name	USER_NAME	• In Windows: `SYSTEM` • In UNIX: `root` (user name whose user ID is `0`)
		Product name	PRODUCT_NAME	`/HITACHI/JP1/PFM/STATE_EVENT`
		Object type	OBJECT_TYPE	`SERVICE`
		Object name	OBJECT_NAME	Service ID of the agent
		Object ID	OBJECT_ID	Service ID of the agent
		Event type	OCCURENCE	`NOTICE`
	Specific information	Manager host name	JPC_MGR	Host name of PFM - Manager for the connection destination
		Agent host name	JPC_AGENT	• In PFM - Agent Host name of PFM - Agent where a status is changed • In PFM-RM (remote agent) Monitored host name of a remote agent where a status is changed • In PFM-RM (group agent) Primary host name of a group agent where a status is changed (PFM RM host name)
		Monitor host name	JPC_MON_HOST	Host name of the PFM - Web Console for the connection destination
		Monitor port number	JPC_MON_PORT	Http request port number of the PFM - Web Console for the connection destination

Chapter

11. Linking with Network Node Manager (NNM) for Operation Monitoring

This chapter describes the system overview and environment setting procedures to link Performance Management with NNM, and the procedures to monitor Performance Management by using NNM.

11.1 Overview of linking with Network Node Manager (NNM) for operation monitoring
11.2 Constructing the linkage with NNM
11.3 Operations for linkage with NNM
11.4 Configuration of MIB objects

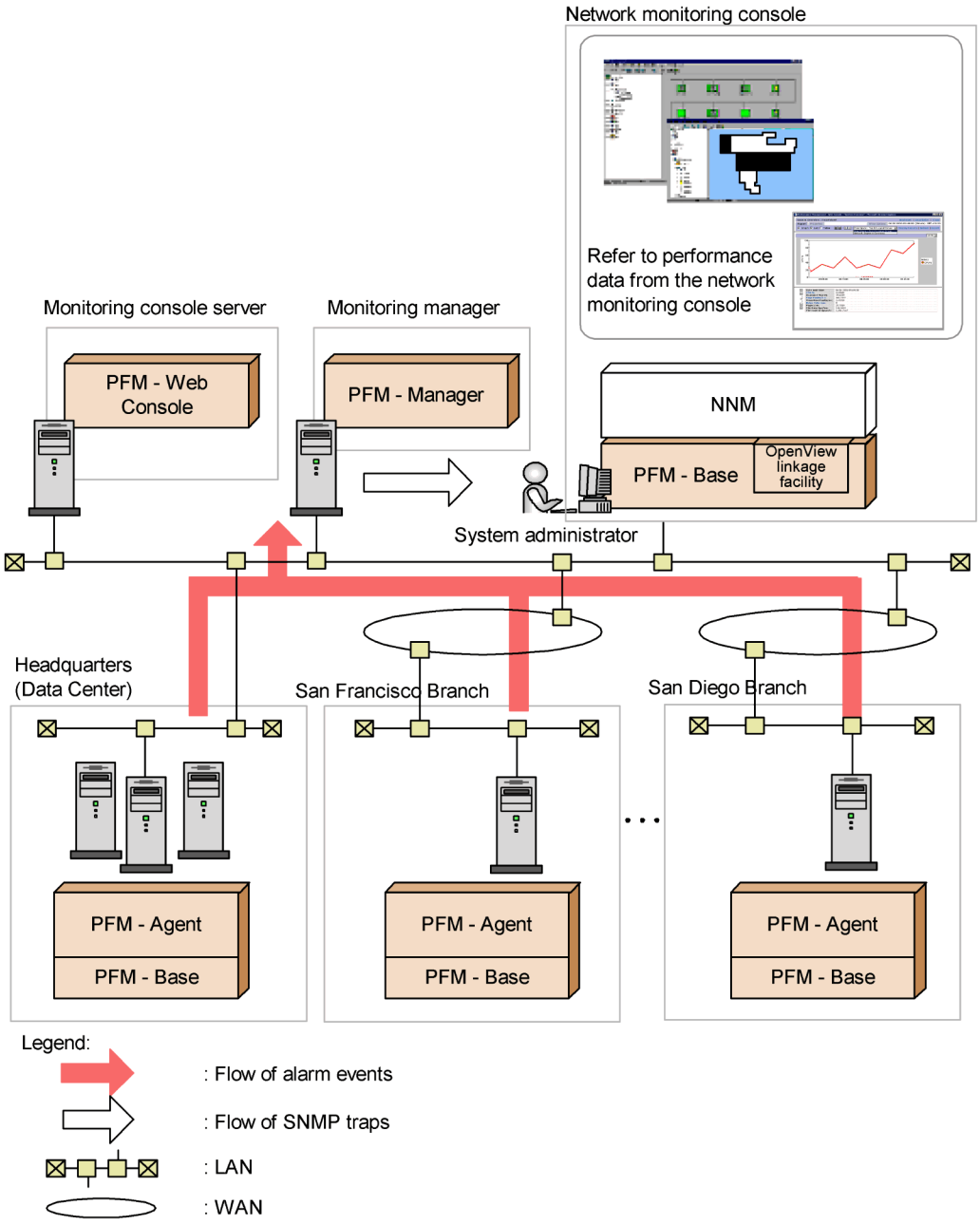
11.1 Overview of linking with Network Node Manager (NNM) for operation monitoring

Performance Management enables you to monitor operations by linking with NNM.

When the program being monitored exceeds a threshold value, an alarm event occurs, enabling Performance Management to issue an SNMP trap. For this reason, you can monitor errors that occur on Performance Management by using SNMP traps from NNM. Linking with NNM enables you to monitor the status of Performance Management or other JP1 products in the network monitoring window of NNM, or to display reports by starting the Performance Management window from the network monitoring window of NNM.

The following figure shows an example of operation monitoring by Performance Management when it is linked with NNM.

Figure 11-1: Example of operation monitoring by Performance Management when linked with NNM



Reference note: What is *NNM*?

NNM is a product for managing JP1 products in the network. NNM provides functionality for integrated management of an entire business information system. Also, NNM provides functionality for integrated management of networks of business information systems. NNM enables you to manage large-scale networks by using SNMP protocols and implement integrated management of node information configurations in systems on the network management console. For details on NNM, see the HP NNM documentation.

11.2 Constructing the linkage with NNM

This section describes procedures to install, set up, perform unsetup, and change configurations for constructing environments required for linking with NNM.

11.2.1 Supported OSs for linking with NNM

The following table lists supported OSs for using the OpenView linkage facility.

- In Windows:

Table 11-1: Supported OSs for linking with NNM (in Windows)

OS name	NNM linkage
Windows Server 2003 (x86)	Y
Windows Server 2003 (x64)	N#
32-bit version of Windows Server 2008	N
64-bit version of Windows Server 2008	N

Legend:

Y: Supported

N: Not supported

#

Although the OpenView linkage facility can be installed, the facility cannot be used.

- In UNIX:

Table 11-2: Supported OSs for linking with NNM (in UNIX)

OS name	NNM linkage
HP-UX	Y
Solaris (SPARC)#1	Y
Solaris (x64) or Solaris (x86)#2	N
AIX	N
Linux	N

Legend:

Y: Supported

N: Not supported

#1

Indicates Solaris 9 (SPARC) and Solaris 10 (SPARC).

#2

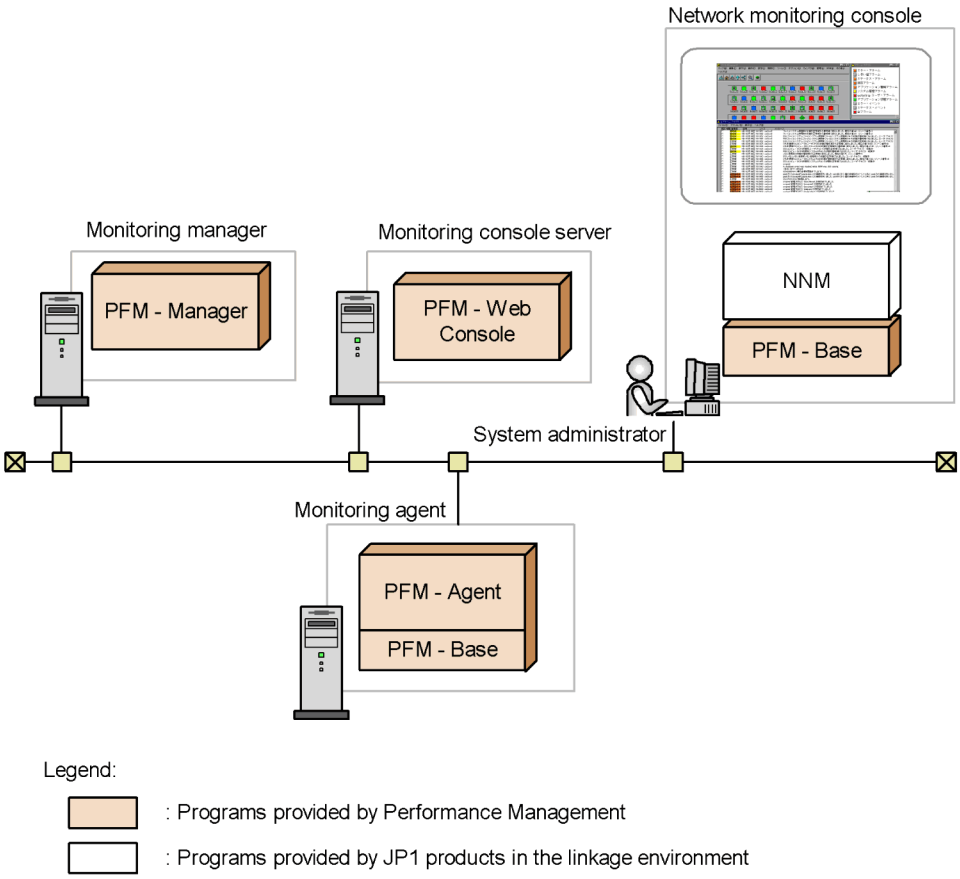
Indicates Solaris 10 (x64) and Solaris 10 (x86).

11.2.2 Installation

To use the OpenView linkage facility, you need to install PFM - Manager or PFM - Base on a host that has NNM installed.

The following figure shows the configuration when PFM - Base is installed.

Figure 11-2: Configuration for using the OpenView linkage facility



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

11.2.3 Setup

This subsection describes the setup procedures for using the OpenView linkage facility. Implement the setup on a host that has NNM installed.

Notes on setting up the OpenView linkage facility:

- Execute the setup command (`jpcconf ov enable` for Windows, `jpcconf ov enable` for UNIX) with the NNM service started and the NNM windows closed.
- NNM command errors during setup are normally output to the standard error output. However, even if an NNM command error occurs, a setup command

might output a normal termination of the NNM command to the standard output.

- To use the OpenView linkage, you need to set **On-Demand: To what level should submaps be persistent?** in `All Levels`. Display the settings of NNM IP Map from the map properties, and check or change the persistent submap level.
- If the name of a Performance Management monitoring host differs from its actual host name, you must change the DNS settings or the `hosts` file settings on the Manager host or on the host where NNM is installed. Changes are as follows:

  When updating the DNS settings

  Use the `A` record to register the actual host name and the `CNAME` record to register the monitoring host name.

  When changing the setting in the hosts file

  After the IP address, first specify the *actual-host-name*, and then that *monitoring-host-name*. If host names other than the Performance Management monitoring host name exist in the file, the *actual-host-name* must be specified before those names, as well.

  Example of the `hosts` file:

  ```
  ****.****.****.**** HostA AliasB
  ```

To add an agent:

1. Execute setup to add an agent.
2. Set up the destination of the SNMP traps.
3. Modify the NNM linkage definition file.
4. Execute the setup command.
5. Define issuing of SNMP traps and reports by alarm definition.

(1) Executing setup to add an agent

Execute setup to add an agent to be monitored through NNM linkage. Skip this procedure if PFM - Manager has been installed on a host that has NNM, and PFM - Agent or PFM - RM is already registered when PFM - Manager is setup.

PFM - Manager version 09-00 or later automatically registers PFM - Agent or PFM - RM, so no additional setup is required for the PFM - Agent or PFM - RM information. However, if the release date of PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent or PFM - RM must be registered manually. For details on the release dates for PFM - Manager, PFM - Agent, and PFM - RM, see the *Release Notes* for each program.

When PFM - Manager has not been installed and PFM - Base has been installed instead on a host that has NNM, copy the setup files for PFM - Agent or PFM - RM onto a host that has NNM, and then execute the setup command in the same way as you would to register PFM - Agent or PFM - RM during the setup of PFM - Manager.

(a) Copying the setup files for PFM - Agent or PFM - RM

To copy the setup files from a host that has PFM - Agent or PFM - RM onto a host that has PFM - Base installed:

1. Copy the setup files for PFM - Agent or PFM - RM in binary mode.

   The following table describes file locations and destinations to which files are copied.

   Table 11-3: Setup files to be copied

Platform		File	
Source PFM - Agent or PFM - RM	Destination PFM - Agent	Source PFM - Agent or PFM - RM	Destination PFM - Agent
Windows	Windows	*installation-folder*\setup\jpc*xxxx*w.EXE	*installation-folder*\setup
	UNIX	*installation-folder*\setup\jpc*xxxx*u.Z	/opt/jp1pc/setup
UNIX	Windows	/opt/jp1pc/setup/jpc*xxxx*w.EXE	*installation-folder*\setup
	UNIX	/opt/jp1pc/setup/jpc*xxxx*u.Z	/opt/jp1pc/setup

Legend:

xxxx indicates the service key for each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

(b) Executing the setup command on the PFM - Base host

Execute the following command on the PFM - Base host to set up PFM - Agent or PFM - RM.

```
jpcconf agent setup -key xxxx
```

xxxx indicates the service key for each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

For example, execute the following command to set up PFM - Agent for Oracle:

```
jpcconf agent setup -key Oracle
```

Note:

An error might occur if you execute the `jpcconf agent setup` command when Performance Management programs and services have not completely stopped on the local host where you want to execute the command. In such cases, make sure that Performance Management programs and services have completely stopped, and then re-execute the `jpcconf agent setup` command.

You can delete the setup files for PFM - Agent or PFM - RM after this procedure has finished.

(2) Setting up the destination of SNMP traps

Set up the required alarms in the window of PFM - Web Console in order to manage networks by using NNM. Set up the destination of SNMP traps in the alarm settings.

To set up the destination of SNMP traps:

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

   You must log on with a user account that has administrator user permissions.

   The Main window of PFM - Web Console appears.

2. In the navigation frame of the Main window, select the **Services** tab.

   The Services window appears.

3. In the navigation frame of the Services window, select the **PFM - Manager** folder.

   Services of PFM - Manager are displayed.

4. Select a Trap Generator service.

   A Trap Generator service is a service whose name begins from `PC`, or `<Trap Generator>`.

   The selected Trap Generator service is marked with a checkmark.

5. Select the **Properties** method in the method frame.

   The Properties window of a Trap Generator service appears with the properties displayed hierarchically.

6. Select the **ADD OR DELETE A TRAP DESTINATION** folder.

   Properties are displayed under the information frame.

7. In **Value** of **ADD A DESTINATION**, specify the host name or IP address of the destination of SNMP traps.

8. Click the **OK** button.

   The folder specified as the destination of SNMP traps is added Under the *Trap Destinations* folder.

9. Select the added folder of the SNMP traps destination.

   Properties are displayed under the information frame.

10. Change the settings.

    You can specify the contents as follows:

    Retry Count

    Specify an integer from 0 to 32767 for the number of times a SNMP trap is transmitted. The default value is `1` (time). The default value is used if you specify `0`.

    Retry Interval

    Specify an integer from 0 to 32767 for the interval (seconds) between retransmissions of SNMP traps. The default value is `5` (seconds). The default value is tentatively used if you specify `0`.

    Trap Port

    Specify a number from 1 to 32767 for the port number of the destination of SNMP traps. The default value is `162`. The default value is tentatively used if you specify `0`.

    Enabled

    Select `Yes` or `No` to specify whether or not to transmit SNMP traps. The default value is `Yes`.

11. Click the **OK** button.

    The settings are saved.

(3) Modifying the NNM linkage definition file

Modify the NNM linkage definition file (`jpcnnm.ini`) to establish linkage with NNM.

The NNM linkage definition file provided by Performance Management is stored in the following directory on a host that contains NNM:

- In Windows:

  installation-folder`\NNMEx\jpcnnm.ini`

- In UNIX:

  `/opt/jp1pc/NNMEx/jpcnnm.ini`

  Define the sections listed in the following table for the `jpcnnm.ini` file.

Table 11-4: Sections to be set up in jpcnnm.ini and their settings

Role	Section name	Setting
Associates PFM - Manager host name with PFM - Web Console host name and port numbers	[Manager Definitions]	*PFM - manager-host-name*=*PFM - Web- Console-host-name*: *PFM - Web- Console-port-number* You can omit the Web Console port number but not the Web Console host name. The port number that is set as a default for clients is used if you omit a port number. Host names of PFM - Manager are case-insensitive. Although you can define multiple host names, you cannot define the same host.
Paths to browsers	[Commons]	`browserpath=`*path-to-browser* This item *cannot* be omitted. If the browser path contains a space, enclose the path in double quotation marks ("").

Notes:

- Lines are ignored if you enter any blank characters (such as spaces) in front of sections or labels.
- Lines are ignored if there are no equal signs (=) after labels.
- The setting will not work properly if you enter any blank characters (such as spaces) after port numbers.

The following table lists examples of settings in the `jpcnnm.ini` file.

Table 11-5: Examples of settings in the jpcnnm.ini file

Setting item	Setting example
PFM - Manager host name	`PFMMGR`
PFM - Web Console host name	`PFMWEBCON`
Port numbers of PFM - Web Console host	`20358`
Browser path of host that has OpenView linkage facility installed.	`C:\Program Files\Internet Explorer\IEXPLORE.EXE`

Figure 11-3: Example of settings in the jpcnnm.ini file

```
        :
[Manager Definitions]

PFMMGR=PFMWEBCON:23015

[Commons]

browserpath="C:\Program Files\Internet Explorer\IEXPLORE.EXE"
        :
```

Note:

Define multiple PFM - Managers in the `Manager Definition` section of the `jpcnnm.ini` file as follows if multiple PFM - Managers exist in the systems.

```
        :
[Manager Definitions]

host-name-of-PFM - manager1 = host-name-of-PFM - web console1: port-number
host-name-of-PFM - manager2 = host-name-of-PFM - web console2: port-number

        :
```

If multiple PFM - Managers are defined, the window for selecting PFM - Manager for the connection destination appears when you start the window of PFM - Web Console from NNM. Select PFM - Manager to be connected in the window to display the Login window of PFM - Web Console. If a single PFM - Manager has been specified in the `Manager Definition` section of the `jpcnnm.ini` file, the window for selecting PFM - Manager for the connection destination does not appear and the Login window of PFM - Web Console appears.

(4) Executing the setup command

Execute the setup command provided by Performance Management. The environment setup for linking with NNM is performed and the services of the OpenView linkage function are started when you execute the command.

Execute the `jpcconf ov enable` command.

Note:

Perform the following setup procedure if you specify multiple PFM - Managers in the `Manager Definition` section of the `jpcnnm.ini` file.

1. Execute the `jpcconf ov enable -mkhtml` command.

   An HTML file for the window to select PFM - Manager is created.

2. Execute the `jpcconf ov enable` command.

(5) Defining issuing of SNMP traps and reports by defining alarms

Set up the following items in the Alarms window of PFM - Web Console:

- Set up issuing of SNMP traps as an action.

  Set up issuing of SNMP traps as an action to be performed when an alarm is issued.

- Associating alarms with reports

  Enable displaying of reports in the window of PFM - Web Console from NNM.

The following procedure mainly describes operations for setting up SNMP traps to be issued and for associating alarms with reports.

To set up SNMP traps to be issued and associate alarms with reports:

1. Log on to PFM - Web Console as a user with administrator user permissions.
2. In the navigation frame of the Main window, click the **Alarms** tab.

   The Alarms window appears.
3. In the navigation frame of the Alarms window, select the alarm definition for which you want to issue SNMP traps.

   The selected alarm is marked with a checkmark.
4. Select the **Edit** method in the method frame.

   The Edit > Main Information window appears in the information frame.
5. Click the **Next** button several times until the Edit > Action window appears.
6. In **Actions to be executed**, select **SNMP**.

   Select the check boxes for the alarm statuses (**Abnormal**, **Warning**, or **Normal**) for which you want to issue SNMP traps.
7. In **Report to be displayed**, click the **Browse** button to select the report to be associated with the alarm.
8. Click the **Finish** button.

   SNMP traps are defined as alarm action, and the selected report is associated.

For details on defining alarms, see *6. Monitoring Operations with Alarms*.

11.2.4 Unsetup

This subsection describes the unsetup procedures for the OpenView linkage facility. Perform unsetup on a host that has NNM fully installed.

To perform unsetup:

1. Delete the destination of SNMP traps.
2. Delete the PFM - Agent or PFM - RM symbols from NNM.
3. Execute the unsetup command.
4. Delete information registered with NNM.

(1) Deleting the destination of SNMP traps

Delete the destination of SNMP traps in the window of PFM - Web Console.

To delete the destination of SNMP traps:

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

   Log on as a user with administrator user permissions.

   The Main window of PFM - Web Console appears.
2. In the navigation frame of the main window, click the **Services** tab.

   The Services window appears.
3. In the navigation frame of the Services window, select the **PFM - Manager** folder.

   Services of PFM - Manager are displayed.
4. Select a Trap Generator service.

   A Trap Generator service is a service whose name begins from `PC`, or `<Trap Generator>`.

   The selected Trap Generator service is marked with a checkmark.
5. Select the **Properties** method in the method frame.

   The Properties window of a Trap Generator service appears with the properties displayed hierarchically.
6. Select the **ADD OR DELETE A TRAP DESTINATION** folder.

   Properties are displayed under the information frame.
7. From the **DELETE A DESTINATION** pull-down list, specify the host name or IP address of the destination of SNMP traps that you want to delete.
8. Click the **OK** button.

   Under the **Trap Destinations** folder, the selected folders of the SNMP trap destinations are deleted.

(2) Delete the PFM - Agent or PFM - RM symbols from NNM

Start `ovw` and delete all of the PFM - Agent or PFM - RM symbols.

(3) Execute the unsetup command

Execute the unsetup command provided by Performance Management. The environment settings for linking with NNM are deleted and the services of the OpenView linkage function are terminated when you execute the command.

Execute the `jpcconf ov disable` command.

(4) Deleting information registered with NNM

Delete information that is not deleted by unsetup scripts, such as the definition for the NNM display.

Note:

Executing the following operations ((a) - (c)) will cause the PFM - Agent or PFM - RM symbols and events to be displayed incorrectly.

(a) Deleting MIB OID

From the ovw menu, choose **Options**, and then **Load/Unload MIB** to unload `jp1pc.oid`.

(b) Deleting the definition for SNMP events

To delete the definition for SNMP events:

1. From the ovw menu, choose **Options**, and then **Event Settings**.

   The Event Settings dialog box appears.

2. Select **PerformanceManagementTrap** from **Enterprises**.
3. Choose **Edit**, **Event**, and then **Delete** to delete events for the Performance Management Trap enterprise.
4. When you finish deleting all the events, choose **Edit**, **Enterprises**, and then **Delete** to delete **PerformanceManagementTrap**.
5. Choose **Edit**, and then **Additional Actions**.

   The Edit Additional Actions dialog box appears.

6. Delete **Performance Management Report**.

(c) Deleting the definition files

Delete the following files:

- In Windows:

  nnm-installation-folder`\fields\C\jpcovobj.frf`

  nnm-installation-folder`\snmp_mibs\vendor\Hitachi\jp1pc.oid`

  All the subordinate folders under *nnm-installation-folder*`\symbols\C\jp1pc\`

- In UNIX:

  `$OV_FIELDS/C/jpcovobj.frf`

  `$OV_SNMP_MIBS/Vendor/Hitachi/jp1pc.oid`

  All the subordinate directories under `$OV_SYMBOLS/C/jp1pc/`

  `$`*xxxx* indicates environment variables defined on NNM.

For details on environment variables of NNM, see the HP NNM documentation.

11.2.5 Changing configuration

You can change the configuration related to each setting of the OpenView linkage facility to match your environment.

This subsection describes items whose configuration can be changed by the OpenView linkage facility and the changing procedures.

Notes on changing configuration:

- When you manage information from multiple PFM - Managers by using NNM, use the same the same port number and connection user information for each PFM - Manager as specified in the application registration file.
- You need to change the configuration again after the re-setup when you again set up the OpenView linkage facility after changing configuration of the OpenView linkage facility.

(1) Changing port numbers

The OpenView linkage facility manages symbols of the NNM GUI via two managers: The object manager that processes SNMP traps as an NNM service and is installed on the same host as PFM - Manager or PFM - Base, and the map manager that is started from the NNM GUI and adds and updates symbols in the background. The `jp1pcovsvr` service is used to communicate between the object manager and map manager. The service uses the `22292/tcp` port number by default.

Reference note:

Use the `jpcconf port define` command to change the port number of the `jp1pcovsvr` service. For details on how to change the port number, see the chapter describing installation and setup in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*. For details on the `jpcconf port define` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

11.3 Operations for linkage with NNM

This section describes operational procedures for monitoring Performance Management from NNM. For details on settings or operations of NNM, see the HP NNM documentation.

11.3.1 Starting and terminating the service of the OpenView linkage facility

Execute the following commands to start or terminate the service of the OpenView linkage facility:

- To start the service of the OpenView linkage facility:

  ```
  %OV_BIN%\ovstart JPCObjMgr
  ```

- To terminate the service of the OpenView linkage facility:

  ```
  %OV_BIN%\ovstop JPCObjMgr
  ```

For details on commands provided by NNM, see the HP NNM documentation.

11.3.2 Monitoring alarm events from NNM

You can use the following methods to monitor alarm events of Performance Management from NNM.

- Monitoring alarm events from the NNM node submap
- Monitoring alarm events from the NNM alarms browser (event browser)
- Monitoring alarm events from the NNM management window

The following subsections describe each method.

(1) Monitoring alarm events from the NNM node submap

The PFM - Agent or PFM - RM symbol in which an alarm occurs is displayed in the node submap when SNMP traps are sent to NNM. If multiple alarms occur at the same time, the symbol is displayed in the color that indicates the most severe condition among the occurring alarms.

You can display reports related to alarms from the node submap if alarms have been associated with reports.

(a) Description of symbols displayed in the node submap

The following table describes the colors of symbols displayed in the node submap and their meanings.

Table 11-6: The symbol colors and their meanings

Symbol color#	Meaning
The color that indicates Normal (green)	Conditions of all the bind alarms are normal.
The color that indicates Minor (yellow)	A warning alarm has occurred.
The color that indicates Critical (red)	An abnormal alarm has occurred.
The color that indicates Unknown (light-blue)	The alarm condition cannot be determined.

#

The display colors in default configuration may differ depending on the NNM that is used.

(b) Displaying reports from the node submap

You can display the report window of PFM - Web Console from the node submap if alarms have been previously associated with reports.

To display reports from the node submap:

1. Click the symbol that indicates PFM - Agent or PFM - RM in the node submap, and choose **Administration**, **Performance Management**, and then **View Report**.

   The Login window of PFM - Web Console appears.

2. Enter the information required for log on to PFM - Web Console.
3. Click the **OK** button.

   A report is displayed in the window of PFM - Web Console.

(c) Initializing symbols

Symbols are not initialized even if status monitoring has finished in NNM. In this case, you must manually reset symbols to Normal.

To initialize symbols displayed in the node submap:

1. Click the symbol that indicates PFM - Agent or PFM - RM, and choose **Administration**, **Performance Management**, **Change Status**, and then **Normal**.

   The symbol that indicates PFM - Agent or PFM - RM is initially set at **Normal**.

(2) Monitoring alarm events from the NNM alarms browser (event browser)

When NNM receives SNMP traps from Performance Management, NNM displays the reported detailed information on the condition in the alarms browser (event browser).

(a) Description of messages displayed in the alarms browser

The event category of Performance Management is *status event*. Event severity differs depending on the conditions of the alarms that occur in Performance Management.

The following table describes event severity and alarm conditions.

Table 11-7: Event severity and alarm conditions

Event severity	Alarm condition
Normal	Normal (green)
Warning	Warning (yellow)
Critical	Abnormal (red)

The format of messages displayed in the alarm browser is as follows:

severity date/time source pfmagent-agent-type condition `status has changed.` *occurrence-location conditional-expression-or-value-of-threshold* |*report-information*| .

Meanings of items displayed in a message are described below.

severity

Indicates the event severity described in *Table 11-7*.

date/time

Indicates the date and time when an alarm event occurs.

source

Indicates PFM - Agent or PFM - RM in which an alarm event occurs.

pfmagent-agent-type

Indicates the agent type of PFM - Agent or PFM - RM in which an alarm event occurs.

condition

Indicates the alarm condition. One of the following values is displayed:

- NORMAL
- WARNING
- CRITICAL

occurrence-location

Indicates the PFM - Agent or PFM - RM instance name.

conditional-expression-or-value-of-threshold

Indicates the conditional expression and value specified in the alarm definition.

report-information

Indicates the report information associated with an alarm. The information is displayed in the following format:

pfm-agent-or-pfm-rm-host-name@pfm-manager-host-name@report-id

(b) Displaying reports from the alarm browser

You can display the report window of PFM - Web Console from the alarm browser if alarms have been previously associated with reports.

To display the report window of PFM - Web Console from the alarm browser:

1. Select an event in the alarm browser, and choose **Actions**, **Additional Actions**, and then **Performance Management Report**.

   The Login window of PFM - Web Console appears.

2. Enter the information required for log on to PFM - Web Console.

3. Click the **OK** button.

   A report is displayed in the window of PFM - Web Console.

(3) Monitoring alarm events from the NNM management window

You can display the window of PFM - Web Console from the NNM management window to check various settings of Performance Management.

To display the window of PFM - Web Console from the NNM management window:

1. In the NNM management window, choose **Administration**, **Performance Management**, and then **Launch WebConsole**.

   - When you define a single piece of PFM - Manager in the NNM linkage definition file

     The Login window of PFM - Web Console appears. Go to step 3.

   - When you define multiple pieces of PFM - Manager in the NNM linkage definition file

     The window to select the Manager appears. Go to step 2.

2. Click the host name of PFM - Manager to be connected.

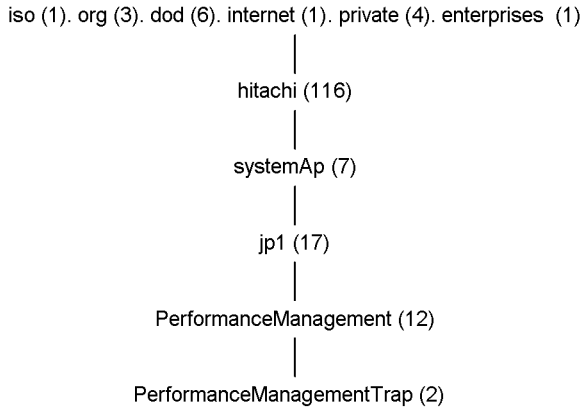
   The Login window of PFM - Web Console appears.

3. Enter the information required for log on to PFM - Web Console.
4. Click the **OK** button.
   The window of PFM - Web Console appears.

11.4 Configuration of MIB objects

The following figure shows the configuration of MIB objects for SNMP traps in Performance Management.

Figure 11-4: MIB object configuration



The following table describes the contents of MIB objects in Performance Management.

Table 11-8: Contents of MIB objects

Object ID	Contents
.1.3.6.1.4.1.116.5.17.12.2.1	PFM - Agent or PFM - RM instance numbers (ASCII codes of instance numbers)
.1.3.6.1.4.1.116.5.17.12.2.3	Report information specified at the definition of alarms *pfm-manager-host-name*@*report-id*
.1.3.6.1.4.1.116.5.17.12.2.6	Names of the Performance Management categories and conditional expressions of alarms
.1.3.6.1.4.1.116.5.17.12.2.7	Alarm values[#1]
.1.3.6.1.4.1.116.5.17.12.2.8	Alarm conditions • NORMAL • WARNING • CRITICAL

Object ID	Contents
.1.3.6.1.4.1.116.5.17.12.2.9	PFM - Agents or PFM - RM product-type identifiers For example, for PFM - Agent for Platform (Windows), the value is `Windows`; for PFM - Agent for Oracle, the value is `ORACLE`.
.1.3.6.1.4.1.116.5.17.12.2.10	Management units[#2] that cause alarms
.1.3.6.1.4.1.116.5.17.12.2.12	• In PFM - Agent Instance names of PFM - Agents • In PFM-RM Device ID of the remote agent or group agent
.1.3.6.1.4.1.116.5.17.12.2.13	Contents of message texts specified at the definition of alarms[#3]
.1.3.6.1.4.1.116.5.17.12.2.14	Names of alarm tables
.1.3.6.1.4.1.116.5.17.12.2.15	Names of alarms
.1.3.6.1.4.1.116.5.17.12.2.16	• In PFM - Agent Names of PFM - Agent hosts • In PFM-RM (remote agent) Monitored host name • In PFM-RM (group agent) Primary host name (PFM-RM host name)
.1.3.6.1.4.1.11.2.17.2.2.0	• In PFM - Agent Names of PFM - Agent hosts • In PFM-RM (remote agent) Monitored host name • In PFM-RM (group agent) Primary host name (PFM-RM host name)

#1

Multi-instance records operate as follows:

- When any value in the warning or abnormal condition is detected in target instances:

  User-defined messages specified when the alarm was defined are displayed in the message text (MIB object ID: 1.3.6.1.4.1.116.5.17.12.2.13). In this case, the data element value that causes event occurrence is the instance value in which an excess threshold value is first detected.

- When conditions return to normal from abnormal or warning:

  Nothing is specified in the message text even though normal events are issued because all the instance values become normal and the value that causes event occurrence is not determined. In this case, `<OK>` is specified as

a value of the data element that causes the event occurrence.

#2

Do not use this value during operations because Performance Management uses the value internally.

#3

Values displayed in message text are as follows:

1. `Alarm updated/deleted`: An alarm definition has been updated or deleted.
2. `Alarm deactivated`: An alarm has been deactivated.
3. `Alarm cleared`: An alarm bind has been cleared.
4. `Alarm expired`: Current time is out of the alarm evaluating hours.
5. *message-defined-by-user*: An alarm condition has changed to abnormal or warning from normal, or an alarm condition has changed to normal from abnormal or warning in a single instance record.
6. None: An alarm condition has changed to normal from abnormal or warning in a multi-instance record.

In the above messages 1 - 4, `(N/A)` is specified as a value of the data element that causes event occurrence.

Chapter

12. Linking with ODBC-Compliant Application Programs for Operation Analysis

This chapter describes setup procedures for linking Performance Management with an ODBC-compliant application program, and explains supported SQL functions.

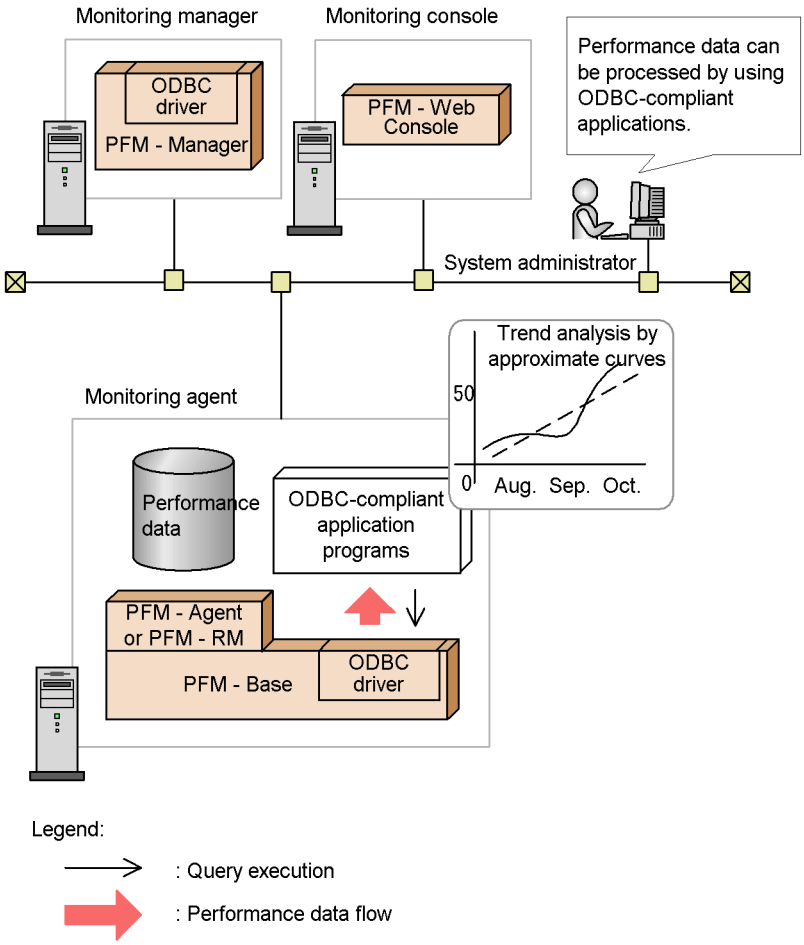
12.1 Overview of linking with an ODBC-compliant operation analysis application program
12.2 Installation and setup
12.3 Example of using Microsoft Excel to extract performance data
12.4 Notes

12.1 Overview of linking with an ODBC-compliant operation analysis application program

Performance Management enables an ODBC-compliant operation analysis application program to access performance data collected by a PFM - Agent or PFM - RM. Use the PFM ODBC driver to access performance data collected by the PFM - Agent or PFM - RM from an OBDC-compliant application program. System administrators can use performance data to analyze operation statuses by extracting or editing the performance data with an ODBC-compliant operation analysis application program such as Microsoft Excel.

The following figure shows the flow of data from Performance Management to an ODBC-compliant operation analysis application program.

Figure 12-1: Data flow from Performance Management to an ODBC-compliant operation analysis application program



Note:

You need to prepare the ODBC-compliant operation analysis application program separately in order to perform operation analysis.

12.2 Installation and setup

This section describes the installation and setup procedures for linking with an ODBC-compliant application program.

12.2.1 Supported OSs for linking with an ODBC-compliant application program

The following table lists supported OSs for linking with an ODBC-compliant application program.

Table 12-1: Supported OSs for linking with an ODBC-compliant application program

OS name	Linkage with an ODBC-compliant application
Windows Server 2003 (x86)	Y
Windows Server 2003 (x64)	--#
Windows Server 2008 (x86)	--
Windows Server 2008 (x64)	--

Legend:

Y: Supported

--: Not supported

#

Although the PFM ODBC driver can be installed, it cannot be used.

12.2.2 Installation

The PFM ODBC driver is installed on a host where PFM - Manager or PFM - Base has been installed. For details on how to install PFM - Manager and PFM - Base, see the chapter describing installation and setup (for Windows) in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The ODBC-compliant application program must be installed on the host where the PFM ODBC driver has been installed.

Note:

The PFM ODBC driver can be installed in Windows environments only.

12.2.3 Setup

The following describes the setup procedures for using the PFM ODBC driver.

(1) Performing additional setup for PFM - Agent or PFM - RM

To use a PFM ODBC driver to collect performance data, you must perform an additional setup for PFM - Agent or PFM - RM.

Skip this procedure if PFM - Manager has been installed on a host that uses the PFM ODBC driver, and PFM - Agent or PFM - RM has already been registered when PFM - Manager is setup.

You can omit this procedure if you are using PFM - Manager version 09-00 or later, because PFM - Agent or PFM - RM is registered automatically. However, if the release date for PFM - Agent or PFM - RM is later than that of PFM - Manager, PFM - Agent or PFM - RM needs to be registered manually.

If PFM - Manager has not been installed but PFM - Base has been installed on a host that uses the PFM ODBC driver, copy the setup files for PFM - Agent or PFM - RM onto a host that uses the PFM ODBC driver, and then execute the setup command in the same way as registering PFM - Agent or PFM - RM during the setup of PFM - Manager.

(a) Copying the setup files for PFM - Agent or PFM - RM

Copy, in binary mode, the setup files from a host that has PFM - Agent or PFM - RM onto a host that has PFM - Base installed. The following table lists the copy source and destination.

Table 12-2: Setup files to copy

Platform		File	
Copy source PFM - Agent or PFM - RM	**Copy destination PFM - Base**	**Copy source PFM - Agent or PFM - RM**	**Copy destination PFM - Base**
Windows	Windows	*installation-folder*\setup\jpc*xxxx*w.EXE[#]	*installation-folder*\setup\
	UNIX	*installation-folder*\setup\jpc*xxxx*u.Z[#]	/opt/jp1pc/setup
UNIX	Windows	/opt/jp1pc/setup /jpc*xxxx*w.EXE[#]	*installation-folder*\setup\
	UNIX	/opt/jp1pc/setup /jpc*xxxx*u.Z[#]	/opt/jp1pc/setup

#

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

(b) Executing the setup command on the PFM - Base host

Execute the following command on the PFM - Base host to set up PFM - Agent or PFM - RM.

```
jpcconf agent setup -key xxxx
```

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys, see the appropriate PFM - Agent or PFM - RM manual.

For example, execute the following command to set up PFM - Agent for Oracle:

```
jpcconf agent setup -key Oracle
```

Note

An error might occur if you execute the `jpcconf agent setup` command when Performance Management programs and services have not completely stopped on the local host where you want to execute the command. In such cases, make sure that the Performance Management programs and services have completely stopped, and then execute the `jpcconf agent setup` command.

You can delete the setup files for PFM - Agent or PFM - RM after this procedure has finished.

(2) Specifying the connection destination PFM - Manager

Before using the PFM ODBC driver, you must specify the PFM - Manager at the connection destination. Use the `jpcconf mgrhost define` command to set the PFM - Manager for the connection destination.

For example, execute the following command to specify the destination when you set the PFM - Manager on host `host01` as the connection target:

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

For details on the `jpcconf mgrhost define` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

Note:

Only one PFM - Manager can be specified as the connection target per host. If

more than one Performance Management program is installed on the same host, you cannot specify different PFM - Managers as connection destinations.

(3) Specifying data sources

Specify the data source of the PFM ODBC driver in the ODBC Data Source Administrator dialog box in Windows.

To specify the data source:

1. Display the ODBC Data Source Administrator dialog box.

   From the Windows **Start** menu, choose **Administrative Tools**, and then **Data Sources (ODBC)**. The ODBC Data Source Administrator dialog box appears.

2. Click the **System DSN** tab.

3. From **Name**, choose **Performance Management**, and then click the **Configure** button.

   The Performance Management Driver Data Source Setup dialog box appears.

4. Enter the information required for creating the data source.

   Specify the settings as follows:

Item	Details
Data Source Name	Specify the data source name that is required for the connection request from an ODBC-compliant application program. You can use 1-32 bytes of alphanumeric characters or symbols to specify the name. However, you cannot use the following symbols: [ ] { } ( ) , ; ? * = ! @ \ The default setting is `Performance Management`.
Description	Specify the text describing the function or contents of the data source. You can use 0-259 bytes of alphanumeric characters or symbols. However, you cannot use the following symbols: [ ] { } ( ) , ; ? * = ! @ You can omit this item.

5. To specify detailed options for the data source, click the **Options** button.

   The Performance Management Driver Data Source Options dialog box appears.

   Specify the settings as follows:

Item	Description
Instance Name Suffix	Specify the suffix to be added to the PFM ODBC driver instance name. You can use 0-8 bytes of alphanumeric characters to specify the suffix. You can omit this item.

Item	Description
Description	Specify the text describing the function or contents of the data source. You can use 0-259 bytes of alphanumeric characters or symbols. However, you cannot use the following symbols: [ ] { } ( ) , ; ? * = ! @ You can omit this item.
Use Alias Names in Output	Specify whether or not the PFM - Manager name of each field of records is included in output data. When you select this item, output data includes the PFM - Manager names.
Cache Node Names	Select whether to access the PFM - Manager each time data is required. When you select this item, the node name that is obtained during the first query is cached. In such a case, the node name is not requested during the second and subsequent queries. Any PFM - Agent or PFM - RM added during linkage with an ODBC-compliant application program is not searched for by the query.
Enable Debugging	Select whether to enable the debug function for the PFM ODBC driver. When you select this item, the debug function becomes active and trace logs are output. Use this item when an error occurs.
Show Progress During Connect	Select whether to display a progress message when the PFM ODBC driver connects to PFM - Manager. When you select this item, a progress message appears.
Trace PQL Requests	Select whether to enable traces of requests for Program Query Language (PQL). When you select this item, the trace function becomes active.
PQL Trace File	When you select **Trace PQL Requests**, specify the name of the file where traces are output. The name must be an absolute path name of 1 - 259 bytes.

6. Click the **OK** button.

   The Performance Management Driver Data Source Setup dialog box appears.

7. Click the **OK** button.

   The ODBC Data Source Administrator dialog box appears.

8. Click the **OK** button.

12.3 Example of using Microsoft Excel to extract performance data

This section describes an example of using Microsoft Excel in Windows, to extract performance data of Performance Management.

To extract the CPU usage of a Web application server, as collected by PFM - Agent for Platform (Windows), into a Microsoft Excel worksheet:

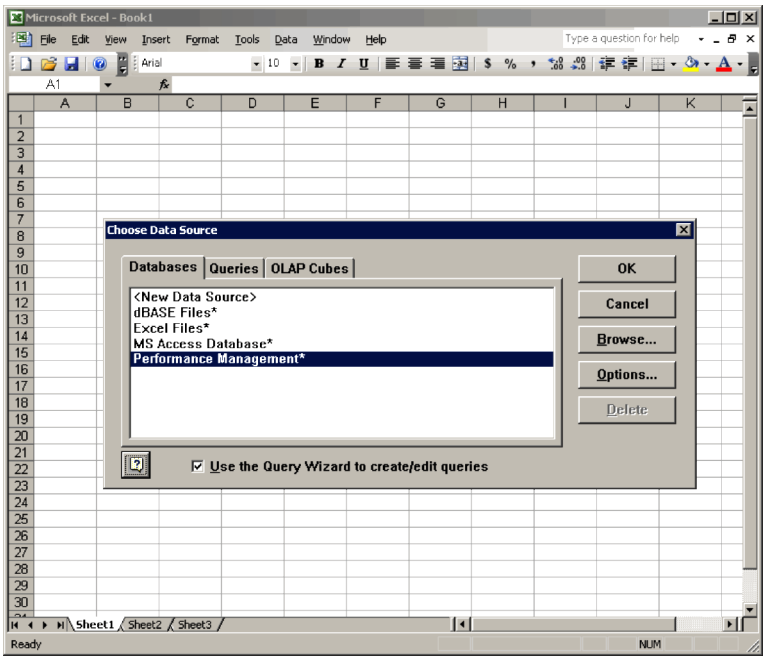
1. In Microsoft Excel, choose **Data**, **Get External Data**, and then **New Database Query**.

   The Choose Data Source dialog box appears.

2. Click the **Databases** tab.

   The **Databases** tab appears.

3. Choose **Performance Management**.



4. Click the **OK** button.

   The Query Wizard - Choose Columns dialog box appears.

   In **Available tables and columns**, each field name of a PFM - Agent or PFM - RM record is displayed as a PFM - Manager name.

For details on the PFM - Manager names used for each record field, see the chapters that describe records in the PFM - Agent or PFM - RM manuals.

5. In **Available tables and columns**, select a table and column from which data is extracted, and then click the **Next** button.

   The selected table and column appears in **Columns in your query**.

   Then, from the NT_PI table, add the following items to **Columns in your query**.

Item name	Description
PI_DATETIME	The record key indicating the record creation date and time.
PI_PCT_TOTAL_PROCESSOR_TIME	Processor usage (%).
PI_DEVICEID	A host name on which PFM - Agent or PFM - RM is running.

   Point:

   You must specify at least one ODBC key field for a query. If you click the **Finish** button without specifying any fields, the KAVE07013-E message is output. For details on ODBC key fields, see *12.4.4 Specifying common key fields*.

6. Click the **Next** button.

   The Query Wizard - Extract Data dialog box appears.

7. Specify the conditions for extracting the data.

   In **Column to extract**, each field name of a PFM - Agent or PFM - RM record is displayed as the PFM - Manager name.

   Note:

   Symbols that you can use to specify conditions are: =, <>, >, <=, <, and <=.

8. Click the **Next** button.

   The Query Wizard - Sort Order Settings dialog box appears.

9. Specify the sort order of data to be extracted.

10. Click the **Next** button.

    The Query Wizard - Finish dialog box appears.

11. Select **Return data to Microsoft Excel** and click the **Finish** button.

    When the query wizard finishes, the Query Wizard terminates and the Extract External Data to Microsoft Excel dialog box appears.

12. Specify the output destination for data to be extracted and then click the **OK** button.

    The extracted performance data is output to the specified output destination.

12.4 Notes

This section gives cautionary notes on accessing Performance Management performance data from an ODBC-compliant application program by using the PFM ODBC driver.

12.4.1 Supported SQL functions

The PFM ODBC driver is a read-only driver that supports a subset of SQL-92 entry level. The following table lists and describes SQL functions supported by the PFM ODBC driver.

Table 12-3: Supported SQL functions

Function		Supported item
Data type	-	Supported data types are as follows: • char • date • double • float • integer • long • real • smallint • time • timestamp • Tinyint • varchar
Syntax	Statement	Only the `SELECT` statement is supported.
	`GROUP BY` clause	Supported.
	`ORDER BY` clause	Supported.
	`WHERE` clause	Supported.
	`FROM` clause	Only one table can be specified for each query.
	Search condition	Symbols including `<`, `>`, `<=`, `>=`, `=`, `<>`, `IN`, `AND`, `OR`, and `NOT` are supported as comparison predicates. Note that subqueries are not available.
	Expression	Supported only in `SELECT` lists.
	Escape sequence	Date, time, and time-stamp (`d`, `t`, `ts`) are supported.

12.4.2 Supported expressions

The PFM ODBC driver supports the use of scalar operation expressions from only those in the selection list of the `SELECT` statement. Operation expressions and subqueries are not supported in search conditions such as the `WHERE` clause. Follow the standard rules for operator precedence, expression syntax, and the use of parentheses except for the following points:

- A string of literal characters cannot contain double quotation marks (`"`).
- In a common key field, only the AND operator can be used. For details on common key fields, see *12.4.4 Specifying common key fields*.
- Operation order is not guaranteed among connection clauses that have the same priority. If you give a condition expression in which the left-to-right ordering does not hold, clarify priority by using parentheses (`( )`). For reference, note the following examples.

  Examples:

  ```
  A and B and C
  ```

  In this case there is no problem because the left-to-right ordering holds.

  ```
  A or B and C
  ```

  In these cases, the left-to-right ordering does not hold so you have to provide a clearer definition: `A or (B and C)` or `(A or B) and C`.

(1) Type conversion

The PFM ODBC driver supports all of the standard type conversions. Internally, a numerical type is one of the following types:

- SQL_TINYINT (1-byte signed integer)
- SQL_SMALLINT (2-byte signed integer)
- SQL_INTEGER (4-byte signed integer)
- SQL_DOUBLE (8-byte floating point number)

The type of each column is defined in the data dictionary of the ODBC Driver. For example, the SQL_SMALLINT-type column can be added to the SQL_DOUBLE-type column. The resulting column from additions is the smallest type to store the result, which in this case is the SQL_DOUBLE column.

(2) Values of date, time, and time-stamp

The PFM ODBC driver supports expressions including the following values, which indicate date, time, and time-stamp.

- SQL_DATE

- SQL_TIME
- SQL_TIMESTAMP

When using these values, the following rules are applied:

- Addition (+) and subtraction (-) can be used.
- The SQL_DATE column is represented as the number of days. For example, adding 3 to the SQL_DATE column results in incrementing the date by 3 days.
- The SQL_ TIME and SQL_TIMESTAMP columns are represented as the number of seconds. For example, adding 3 to the SQL_TIME column results in incrementing the value by 3 seconds. The following are reference time values:
  - SQL_TIME: 0:00 a.m.
  - SQL_TIMESTAMP: 1970-01-01 at 0:00
- The SQL_TIME column can only be added to the SQL_DATE column. Also, the SQL_DATE column can only be added to the SQL_TIME column. The addition result column is the SQL_TIMESTAMP column. This feature comes in useful when you perform an operation that can affect both time and date. Note that other operations that relate to the date, time, and time-stamp columns are not supported on either side of an expression operator.
- Specify 0:00 a.m. as `00:00:00`. Also, specify 0:00 p.m. as `12:00:00`.
- When you specify the `DATE` value, `TIME` value, or `DATETIME` value in the `WHERE` clause, escape sequences and literal characters must be specified in the following format: Specify character strings in the *YYYY/MM/DD hh:mm:ss* format. For details on how to specify the names of columns and tables, see *12.4.3 Specification rules for the names of columns and tables*.

  Escape sequence:

  ```
  WHERE NT_PI_TCP.PI_TCP_DATETIME = {ts 'YYYY-MM-DD hh:mm:ss'}
  WHERE NT_PI_TCP.PI_TCP_DATE = {d 'YYYY-MM-DD'}
  WHERE NT_PI_TCP.PI_TCP_TIME = {t 'hh:mm:ss'}
  ```

  String of literal characters:

  ```
  WHERE NT_PI_TCP.PI_TCP_DATETIME > 'YYYY/MM/DD hh:mm:ss'
  WHERE NT_PI_TCP.PI_TCP_DATE = 'YYYY/MM/DD'
  WHERE NT_PI_TCP.PI_TCP_TIME = 'hh:mm:ss'
  ```

12.4.3 Specification rules for the names of columns and tables

The following are the specification rules for names of columns and tables for when you

extract performance data of Performance Management by using the PFM ODBC driver:

- Column name

  database-id_field-name

- Table name#

  product-type-identifier_record-name

#

When a PFM - Agent or PFM - RM has multiple data models, the data model version must be specified for the table name, for all except the latest data model.

When you need to specify the data model version, specify the table name as follows:

product-type-identifier_record-name_data-mode-version

Items to be specified are as follows:

database-id

For the database ID, specify an identifier that indicates the type of the Store database.

Identifiers that can be specified and their meanings are as follows:

- `PI`: Indicates a record of the PI record type.
- `PD`: Indicates a record of the PD record type.

You may also be able to specify another database ID depending on the PFM - Agent or PFM - RM. The database ID consists of the initials of the record type. For details on record types of each PFM - Agent or PFM - RM, see the chapters giving an overview of PFM - Agent or PFM - RM in the PFM - Agent or PFM - RM manuals.

field-name

Use the PFM - Manager name to specify the field name of each record where performance data collected by PFM - Agent or PFM - RM is stored. For details on field names of each record, see the chapters that describe records in the PFM - Agent or PFM - RM manuals.

product-type-identifier

Specify an identifier that indicates the type of each Performance Management program. For details on product type identifiers of each PFM - Agent or PFM - RM, see the lists of identifiers in the Appendixes of the PFM - Agent or PFM - RM manuals.

record-name

Use the PFM - Manager name to specify the name of the record where performance data collected by the PFM - Agent or PFM - RM is stored. For details on record names, see the appropriate chapters that describe records in each PFM - Agent or PFM - RM manual.

data-model-version

When the PFM - Agent or PFM - RM has multiple data models, the data model versions need to be specified. For details on the data model versions, see the appropriate chapters that describe records in each PFM - Agent or PFM - RM manual.

When you extract the Active Transactions (`ACTIVE_TRANSACTIONS`) field of the Activity Summary (`PD_PDAS`) record by using the PFM - Agent for Oracle, specify the names of a column and table as follows:

- Column name: `PD_ACTIVE_TRANSACTIONS`
- Table name: `ORACLE_PD_PDAS`

Also, when you extract the Active Transactions (ACTIVE_TRANSACTIONS) field of the Activity Summary (PD_PDAS) record by using the PFM - Agent for Oracle with multiple data models, specify the table name as follows:

- Table name: `ORACLE_PD_PDAS_4.0`

12.4.4 Specifying common key fields

The PFM - Agent or PFM - RM store database contains records with keys. You must specify at least one ODBC key field for a query.

The following table lists and describes the ODBC key fields that are common among PFM - Agents or PFM - RM.

Table 12-4: Common ODBC key fields

Common ODBC key field	Description
record-id`_DATE`	The record key that indicates the record creation date
record-id`_DATETIME`	Combination of *record-id*`_DATE` and *record-id*`_TIME` fields
record-id`_DEVICEID`	For an Agent which starts an instance: *instance-name* [*host-name*] For an Agent which does not start an instance: *host-name*

Common ODBC key field	Description
*record-id*_DRAWER_TYPE	Classification. Valid values are as follows: *m*: minute *H*: hour *D*: date *W*: week *M*: month *Y*: year
*record-id*_PROD_INST	Name of monitored system
*record-id*_PRODID	Product identifier
*record-id*_RECORD_TYPE	The 4-byte identifier that indicates the record type
*record-id*_TIME	Record creation time (GMT: Greenwich Mean Time)

Note:

For *record-id*, enter the record ID of each PFM - Agent or PFM - RM. For details on record IDs of each PFM - Agent or PFM - RM, see the chapters that describe records (record list) in the PFM - Agent or PFM - RM manuals.

Depending on the PFM - Agent or PFM - RM records, you may also be able to specify key fields other than common ODBC key fields. For details on available ODBC key fields, see the chapters that describe records (ODBC key field list) in the PFM - Agent or PFM - RM manuals.

12.4.5 Adjusting the time

Performance data of Performance Management is stored based on GMT by default. To adjust time to local time, add the GMT_ADJUST field.

For example, to adjust the time-stamp value to local time, specify the value as follows:

```
SELECT PI_TCP_DATETIME+PI_TCP_GMT_ADJUST, ...
FROM PI_TCP WHERE ...
```

12.4.6 Executing a query among multiple agents

When using the GROUP BY clause or ORDER BY clause to execute a query among multiple agents, the result is returned for each agent.

For example, when you collect data from Agent A and Agent B as follows, the collected result sets are returned as a group of separately sorted results for Agent A and Agent B. A result set for Agent A and Agent B is not sorted.

```
SELECT record-id_DATE, ... from ... where ...record-id_PROD_INST='A'
and
record-id_PROD_INST='B' ORDER BY record-id_DATE
```

12.4.7 Notes on using ODBC from Microsoft Excel

- When you execute a query from Microsoft Excel, you cannot specify strings including question marks (?) for values of the extraction condition fields. If you specify such a string, the KAVE07000-E message is output.
- When you obtain data by using the ODBC Driver from Microsoft Excel (Microsoft Query), you need to perform the following settings before filtering the data by date and time.

  Setting location:

  - In Windows

    Time tab (Choose **Control Panel**, **Regional and Language Options**, and then click the **Customize** button. The Customize Regional Options dialog box appears. Click the **Time** tab.)

  Setting contents:

  - Display the time in the 12-hour time format.
  - Select **AM** as the symbol to represent morning.
  - Select **PM** as the symbol to represent afternoon.
- You cannot specify extraction conditions based on multiple tables. Make sure that the columns you specify come from a single table.

Chapter

13. Detecting Problems within Performance Management

This chapter describes how to detect problems within Performance Management.

13.1 Overview of detecting problems within Performance Management
13.2 Using the health check function to check the operating status of monitoring agents and their hosts
13.3 Using the status management function to check service status
13.4 Using the PFM service automatic restart functionality to restart PFM services
13.5 Detecting problems by linking with the integrated system monitoring product

13.1 Overview of detecting problems within Performance Management

By using the health check function, you can detect problems within Performance Management itself. The health check function monitors the operating status of monitoring agents and their hosts, and makes the user aware of changes in the operating status by displaying the results in PFM - Web Console. If you use PFM - RM, you can check whether each monitoring host is running.

Also, you can use the PFM service automatic restart functionality to automatically restart a PFM service if it stops abnormally, or to schedule it to restart.

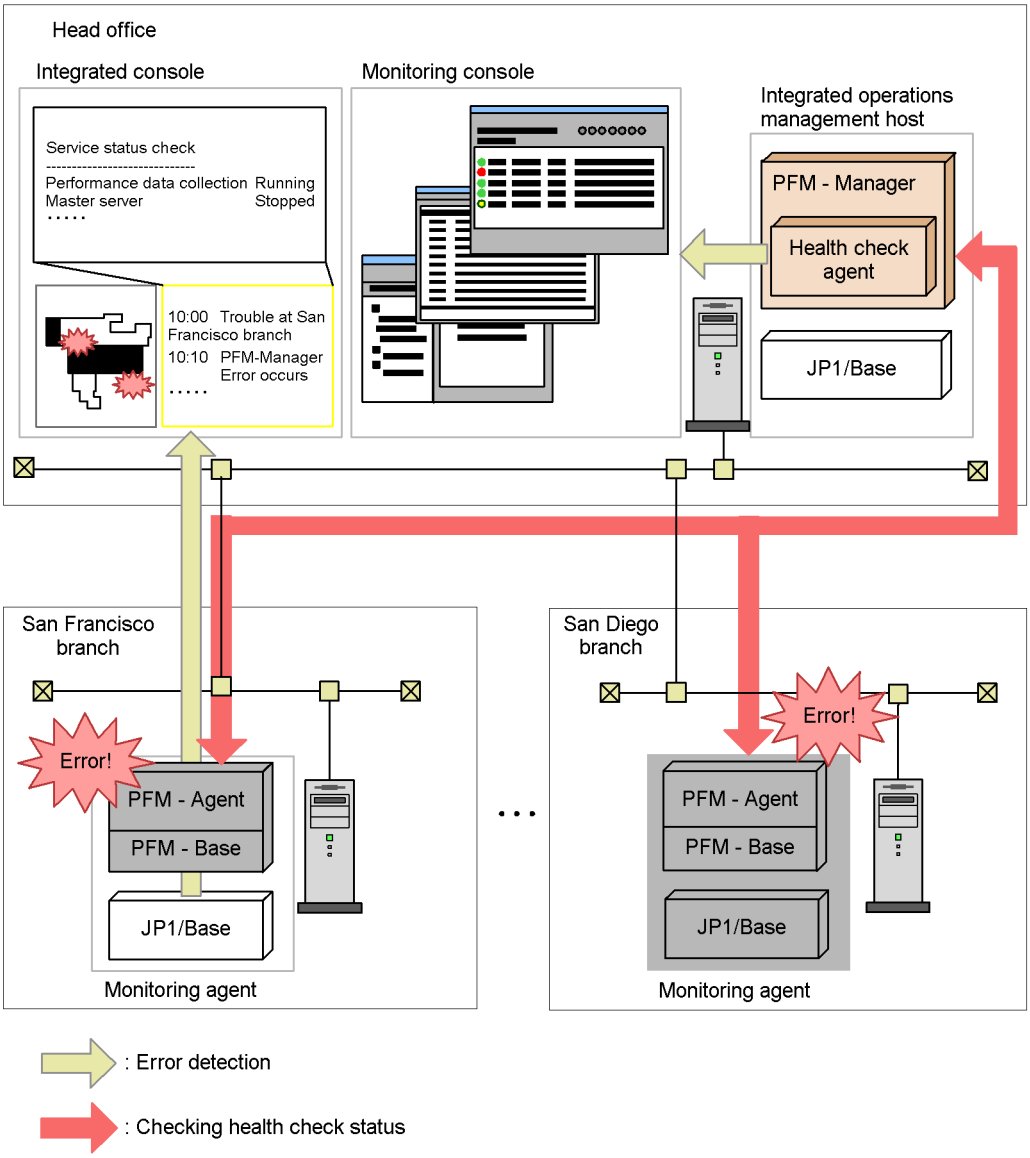
To use the health check function to monitor the operating status of monitoring agents, or to use the PFM service automatic restart functionality, use the status management function to monitor detailed information about Performance Management services.

For this reason, the version of the monitoring agent monitored by the health check function must support the status management function, and the status management function must be active. There are no prerequisites associated with monitoring the operating status of a host. To monitor the operating status of a host monitored by PFM - RM, you must enable the status management function on the PFM - RM host. Versions of PFM - Agent or PFM - RM that support the status management function differ for each Agent product. For details on the versions of PFM - Agent or PFM - RM that support the status management function, see *13.3 Using the status management function to check service status*.

You can also detect problems within Performance Management by using the integrated systems monitoring product JP1/Base to monitor the Performance Management log files. By using this feature, the system administrator can be made aware of problems in the system, identify the cause of the problem, and take the appropriate measures to resolve it.

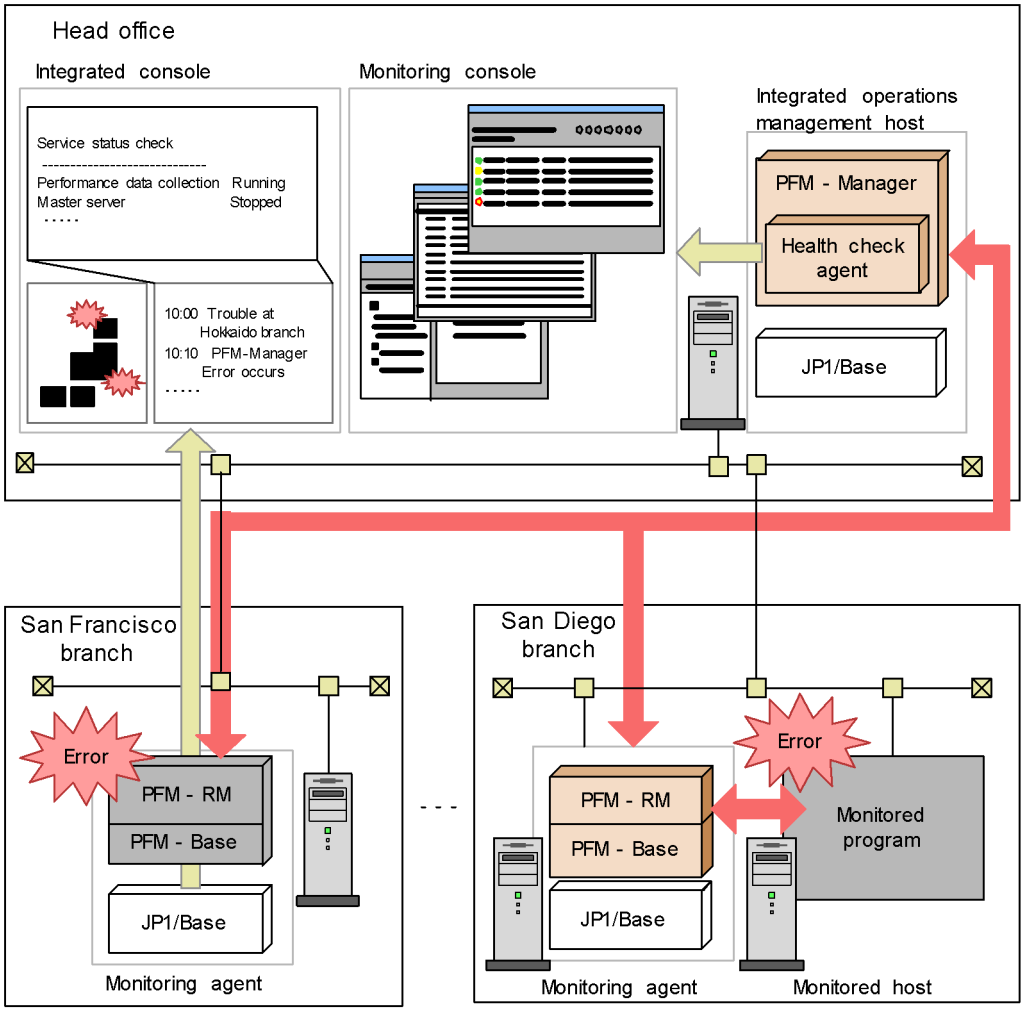
The following figure shows an example of using Performance Management to detect problems with the PFM - Agent at the San Francisco branch, and the host at the San Diego branch on which PFM - Agent is running.

Figure 13-1: Example of detecting problems in Performance Management itself(PFM - Agent)



The following figure shows an example of using Performance Management to detect problems with the PFM - RM at the San Francisco branch, and the host at the San Diego branch on which PFM - RM is running.

Figure 13-2: Example of detecting problems in Performance Management itself (PFM - RM)



13.2 Using the health check function to check the operating status of monitoring agents and their hosts

This section describes the health check function used to check the operating status of PFM - Agent or PFM - RM services, hosts running PFM - Agent or PFM - RM, or monitored host of PFM - RM.

Reference note:

You cannot use the health check function to monitor the status of the group agent.

13.2.1 Configuring the health check function

(1) Setting up the health check function

The following prerequisites must be met prior to using the health check function. If these prerequisite conditions are not met, you will not be able to use the health check function.

Monitoring the operating status of the host running the monitoring agent:

- Version 08-11 or later of PFM - Manager and Web Console
- Any version of PFM - Agent or PFM - RM

To monitor the operating status of a host monitored by PFM - RM, you must enable the status management function on the PFM - RM host. If the status management function is not enabled, the status of the remote agent is not recognized correctly.

Monitoring the operating status of the monitoring agent service:

The health check function uses the status management function to monitor the operating status of PFM - Agent services. For this reason, the product being monitored by the health check function must support the status management function. The prerequisite conditions for using the function are as follows. Any version of PFM - RM can be used.

- Version 08-11 or later of PFM - Manager and Web Console
- The version of PFM - Agent used supports the status management function.
- The status management function on the PFM - Agent or PFM - RM host is enabled.

Unless the second and third conditions are satisfied, the health check function will be unable to check the status of PFM - Agent or PFM - RM. For details on the versions of PFM - Agent that support the status management function, see *13.3*

Using the status management function to check service status. The following table describes support for operating status monitoring of services by PFM - Agent version.

Table 13-1: Support for operating status monitoring of services by PFM - Agent version

Status management function on monitored agent host	Version of monitored agent	Operating status monitoring of services
Enabled	07-00-01 or later	Can be used
Enabled	07-00 or earlier#1	Cannot be used#2
Disabled	n/a	Cannot be used#3

Legend:

n/a: Not applicable.

#1

When PFM - Agent 07-00 or earlier is installed on the same host as PFM - Agent 07-00-01 or later or PFM - Base 08-00 or later, and the status management function is enabled on the target PFM - Agent host

#2

The operating status monitoring of the agent service appears as `Not Supported`.

#3

The operating status monitoring of the agent service appears as `Unconfirmed`.

For details on how to configure the status management function, see *13.3.1 Configuring the status management function*.

To monitor the status of a host monitored by PFM - RM, you must enable polling with an appropriate PFM - RM property. For details on settings for PFM - RM polling, see *(d) Setting PFM - RM polling*.

(a) Enabling the health check function

To enable the health check function on the PFM - Manager host:

1. Stop Performance Management services.

   If Performance Management services are running on a physical host, stop the services by using the following command:

```
jpcspm stop -key jp1pc
```

To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpcconf hc enable` command

   To enable the health check function, use the following command:

   ```
   jpcconf hc enable
   ```

3. Check the status of the health check function.

   To confirm that the status of the health check function is `available`, use the following command:

   ```
   jpcconf hc display
   ```

4. Start Performance Management services.

   To start all Performance Management services on a physical host, use the following command:

   ```
   jpcspm start -key jp1pc
   ```

   To start all Performance Management services on a logical host, use the cluster software.

   The service ID is `0A1`*host-name* or `0S1`*host-name*.

Note:

When one of the services you are starting is PFM - Manager, and the health check function is enabled on the PFM - Manager host, the health check agent starts as one of the PFM - Manager services when you execute the `jpcspm start` command. When you execute the `jpcspm stop` command to stop the PFM - Manager services, the health check agent also stops.

You cannot specify `agt0` as the service key when you execute the `jpcspm start` or `jpcspm stop` commands.

(b) Disabling the health check function

To disable the health check function on the PFM - Manager host:

1. Stop Performance Management services.

   If Performance Management services are running on a physical host, stop the

services by using the following command:

```
jpcspm stop -key jp1pc
```

To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpcconf hc disable` command.

   To disable the health check function, use the following command:

   ```
   jpcconf hc disable
   ```

3. Check the status of the health check function.

   To confirm that the status of the status management function is `unavailable`, use the following command:

   ```
   jpcconf hc display
   ```

   If PFM - Manager is running in a logical host environment, execute the `jpcconf hc display` command on the PFM - Manager host on the executing or standby node.

4. Start Performance Management services.

   To start all Performance Management services on a physical host, use the following command:

   ```
   jpcspm start -key jp1pc
   ```

   To start all Performance Management services on a logical host, use the cluster software.

For details on each command, see the chapter describing the command in the manual *Job Management Partner 1/Performance Management Reference*.

(c) Checking the status of the health check agent

Use the `jpctool service list` command to check the status of the health check agent. You can also use the health check function to check the operating status of the health check agent. If the Agent Collector or Remote Monitor Collector service of the health check agent has terminated abnormally, the wrong health check results might be displayed.

(d) Setting PFM - RM polling

To monitor the status of a host monitored by PFM - RM, you must enable polling of the monitored host with an appropriate PFM - RM property. The following table describes the property to be set.

Table 13-2: Setting the polling property

Folder name	Property name	Description
Health Check Configurations	Health Check for Target Hosts	Specifies whether to perform polling to the monitored hosts. The default is `No`. `Yes`: Performs polling. `No`: Does not perform polling.

If polling is disabled, the operating status of the monitored host appears as `Not Supported`.

(2) Setting the health check agent properties

When the health check function is enabled, you can make settings related to the health check function, such as the collection interval for operation monitoring data and the monitoring level, by setting the properties of the health check agent from the Services tree of PFM - Web Console. The following table lists the health check agent properties you can set.

Table 13-3: Health check agent properties

Folder name	Property name	Description
Detail Records - HC	Description	Displays `Health Check Detail` as a description for the record.
	Log	Specifies whether to collect performance data. The default is `No`. `Yes`: Collects performance data. `No`: Does not collect performance data.
	Collection Interval	Specifies the collection interval in seconds, as a value in the range from 0 to 2,147,483,647. The default is 300. This value serves as the polling interval of the health check function.
	Collection Offset	Specifies the offset of the collection start time in seconds, as a value in the range from 0 to 32,767. The default is 0.
	LOGIF	Specifies the conditions for acquiring logs.

Folder name	Property name	Description
Health Check Configurations[#1]	Monitoring Level[#2]	Specifies the monitoring level. To monitor the operating status of the agent service, specify `Service`. To monitor the operating status of the agent host, specify `Host`. The default is `Host`.
	Polling Interval	Displays the polling interval. This value is taken from the Collection Interval in the PD_HC record.
	Incl. Action Handler	Specifies whether to include the Action Handler service when monitoring service operating statuses. The default is `No`. `Yes`: The Action Handler service is monitored. `No`: The Action Handler service is not monitored.
	Busy as Inactive	Specify whether agents whose service status remains Busy for extended periods should be considered inactive. The default is `No`. If you specify `Yes`, the Time to Busy as Inactive setting takes effect. `Yes`: The agent is considered inactive[#3]. `No`: The agent is not considered inactive. You can check the service status of an agent in the Status column in the output of the `jpctool service list` command.
	Time to Busy as Inactive Collector	Specifies how long[#3] busy statuses should persist for the Agent Collector and Remote Monitor Collector services before the services are considered inactive. Specify this item in seconds. The default is 300.
	Time to Busy as Inactive Store	Specifies how long[#3] busy statuses should persist for the Agent Store and Remote Monitor Store services before the services are considered inactive. Specify this item in seconds. The default is 300.
	Time to Busy as Inactive AH	Specifies how long[#3] a busy status should persist for the Agent Handler service before the service is considered inactive. Specify this item in seconds. The default is 300.

#1

When you change a setting in the Health Check Configurations folder, the new setting takes effect from the next polling interval.

#2

When you change the Monitoring Level setting, the health check results displayed in a realtime report of the health check agent differ according to whether polling under the new setting had taken place by the time the report was displayed.

Monitoring agent	Displayed health check results
Monitoring agent for which polling under the new setting has completed	The newest health check results recorded under the new setting
Monitoring agent for which polling under the new setting has not yet taken place	The newest health check results recorded under the old setting

For this reason, the report may briefly display results from both the old and new settings.

#3

The length of time a service is in Busy status is calculated from the difference between the time when polling occurred (the time on the host running PFM - Manager) and the time when the status of the service changed to Busy (the time on the host running PFM - Agent or PFM - RM). Make sure that the clocks are synchronized on all hosts that run Performance Management services.

13.2.2 Checking operating statuses

You can check the health check status of an agent by its icon in the agents tree of PFM - Web Console, as well as in the Event Monitor window and Event History window. You can also view more detailed information about the health check status by using the reports generated by the health check agent. Because health check agent reports only show information from monitoring agents for which polling has completed, you cannot display reports before polling has taken place. For details on the content of each window, see the chapters that describe the windows in the manual *Job Management Partner 1/Performance Management Reference*.

(1) In PFM - Agent

(a) Events issued when monitoring the operating status of the host running PFM - Agent

The following table describes the events that can occur when monitoring the operating status of the host on which the PFM - Agent is running.

Status	Description
Running	The health check function can communicate with the host where the monitoring agent is running.
Host Not Available	The health check function cannot communicate with the host where the monitoring agent is running.

You cannot check the status of the service when monitoring the operating status on a host level. When you want to see detailed information about the service, use the `jpctool service list` command.

(b) Events issued when monitoring the operating status of the PFM - Agent service

The following table describes the events that can occur when monitoring the operating status of the PFM - Agent service.

Table 13-4: Events issued when monitoring the operating status of the PFM - Agent service

Status	Description
Running	*The agent is fully functional and working normally* This status appears when the Agent Collector service and Agent Store service on the agent are both running. If you have configured the health check function to also monitor the Action Handler service on the host, then this status appears when all three services are running.
Incomplete	*The agent is only partially functional* This status appears in the following cases: • When the monitored agent allows the Action Handler service on the same host to be added as a monitoring target in the properties of the health check agent but the Action Handler service is not monitored, this status appears when the Agent Collector service is running and the Agent Store service is stopped#. If the Action Handler service is added as a monitored service, this status appears when the Agent Collector service is running but the Agent Store service or Action Handler service is stopped#. • The Agent Collector service on the agent is working in standalone mode
Not supported	*The agent does not support the status management function* This status appears when software that provides the status management function such as PFM - Base version 08-00 or later is installed on the host and the status management function is enabled, but the agent version is one that does not support the status management function, such as PFM - Agent 07-00. If the status management function is disabled on the host, Unconfirmed appears as the status.
Stopped	*The agent functionality is stopped* This status appears when the Agent Collector service on the agent is stopped#.
Unconfirmed	*The status of the agent cannot be confirmed* This status appears when the health check function cannot communicate with the Status Server service on the host where the agent is located. This may be because the status management function is disabled, or PFM - Agent 07-00 is running alone.
Host Not Available	*The host where the agent is located is stopped* This status appears when the health check function cannot communicate with the host where the agent is located.

#

A service is judged to have stopped when it has any status other than Active or

Busy. However, you can configure the health check function to consider a service stopped if the Busy status persists for longer than the period of time that you specify in the properties of the health check agent.

The following table describes the operating statuses of the host and monitoring agent services for each status.

Table 13-5: Health check status, host operating status and monitoring agent operating status

Status	Host where monitoring agent is running	Status Server	Agent Collector	Agent Store or Action Handler
Running	Y	Y	Y	Y
	Y	Y	Y	Y#
Incomplete	Y	Y	Y	N
	Y	Y	Y#	n/a
Not supported	Y	Y	(N)	n/a
Stopped	Y	Y	N	n/a
Unconfirmed	Y	N	n/a	n/a
Host Not Available	N	n/a	n/a	n/a

Legend:

Y: The host or service is running.

N: The host or service is stopped.

(N): The Agent Collector service does not support the health check function.

n/a: Has no bearing on status determination.

#: When running in standalone mode

(2) In PFM-RM

(a) Events issued when monitoring the operating status of the host running PFM - RM

The following table describes the events that can occur when monitoring the operating status of the host on which PFM - RM is running.

Table 13-6: Events issued when monitoring the operating status of the host running PFM - RM

Status	Description
Running	The health check function can communicate with the host where the monitoring agent is running.
Host Not Available	The health check function cannot communicate with the host where the monitoring agent is running.

You cannot check the status of the service when monitoring the operating status on a host level. When you want to see detailed information about the service, use the `jpctool service list` command.

(b) Events issued when monitoring the operating status of the PFM - RM service

The following table describes the events that can occur when monitoring the operating status of the PFM - RM service.

Table 13-7: Events issued when monitoring the operating status of the PFM - RM service

Status	Description
Running	*The PFM - RM is fully functional and working normally* This status appears when the Remote Monitor Collector service and Remote Monitor Store service on the PFM - RM are both running. If you have configured the health check function to also monitor the Action Handler service on the host, then this status appears when all three services are running.
Incomplete	*The PFM - RM is only partially functional* This status appears in the following cases: • When the PFM - RM allows the Action Handler service on the same host to be added as a monitoring target in the properties of the health check agent but the Action Handler service is not monitored, this status appears when the Remote Monitor Collector service is running and the Remote Monitor Store service is stopped#. If the Action Handler service is added as a monitored service, this status appears when the Remote Monitor Collector service is running but the Remote Monitor Store service or Action Handler service is stopped#. • The Remote Monitor Collector service on the PFM - RM is working in standalone mode
Stopped	*The PFM - RM functionality is stopped* This status appears when the Remote Monitor Collector service on the PFM - RM is stopped#.

Status	Description
Unconfirmed	*The status of the PFM - RM cannot be confirmed* This status appears when the health check function cannot communicate with the Status Server service on the host where the PFM - RM is located. This may be because the status management function is disabled.
Host Not Available	*The host where the PFM - RM is located is stopped* This status appears when the health check function cannot communicate with the host where the PFM - RM is located.

#

A service is judged to have stopped when it has any status other than `Active` or `Busy`. However, you can configure the health check function to consider a service stopped if the `Busy` status persists for longer than the period of time that you specify in the properties of the health check agent.

The following table describes the operating statuses of the host and monitoring agent services for each status.

Table 13-8: Health check status, host operating status and monitoring agent operating status

Status	Host where monitoring agent is running	Status Server	Remote Monitor Collector	Remote Monitor Store or Action Handler
Running	Y	Y	Y	Y
	Y	Y	Y	Y#
Incomplete	Y	Y	Y	N
	Y	Y	Y#	n/a
Stopped	Y	Y	N	n/a
Unconfirmed	Y	N	n/a	n/a
Host Not Available	N	n/a	n/a	n/a

Legend:

Y: The host or service is running.

N: The host or service is stopped.

n/a: Has no bearing on status determination.

#: When running in standalone mode

(c) Events issued when monitoring the operating status of the host monitored by PFM - RM

When the operating status of the PFM - RM monitoring host is monitored, different events are output depending on the monitoring level settings for the health check function.

The timing for the polling of the PFM - RM host by the health check agent is different from the timing for the polling of the monitored host by the PFM - RM host. If polling of the monitored host has not been performed yet, the operating status of the monitored host appears as `Not Supported`.

■ When the status management function is disabled

The following table describes the events that can occur when monitoring the operating status of the host monitored by PFM - RM.

Table 13-9: Events when monitoring PFM - RM-monitored host operating status (when polling is disabled)

Status	Description
Not supported	The PFM - RM monitoring host and the Status Service are operating normally.
Unconfirmed	Cannot communicate with the PFM - RM monitoring host or the Status Server service.

The following table describes the operating statuses of the monitored host and PFM - RM services for each status.

Table 13-10: Events when monitoring PFM - RM-monitored host operating status (when polling is disabled)

Status	PFM-RM host	Status Server	Remote Monitor Collector	Monitored host
Not Supported	Y	Y	n/a	n/a
Unconfirmed	N	n/a	n/a	n/a
	Y	N	n/a	n/a

Legend:

Y: The host or service is running

N: The host or service is stopped.

n/a: Has no bearing on status determination.

■ When the monitoring level is Host and polling is enabled

The following table describes the events that can occur when monitoring the operating

status of the host monitored by PFM - RM.

Table 13-11: Events when monitoring PFM - RM-monitored host operating status (when the monitoring level is Host and polling is enabled)

Status	Description
Running	*The monitored host is fully functional and working normally*
Not supported	*The monitored host has not been polled.*
Unconfirmed	*The status of the monitored host cannot be confirmed* This status appears in the following cases: • This status appears when the health check function cannot communicate with the PFM - RM monitoring host. • This status appears when the health check function cannot communicate with the Status Server service on the PFM - RM monitoring host. This may be because the status management function is disabled. • The Remote Monitor Collector service for the monitoring PFM - RM is not running. • Polling of the monitored host failed.
Host Not Available	*The monitored host is stopped.*

The following table describes the operating statuses of the monitored host and PFM - RM services for each status.

Table 13-12: Health check status, PFM - RM service status and monitored host operating status

Status	PFM-RM host	Status Server	Remote Monitor Collector	Monitored host
Not Supported	Y	Y	Y	P
Running	Y	Y	Y	Y
Unconfirmed	N	n/a	n/a	n/a
	Y	N	n/a	n/a
	Y	Y	N	n/a
	Y	Y	Y	C
Host Not Available	Y	Y	Y	N

Legend:

Y: The host or service is running.

P: Has not been polled

C: Communication failed.

N: The host or service is stopped.

n/a: Has no bearing on status determination.

■ When the monitoring level is Service and polling is enabled

The following table describes the events that can occur when monitoring the operating status of the host monitored by PFM - RM.

Table 13-13: Events when monitoring PFM - RM-monitored host operating status (when the monitoring level is Service and polling is enabled)

Status	Description
Running	*The monitored host is fully functional and working normally*
Incomplete	*The monitoring PFM -RM service is only partially functional* This status appears in the following cases: • The Remote Monitor Collector service on the monitoring PFM - RM is in `Incomplete` status. • This status appears when the Remote Monitor Collector service on the monitoring PFM - RM is stopped#. If the Action Handler service is added as a monitored service, this status appears when the Remote Monitor Collector service is running but the Remote Monitor Store service or Action Handler service is stopped#.
Not supported	*The monitored host has not been polled.*
Unconfirmed	*The status of the monitored host cannot be confirmed* This status appears in the following cases: • This status appears when the health check function cannot communicate with the PFM - RM monitoring host. • This status appears when the health check function cannot communicate with the Status Server service on the PFM - RM monitoring host. This may be because the status management function is disabled. • The Remote Monitor Collector service for the monitoring PFM - RM is not running. • Polling of the monitored host failed.
Host Not Available	*The monitored host is stopped.*

#

A service is judged to have stopped when it has any status other than `Active` or `Busy`. However, you can configure the health check function to consider a service stopped if the `Busy` status persists for longer than the period of time that you specify in the properties of the health check agent.

The following table describes the operating statuses of the monitored host and PFM - RM services for each status.

Table 13-14: Health check status, PFM - RM service status and monitored host operating status

Status	PFM-RM host	Status Server	Remote Monitor Collector	Monitored host	Remote Monitor Store or Action Handler
Not Supported	Y	Y	Y or I	P	n/a
Running	Y	Y	Y	Y	Y or I
Incomplete	Y	Y	I	Y	n/a
	Y	Y	Y	Y	N
Unconfirmed	N	n/a	n/a	n/a	n/a
	Y	N	n/a	n/a	n/a
	Y	Y	N	n/a	n/a
	Y	Y	Y or I	C	n/a
Host Not Available	Y	Y	Y or I	N	n/a

Legend:

Y: The host or service is running.

I: The host or service is in `Incomplete` status.

P: Has not been polled.

C: Communication failed.

N: The host or service is stopped.

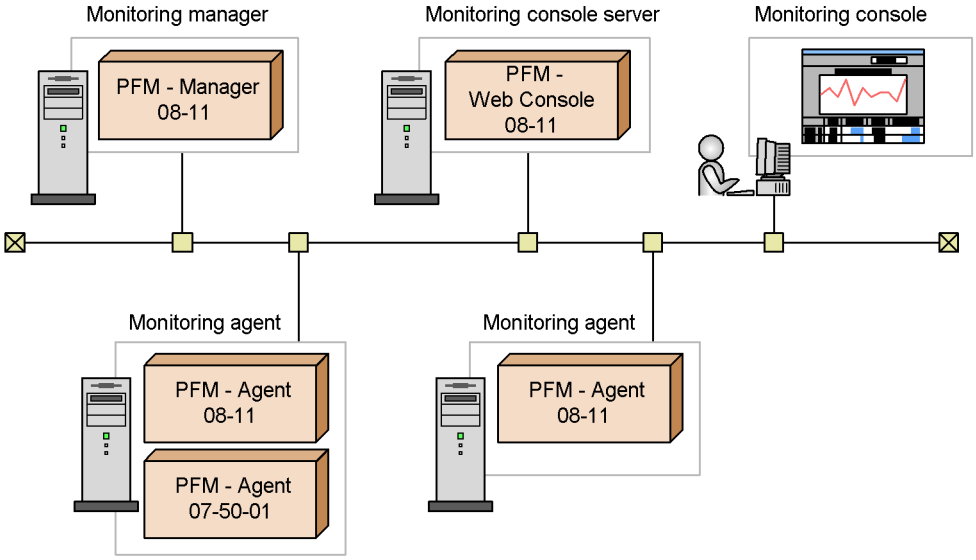
n/a: Has no bearing on status determination.

13.2.3 Examples of using the health check function

(1) When all instances of PFM - Agent or PFM - RM in the system meet the requirements for monitoring the operating status of services

The health check function can be used to its full potential by using a monitoring level that provides service-level monitoring of operating statuses, in a Performance Management system where all instances of PFM - Agent and PFM - RM meet the conditions that allow this monitoring level. The following figure shows an example of a system where all instances of PFM - Agent and PFM - RM meet the conditions under which the health check function can perform service-level monitoring of operating statuses.

Figure 13-3: Example of a system where all instances of PFM - Agent and PFM - RM meet the requirements for service-level monitoring of operating statuses



To use the health check function with service-level monitoring of operating statuses as the monitoring level:

1. Enable the health check function.

   Execute the `jpcconf hc enable` command on the PFM - Manager host.

2. Configure the health check function.

   Start PFM - Manager, and display the properties of the health check agent in PFM - Web Console. Set the monitoring level to **Service**, and set the other properties as required.

3. Start using the health check function.

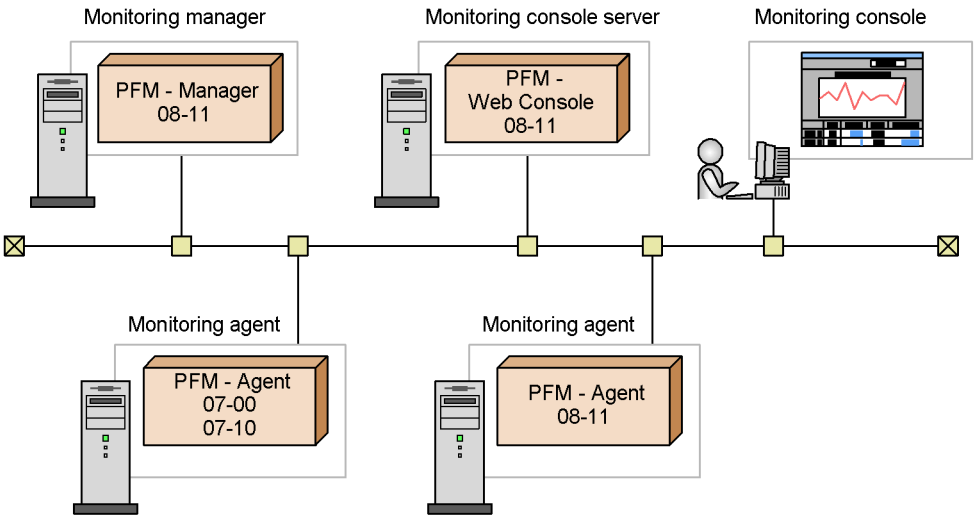
   In the Agents tree of PFM - Web Console, you can check the operating status of the services of each agent. You can also monitor the Event Monitor window or the Event History window for changes in the health check status. The status of each agent is derived from the results of the health check function checking the operating status of each of the agent's services. You can also view more detailed information about the health check status in the form of a report. Some health check reports are provided as monitoring templates. For details on the monitoring template of the health check function, see the overview of the monitoring template in the appendixes of *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

When the health check status of an agent is reported as abnormal, take action to resolve the problem such as restarting the agent.

(2) When not all instances of PFM - Agent or PFM - RM in the system meet the requirements for service-level monitoring

In a system where some instances of PFM - Agent or PFM - RM in the Performance Management system do not meet the conditions that allow service-level monitoring, you can monitor the status of the host instead by using the monitoring level that provides host-level monitoring of operating statuses. If you use the monitoring level that provides service-level monitoring, the operating status of the instances of PFM - Agent or PFM - RM that do not meet the conditions will not be accurate. Polling will also take longer than normal. The following figure shows an example of a system where some instances of PFM - Agent or PFM - RM do not meet the conditions under which the health check function can perform service-level monitoring of operating statuses.

Figure 13-4: Example of a system where not all instances of PFM - Agent or PFM - RM meet the requirements for service-level monitoring of operating statuses



To use the health check function with service-level monitoring of operating statuses as the monitoring level:

1. Enable the health check function.

   Execute the `jpcconf hc enable` command on the PFM - Manager host.

2. Configure the health check function.

   Start PFM - Manager, and display the properties of the health check agent in PFM - Web Console. Set the properties as required.

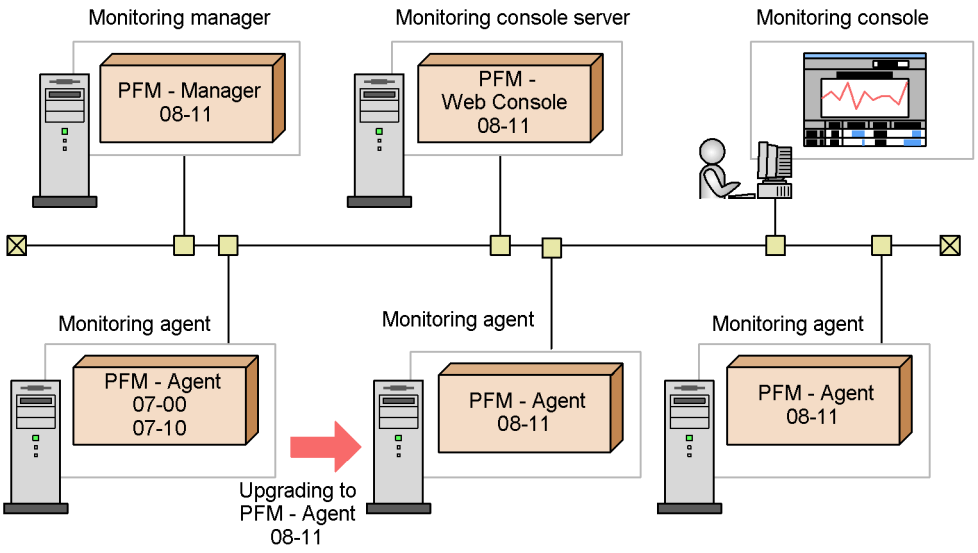
3. Start using the health check function.

   In the Agents tree of PFM - Web Console, you can check the operating status of the host for each agent. You can also monitor the Event Monitor window or the Event History window for changes in the health check status. The status of each agent is derived from the results of the health check function checking the status of the host. You can also view more detailed information about the health check status in the form of a report. Some health check reports are provided as monitoring templates. For details on the monitoring template of the health check function, see the overview of the monitoring template in the appendixes of *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

   When the health check status of an agent is reported as abnormal, take action to resolve the problem such as restarting the host.

   You can switch to service-level monitoring as soon as all instances of PFM - Agent or PFM - RM in the system support it. The following figure shows an example of switching from host-level monitoring to service-level monitoring.

   Figure 13-5: Switching from host-level monitoring to service-level monitoring



(3) When monitoring operating statuses by linking with JP1/IM

By linking with JP1/IM, you can be made aware of problems related to the operating status of Performance Management via the JP1/IM interface. Also, by displaying the reports that are associated with alarms, you can analyze and view detailed information about the operating status of Performance Management.

You can use alarms to notify JP1/IM of changes in the health check status. The monitoring template includes three alarms, each of which provides a different level of detail. Use the alarm that best suits your purpose. When linking with JP1/IM, copy the chosen alarm from the monitoring template and configure it to issue a JP1 event as an action. For details on how to do so, see *10. Linking with the Integrated Management Product JP1/IM for Operation Monitoring* .

(4) Using the health check function in a firewall or NAT environment

The health check agent must be able to communicate with the Status Server on each host running PFM - Agent or PFM - RM. For this reason, when you use the health check function in a firewall or NAT environment, the firewall or NAT must be set up so that the health check agent's traffic can be routed through the firewall or NAT. For details on the settings, see the description of firewall routing in the appendixes of the manual *Job Management Partner 1/Performance Management Reference*. The following table describes the port numbers used by the health check agent.

Table 13-15: Port numbers used by the health check agent

Service name	Parameter	Port number	Note
Agent Collector (health check agent)	`jp1pcagt0`	Automatic#	This port is used for such tasks as binding alarms and acquiring realtime reports.
Agent Store (health check agent)	`jp1pcsto0`	Automatic#	This port is used for such tasks as recording performance data and acquiring historical reports.

#: Each time the service restarts, it is automatically allocated a port number that is not already in use in the system.

A PFM - RM host uses the ICMP protocol to poll monitored hosts. To check the operating status of a PFM - RM monitored host, configure the firewall so that the PFM - RM host can communicate with the monitored host using the ICMP protocol. For details, see the appendixes of the appropriate PFM - RM manual.

(5) Using the health check function in a cluster system

You can use the health check function in the same manner as in a non-cluster system. The health check function must be set up on the host where PFM - Manager is installed. When you set up PFM - Manager version 09-00 or later in a logical host environment, the health check function settings are inherited from the physical host

environment. You must modify the settings of the health check function, if necessary. For details on how to configure the health check function for use in a cluster system, for Windows see *9.2.2 Installing and setting up PFM - Manager*, and for UNIX see *9.4.2 Installing and setting up PFM - Manager*.

13.3 Using the status management function to check service status

This section describes the status management function, which is used to check the status of Performance Management services when PFM - Manager is starting or stopping or if PFM - Manager stops due to a problem.

The version from which support for the status management function was added differs between agent types. The following table describes which versions of each agent type support the status management function.

Table 13-16: Support for the status management function by agent type

Agent	Supported in
PFM - Agent for Enterprise Applications	08-00 or later
PFM - Agent for JP1/AJS2	08-00 or later
PFM - Agent for Microsoft SQL Server	08-00 or later
PFM - Agent for Oracle	08-00 or later
PFM - Agent for Platform (UNIX) (for HP-UX, AIX, Solaris, and Linux(x86))	08-00 or later
PFM - Agent for Platform (UNIX) (for Linux(IPF))	08-00 or later
PFM - Agent for Platform (Windows)	08-00 or later
PFM - Agent for Service Response	08-00 or later
PFM - Agent for Virtual Machine	09-00 or later
All PFM - RMs	All versions

13.3.1 Configuring the status management function

(1) Setting up the status management function

The status management function is a function provided by PFM - Manager and PFM - Base.

The status management function is enabled by default if PFM - Base or PFM - Manager version 08-00 or later is newly installed. However, the setting prior to installation is used in the following cases:

- When PFM - Manager version 06-70 to 07-00 is upgraded to version 08-00 or later

- When a new installation of version 08-00 or later of PFM - Manager or PFM - Base is performed in an environment where version 06-70 to 07-00 of PFM - Agent is installed

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

The following describes how to enable and disable the status management function.

Note:

The Status Server service for the status management function is assigned a fixed port number by default.

(a) Enabling the status management function

To enable the status management:

1. Stop Performance Management services.

   If Performance Management services are running on a physical host, stop the services by using the following command:

   ```
   jpcspm stop -key jp1pc
   ```

   To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpcconf stat enable` command.

   To enable the status management function, use the following command:

   ```
   jpcconf stat enable
   ```

3. Check the status of the status management function.

   To confirm that the status of the status management function is `available`, use the following command:

   ```
   jpcconf stat display
   ```

4. Start Performance Management services.

   To start all Performance Management services on a physical host, use the following command:

   ```
   jpcspm start -key jp1pc
   ```

To start all of Performance Management's services on a logical host, use the cluster software.

(b) Disabling the status management function

To disable the status management function:

1. Stop Performance Management services.

   If Performance Management services are running on a physical host, stop the services by using the following command:

   ```
   jpcspm stop -key jp1pc
   ```

   To stop Performance Management services on a logical host, use the cluster software.

2. Execute the `jpcconf stat disable` command.

   To disable the status management function, use the following command:

   ```
   jpcconf stat disable
   ```

3. Check the status of the status management function.

   To confirm that the status of the status management function is `unavailable`, use the following command:

   ```
   jpcconf stat display
   ```

4. Start Performance Management services.

   To start all of Performance Management services on a physical host, use the following command:

   ```
   jpcspm start -key jp1pc
   ```

   To start all of Performance Management services on a logical host, use the cluster software.

Note:

The service key that can be specified by the `jpcspm start` and `jpcspm stop` commands differs depending on whether the status management function is enabled or disabled.

For details on each command, see the chapter describing the command in the manual

Job Management Partner 1/Performance Management Reference.

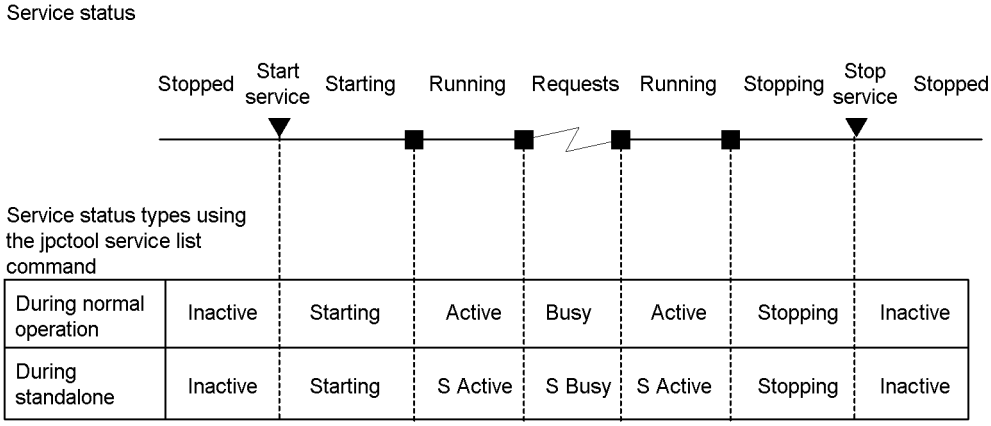
13.3.2 How to check the service status

The service status information that can be checked by the `jpctool service list` command differs depending on whether the status management function is enabled or disabled. The following subsections indicate the different situations in which service status information can be checked.

(1) When the status management function is enabled

If the status management function is enabled, the `jpctool service list` command can be used to check detailed status information while a service is running or stopped.

Figure 13-6: Status information if the status management function is enabled



During normal operation	Inactive	Starting	Active	Busy	Active	Stopping	Inactive
During standalone	Inactive	Starting	S Active	S Busy	S Active	Stopping	Inactive

The following figures show an example configuration when the status management function is enabled in PFM - Manager and PFM - Agent or PFM - RM and an example of output of the `jpctool service list` command.

Figure 13-7: Example of system configuration if the status management function is enabled

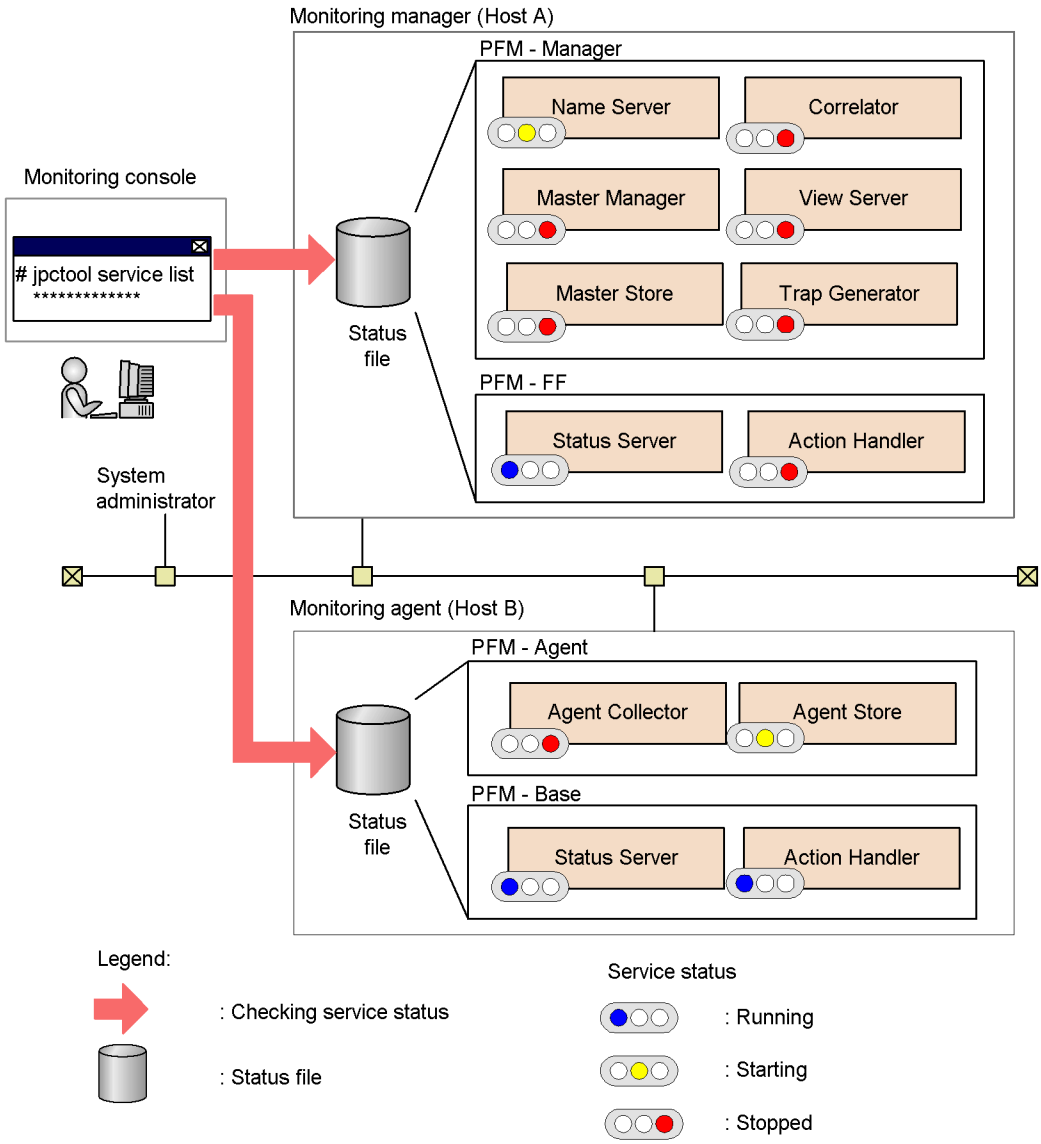


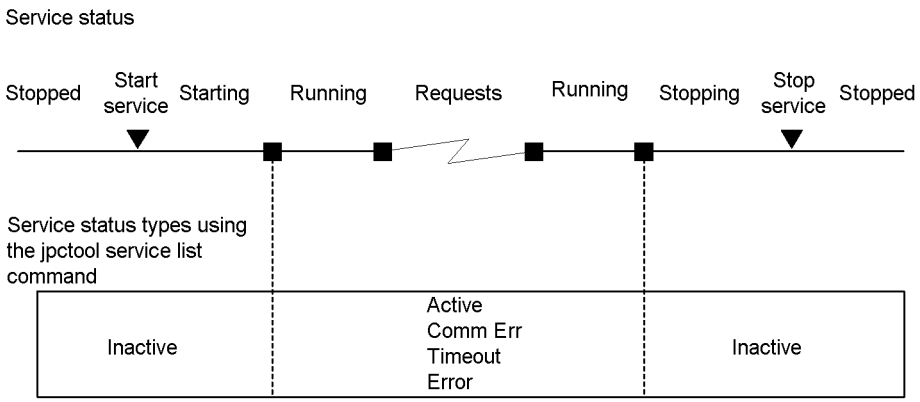
Figure 13-8: Example of output of the jpctool service list command

```
# jpctool service list * host=*
Host Name   ServiceID         Service Name      PID    Port     Status
---------   ---------         -------------     -----  -------- ---------

HOSTA       PT1HOSTA          Status Server      483    8206   Busy
HOSTA       PN1001            Name Server       6588           Starting
HOSTA       PM1001            Master Manager                   Inactive
HOSTA       PS1001            Master Store                     Inactive
HOSTA       PE1001            Correlator                       Inactive
HOSTA       PC3HOSTA          Trap Generator                   Inactive
HOSTA       PP1HOSTA          View Server                      Inactive
HOSTA       PH1HOSTA          Action Handler                   Inactive
HOSTB       PT1HOSTB          Status Server     9876   22291   Busy
HOSTB       PH1HOSTB          Action Handler     4872   1116   Active
HOSTB       OS1inst1[HOSTB]   Agent Store        4321           Starting
HOSTB       OA1inst1[HOSTB]   Agent Collector                   Inactive

KAVE06003-I List processing of the service information terminated normally.
```

(2) When the status management function is disabled

If the host has a version installed that does not support the status management function or if the function is disabled on the host, when the `jpctool service list` command is executed, a message is displayed explaining that the status management function is not supported. When this happens, the following status information is displayed. The service status cannot be checked, however, if PFM - Manager is not running.

Figure 13-9: Status information if the status management function is disabled



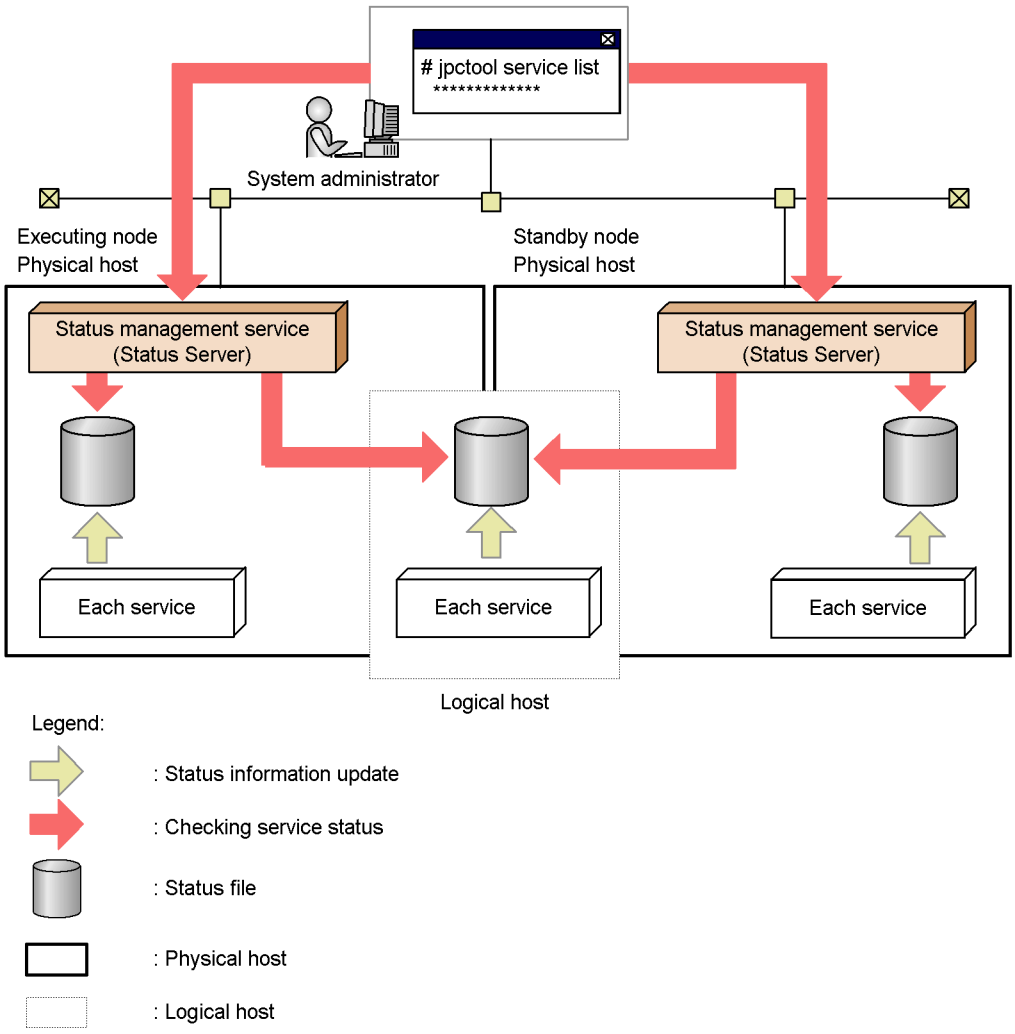
13.3.3 Status management during cluster system operation

Only one Status Server service is started per host. As a result, when the cluster system is running, the status of the services on the physical and logical hosts is managed by

the Status Server service on the physical host.

The following figure shows an overview of the status management function during cluster system operation:

Figure 13-10: Overview of the status management function when the cluster system is used



Note:

If the cluster system is in an active-active configuration, configure the Status Server service so that the service does not failover or so that the service always

starts up.

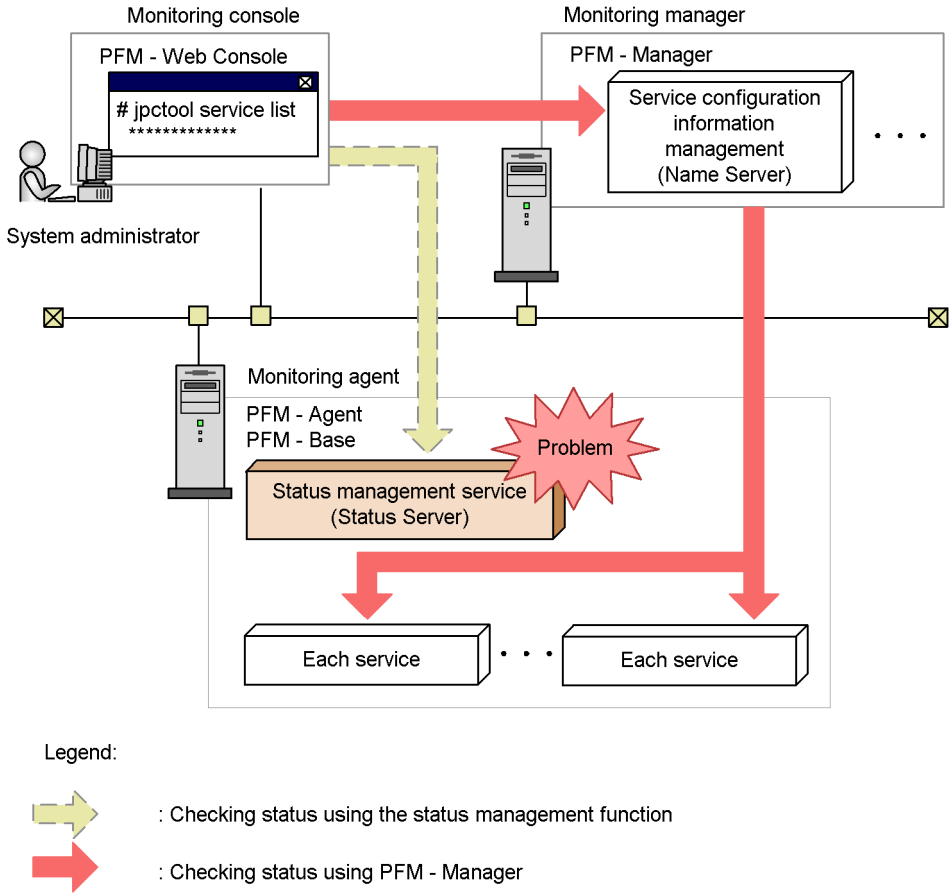
13.3.4 When a problem occurs within the status management function

This section gives details about checking the service status when a problem occurs within the status management function.

(1) When the Status Server service stops abnormally

When the Status Server service is stopped, the KAVE00203-W message is output to the common message log. In this case, the detailed service status cannot be checked, but the service status can be checked with the same method as when the status management function is disabled. The service status cannot be checked, however, when PFM - Manager is not running.

Figure 13-11: Example of when the Status Server service stops abnormally



(2) When a service other than the Status Server service stops abnormally

If a service other than the Status Server service stops abnormally, the status file contents might not be properly updated. In this case, the status management function determines the service status based on the internal file generated by each service. As a result, the service status can be checked in the same manner as when the status management function is enabled.

13.4 Using the PFM service automatic restart functionality to restart PFM services

This section describes the PFM service automatic restart functionality, which is used to automatically restart PFM services that have stopped abnormally.

Performance Management provides the PFM service automatic restart functionality, which you can use you to automatically restart a PFM service in the unlikely event that it stops abnormally for some reason. The PFM service automatic restart functionality has the following two functionalities:

Automatic restart functionality

If a PFM service stops abnormally for some reason, the PFM service automatic restart functionality restarts the PFM service so that it continues monitoring. If you are not using a cluster system, which provides high system availability, we recommend that you consider using this functionality.

Scheduled restart functionality

The scheduled restart functionality allows you to schedule the restart of a PFM service so that it continues monitoring even if there is a problem with the OS or the service itself (such as a memory or handle leak) that prevents the service from running for an extended period of time. This functionality is typically not used.

13.4.1 Prerequisite conditions

You must install version 09-00 or later of PFM - Base or PFM - Manager on the host and enable the status management function. For PFM-RM, any version of the program can be used. To restart PFM - Agent services, the PFM - Agent version must be 08-00 or later. PFM - Agent and Action Handler services that meet these prerequisite conditions can be automatically restarted even if PFM - Agent services that do not meet these conditions exist on the host. The following table describes possible product combinations on the same host and support for automatic service restart for each PFM service.

Table 13-17: Possible product combinations on the same host and support for automatic service restart

PFM - Manager or PFM - Base version	Whether automatic restart of the service is available								
	PFM - Agent 08-00 or later, or PFM - RM			Earlier version than PFM - Agent 08-00			No PFM - Agent		
	M	A	AH	M	A	AH	M	A	AH
PFM - Manager 09-00 or later	Y	Y	Y	Y	N	Y	Y	n/a	Y
Earlier version than PFM - Manager 09-00	N	N	N	N	N	N	N	n/a	N
PFM - Base 09-00 or later	n/a	Y	Y	n/a	N	N	n/a	n/a	N
Earlier version than PFM - Base 09-00	n/a	N	N	n/a	N	N	n/a	n/a	N
None	n/a	n/a	n/a	n/a	N	N	n/a	n/a	n/a

Legend:

M: PFM - Manager service

A: PFM - Agent service

AH: Action Handler service

Y: Available

N: Not available

n/a: Not applicable or impossible combination

13.4.2 Service startup unit for the PFM service automatic restart functionality

The service startup unit for the PFM service automatic restart functionality is the minimum unit that can be specified in the `jpcspm start` command. The following table lists the service startup units of the PFM service automatic restart functionality.

Table 13-18: Service startup unit for the PFM service automatic restart functionality

Service	Service startup unit
PFM - Manager service	• Name Server service • Master Manager service • Master Store service • Correlator service • Trap Generator service • View Server service
PFM - Agent service	• Agent Collector service • Agent Store service However, for a multi-instance agent, the instances can be started individually. For a health check agent, the PFM - Manager services are started as well.
PFM - RM service	• Remote Monitor Collector service • Remote Monitor Store service
Action Handler service	Action Handler service

13.4.3 Configuring the PFM service automatic restart functionality

In the **Services** tree of PFM - Web Console, you can specify the property to configure the PFM service automatic restart functionality for each service. For a health check agent, use the Agent Collector service to set the automatic restart functionality for the agent. If a service does not meet any of the above prerequisite conditions, the property for this setting is not displayed. The following table lists the properties to be set for each target service.

Table 13-19: Correspondence between the service names targeted for automatic restart and the service names to be used for setting the service properties

Supported service	Use this for setting the service property
PFM - Manager service • Name Server • Master Manager • Master Store • Correlator • Trap Generator • View Server	Master Manager
PFM - Agent service • Agent Collector • Agent Store	Agent Collector

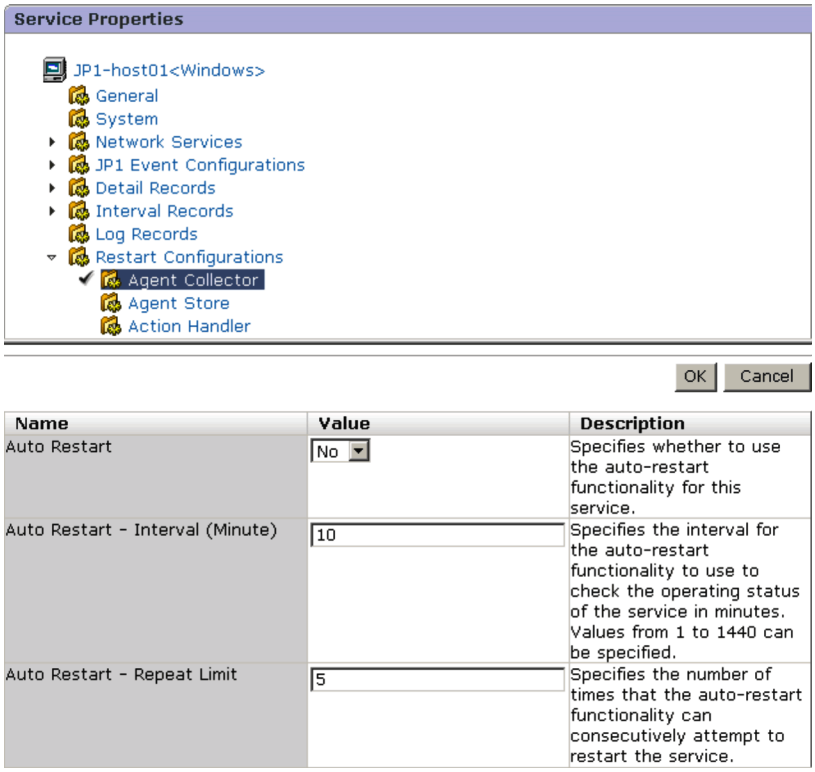
Supported service	Use this for setting the service property
PFM - RM service • Remote Monitor Collector • Remote Monitor Store	Remote Monitor Collector
Action Handler service • Action Handler	Master Manager, Agent Collector, and Remote Monitor Collector#

#: The property settings for each of these services are shared across the same host, regardless of which program is used to make the property settings.

If there are multiple instances of PFM - Agent or PFM - RM that are of the same type and that use the same data model, you can distribute the property settings to these multiple hosts.

The following figure shows an example display of properties of the Agent Collector service.

Figure 13-12: Example display of properties of the Agent Collector service



The following table lists the setting items for each target service.

Table 13-20: Setting items for the service automatic restart functionality

Folder name	Property name	Description
Restart Configurations	Restart when Abnormal Status[#1]	Specifies whether the service is to be restarted when the automatic restart functionality detects an `Abnormal Status`[#2]. This setting is applied to all services on the host. The default is `Yes`. `Yes`: Restarts `No`: Does not restart
	Restart when Single Service Running[#1]	Specifies whether the service is to be restarted when the automatic restart functionality detects a `Single Service Running`[#3]. This setting is applied to all services on the host. The default is `No`. `Yes`: Restarts `No`: Does not restart
Service-name[#4]	Auto Restart	Specifies whether to use the automatic restart functionality for the target service. The default is `No`. `Yes`: Uses the automatic restart functionality. `No`: Does not use the automatic restart functionality.
	Auto Restart - Interval(Minute)	Specifies, in minutes, how often the automatic restart functionality checks the operating status when the function is used. You can specify an integer value from 1 to 1440. The default is 10 (minutes).
	Auto Restart - Repeat Limit	Specifies how many times the automatic restart functionality attempts to restart the service when the functionality is used. You can specify an integer value from 1 to 10. The default is 5 (times).
	Scheduled Restart	Specifies whether to use the scheduled restart functionality for the service. The default is `No`. `Yes`: Uses the scheduled restart functionality. `No`: Does not use the scheduled restart functionality.
	Scheduled Restart - Interval	Specify an integer value from 1 to 1,000 for the interval between restarts when you use the scheduled restart functionality. The default is 1. The units for the interval are specified in the Scheduled Restart - Interval Unit.

Folder name	Property name	Description
	Scheduled Restart - Interval Unit	Specifies the restart interval units (Month/Week/Day/Hour) used by the scheduled restart functionality for restarting the service when the functionality is used. The default is Month. Month Week Day Hour
	Scheduled Restart - Origin - Year	Specifies the calendar year from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 1971 to 2035[#5]. The default is the current year[#6].
	Scheduled Restart - Origin - Month	Specifies the month of the year from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 1 to 12[#5]. The default is the current month[#6].
	Scheduled Restart - Origin - Day	Specifies the day of the month from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 1 to 31[#5]. The default is the current date[#6].
	Scheduled Restart - Origin - Hour	Specifies the hour of the day from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 0 to 23. The default is the current hour[#6].
	Scheduled Restart - Origin - Minute	Specifies the minute of the hour from which the scheduled restart functionality initiates the restart interval when the functionality is used. You can specify an integer value from 0 to 59. The default value is the current minute[#6].

#1: The property settings for each of these services are shared across the same host, regardless of which program is used to make the property settings.

#2: Indicates that the Status Server cannot obtain the status of the PFM service normally (for example, because the PFM service has ended abnormally due to an exception).

#3: Indicates that only one of the PFM - Agent or PFM - RM services is running.

#4: The Master Manager services shown are the PFM - Manager and Action Handler services. The Agent Collector or Remote Monitor Collector services shown are the PFM - Agent or PFM - RM and Action Handler services.

#5: If a non-existing date (such as 2007/2/30) is specified, the last day of the month is assumed.

#6: The date and time displayed for the property is based on the time zone setting of the host running the service.

Note:

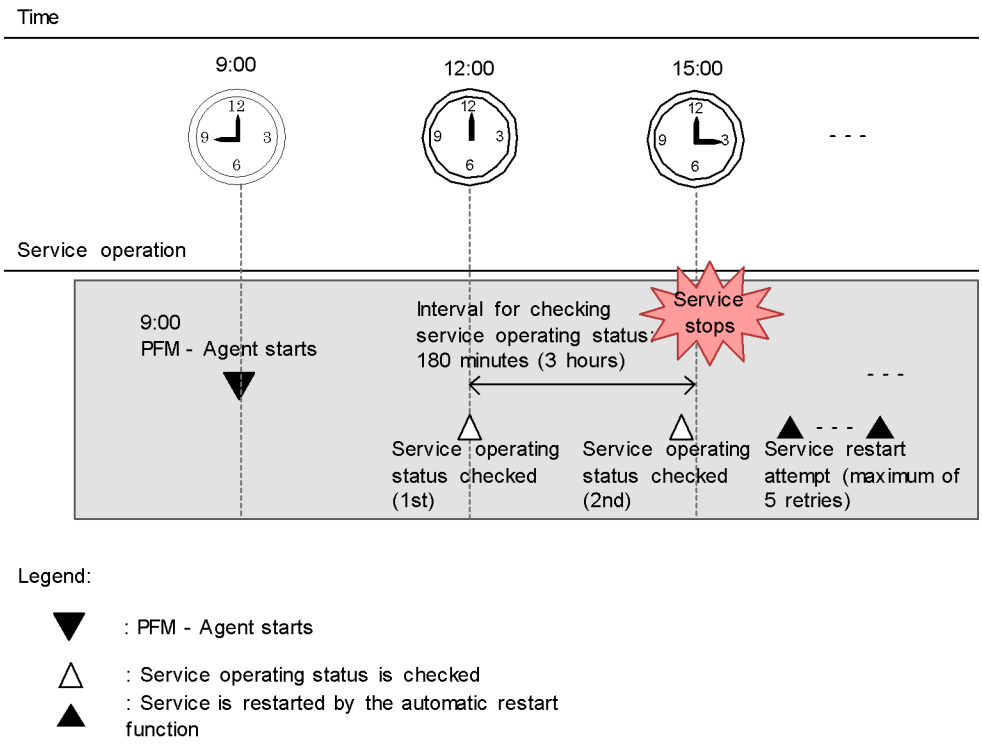
Placing priority on continued monitoring, the PFM service automatic restart functionality restarts only specific services. The PFM - Manager services link with each other at a high level, so if only particular services are restarted, some of these links may fail. If you use the scheduled restart functionality for a PFM - Manager service, you should also set any PFM - Manager services that usually start after that service to restart. Adjust the restart time so that the services are restarted in the correct order. For details on the start sequence for PFM - Manager services, see *1.1.1 Start sequence for the entire Performance Management system*. If you use the automatic restart functionality for a PFM - Manager service, after you restart the service you should select a time when there will be the least impact on system operation and stop all PFM - Manager services, and then restart them. To realize high availability of the PFM - Manager services, we recommend you use a cluster system.

13.4.4 Using the PFM service automatic restart functionality

(1) Automatic restart functionality

The following figure shows an example of operating a system by using the automatic restart functionality. In this example, the automatic restart functionality checks the operating status of the Agent Collector service every three hours, and if the service stops, it restarts the service.

Figure 13-13: Example of using the automatic restart functionality



Restart Configurations settings

Restart when Abnormal Status: Yes (default)

Agent Collector service settings

Auto Restart: Yes

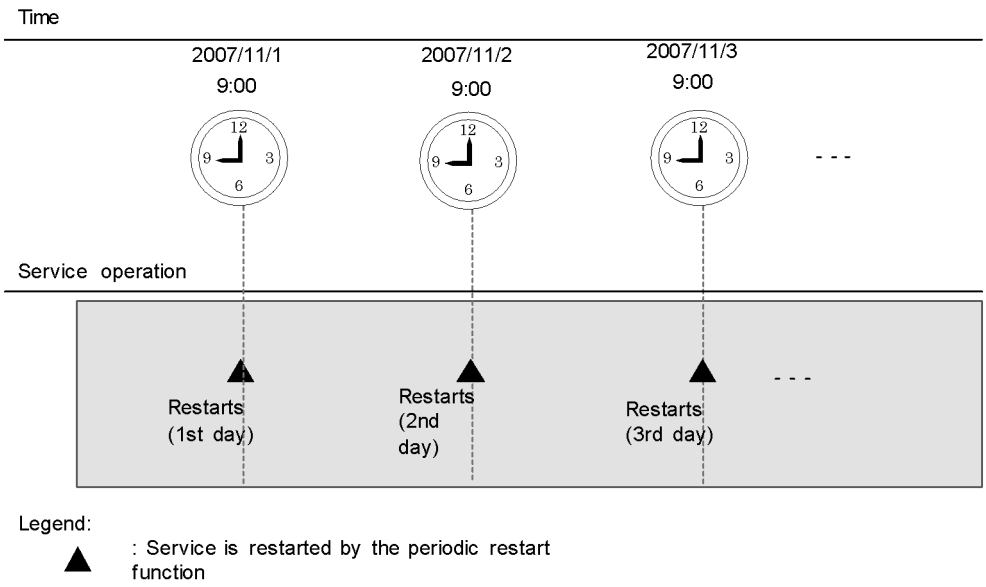
Auto Restart - Interval (minute): 180

Auto Restart - Interval (minute): 5 (default)

(2) Scheduled restart functionality

The following figure shows an example of operating a system by using the scheduled restart functionality. In this example, a PFM - Agent service is restarted at 9:00 every day.

Figure 13-14: Example of using the scheduled restart functionality



Agent Collector service settings

Scheduled Restart: Yes

Scheduled Restart - Interval: 1 (default)

Scheduled Restart - Interval Unit: Day

Scheduled Restart - Origin - Year: 2007 (year)

Scheduled Restart - Origin - Month: 11 (month)

Scheduled Restart - Origin - Day: 1 (day)

Scheduled Restart - Origin - Hour: 9 (hour)

Scheduled Restart - Origin - Day: 0 (minute)

13.5 Detecting problems by linking with the integrated system monitoring product

The JP1/Base log file trapping function can be used to change the contents of Performance Management's common message log to JP1 events. Therefore, when a problem occurs within Performance Management, the problem can be detected with JP1/IM by issuing a JP1 event.

However, to detect problems other than those that occur within Performance Management, we recommend that you use the health check function. For details on the health check function, see *13.2 Using the health check function to check the operating status of monitoring agents and their hosts*.

The following subsections describe the steps to link Performance Management with the JP1/Base log file trapping function and issue a JP1 event.

13.5.1 Configuring the log output method

In order to link with the JP1/Base log file trapping function, the output method of Performance Management's common message log must be configured.

The following table shows the log file output methods Performance Management supports:

Table 13-21: Log file output format supported by Performance Management

Log file output method	Description	Output log file name
Sequential file method	This method always writes the newest log information to a file called `jpclog01`. When the log file size reaches the set value, `jpclog01` is renamed and saved as `jpclog02`, the contents of `jpclog01` are cleared, and the newest log information is written.	*installation-folder*`\log\jpclog{01|02}`
Wrap-around file method	When the log file size reaches the set value, the next log file contents are cleared, and the newest log information is written in the next log file. The file to be written to changes in the following manner: the file after `jpclogw01` is `jpclogw02` and the file after `jpclogw02` is `jpclogw01`.	*installation-folder*`\log\jpclogw{01|02}`

Note:

- With the wrap-around file method, the time of the most recent update for the log file is used to determine the newest log information. Therefore, an error might occur if the time is changed on the host on which Performance Management is running or if the most recent update time for the log file is modified.
- Because versions earlier than 08-00 do not support the wrap-around file method, the log is output using the sequential file method even if the wrap-around file method is specified for the common message log's output method. In this case, versions earlier than 08-00 output the log to `jpclog` and versions 08-00 and later output the log to `jpclogw`.
- The sequential file method used is SEQ2 and the wrap-around file method used is WRAP2.

To configure the log output method:

1. Stop all Performance Management services on the host on which the log output method is to be changed.
2. Open the file `jpccomm.ini` with a program such as a text editor.
3. Change the log file trapping method of the common message log.

   Correct the shaded part indicated below:

```
:
[Common Section]
Commom Msglog Type=0|1
:
```

Table 13-22: Items to edit in the file jpccomm.ini

Section	Label	Values	Default value	Description
`[Common Section]`	`Common Msglog Type`	`0|1`	`0`	Log file output method for the common message log. • `0`: Sequential file method • `1`: Wrap-around file method

Note the following when editing the file `jpccomm.ini`:

- Do not enter a space at the beginning of a line or before or after an equal sign.

- The file `jpccomm.ini` contains definition information in addition to the common message log file size. Do not change any values other than `Common Msglog Type` in the section `Common Section`. Performance Management might not run properly if values other than that for the required item are changed.

4. Save, and then close the file `jpccomm.ini`.
5. Start Performance Management services.

Notes:

- The settings for the common message log file are shared by the Performance Management programs on the same host.
- Backup the file `jpccomm.ini` as necessary.
- To restore the settings for the file `jpccomm.ini` to the default settings, copy the file `jpccomm.ini.model`, which is in the same folder, to `jpccomm.ini`.

13.5.2 Example of creating a definition file for the JP1/Base log file trapping function

Use the JP1/Base log file trapping function to create an action definition file for issuing JP1 events.

For example, if the message `KAVE00116-E` is output to the common message log with the wrap-around method (WRAP2), the action definition file for issuing a JP1 event with a severity of `Abnormal` and event ID of `999` is described below.

Figure 13-15: Example of configuring the JP1/Base action definition file

```
:
FILETYPE=WRAP2
HEADLINE=0
RECTYPE=VAR '\n'
ACTDEF=<Error>999 "KAVE00116-E"
:
```

For details on the JP1/Base action definition file, see *Job Management Partner 1/Base User's Guide*.

13.5.3 Starting the JP1/Base log file trapping function

Execute the following commands to start the JP1/Base log file trapping function:

- For Windows:
  jp1/base-installation-directory\bin\jevlogstart -r -f *action-definition-file-name performance-management-installation-directory*\log\jpclogw01 *performance-management-installation-directory*\log\jpclogw02

- For UNIX:
  jp1/base-installation-directory/bin/jevlogstart -r -f *action-definition-file-name performance-management-installation-directory*/log/jpclogw01 *performance-management-installation-directory*/log/jpclogw02

For details on the JP1/Base log file trapping function, see *Job Management Partner 1/Base User's Guide*.

Chapter
14. Error Handling Procedures

This chapter explains how to handle any errors that might occur while you are using Performance Management.

14.1 Error handling procedures
14.2 Troubleshooting
14.3 Log information
14.4 Data to be collected in the event of trouble
14.5 Data collection procedure
14.6 Restoring the Performance Management system

14.1 Error handling procedures

This section describes how to handle errors that might occur while you are using Performance Management.

Checking the event

Check the following:

- Context in which the problem occurred
- Content of the message (when a message is output)
- Common message logs and other log information

For details on the messages and how to respond to each message, see the chapter that describe the messages in the manual *Job Management Partner 1/ Performance Management Reference*. For details on the log information output by Performance Management, see *14.3 Log information*.

Data to be collected

Collect data to determine the cause of an error. For details on collecting the necessary data, see *14.4 Data to be collected in the event of trouble* and *14.5 Data collection procedure*.

Determining the cause

Use the collected data to determine the cause and the extent of the error, as well as the range of its consequences.

14.2 Troubleshooting

This section describes how to conduct troubleshooting while you are using Performance Management. If an error occurs while you are using Performance Management, you should first check to see if any of the events described in this section have occurred.

The following table lists and describes the principal errors that might occur while you are using Performance Management.

Table 14-1: Errors

Classification	Error	Reference
Setting up and starting service	• A Performance Management program service does not start. • A service takes a long time to start once startup is requested. • Immediately after a Performance Management program service is stopped, another program starts service and communication is not performed properly. • After the message `The disk capacity is insufficient` is output, the Master Store service, Agent Store service, or Remote Monitor Store service stops.	*14.2.1*
Connecting to agents	An error message, such as `Cannot connect to an agent` is output to PFM - Web Console.	*14.2.2*
Logging on to PFM - Web Console	• The specified Performance Management user name is not recognized during logon. • Cannot establish a connection from PFM - Web Console to the View Server service.	*14.2.3*
Executing commands	• When the `jpctool service list` command is executed, the names of services not operating are output. • When the `jpctool db dump` command is executed, the output data does not match the data in the specified Store database.	*14.2.4*
Agent management	• No agent is displayed in the Agents window of PFM - Web Console. • The operating status of the server or agent is `Unconfirmed` or `Not Supported`.	*14.2.5*

Classification	Error	Reference
Report definition	• There is a time period not indicated on the history report. • A memory shortage can occur with the View Server service when a large number of reports are displayed simultaneously.	*14.2.6*
Alarm definition	• The program defined to be executed by an action does not work properly. • No alarm event is displayed.	*14.2.7*
Collecting and managing performance data	• Even if the data storage time is set for a shorter period, the size of the Store database for the Agent Store service and the Remote Monitor Store service does not become smaller. • The message `Illegal data was detected in the Store database.` is output to the common message log.	*14.2.8*
Linking with other programs	• A server request error occurs and no connection is established when linking with an ODBC-compliant program. • A status change event is not displayed in the event browser when linking with NNM. • No symbol appears in ovw when linking with NNM. • JP1 events are not reported when linking with JP1/IM. • Monitored PFM - Agent or PFM - RM is not displayed in the monitoring tree window when linking with a monitored object function of JP1/IM. • The display color of the monitored object does not change when linking with a monitored object function of JP1/IM.	*14.2.9*

14.2.1 Setting up and starting a service

This subsection describes how to handle errors related to setup or service startup.

(1) A Performance Management program service does not start.

Possible causes and solutions:

- PFM - Manager stopped

  If PFM - Manager and PFM - Agent or PFM - RM are installed on the same host, the PFM - Agent or PFM - RM service cannot start when PFM - Manager is stopped. Determine whether the PFM - Manager service has started. If the PFM - Manager service has not started, start the service. For details on service startup,

see *1. Starting and Stopping Performance Management*.

- The same port number is set for multiple Performance Management program services.

  When the same port number is set for multiple Performance Management program services, none of the Performance Management program services can start. Since port numbers are allocated automatically by default, they cannot be duplicated. When port numbers for Performance Management program services are fixed during Performance Management setup, check the port number settings. If the same port number is set for more than one Performance Management program service, you must make appropriate corrections in the port number settings. For details on how to set a port number, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- There is an error in a setting for a Store database installation directory.

  If any of the following directories are set to a directory that cannot be accessed or a directory that does not exist, the Agent Store or Remote Monitor Store service cannot start. Review the directory name and attributes, and correct the settings if necessary.

  - Store database installation directory
  - Store database backup directory
  - Store database partial backup directory
  - Store database export directory
  - Store database import directory

  In addition, if one of these directories is set for multiple Agent Store or Remote Monitor Store services, the Agent Store or Remote Monitor Store service cannot start. Review the directory settings and correct the settings if necessary.

- The host name of the machine was changed using a non-permitted procedure.

  For details on how to change the host name of the machine, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. Under some circumstances when the host name is changed using a procedure other than those permitted, a Performance Management program service might not start. This is the reason why the following issues might occur.

  - If you execute the `jpctool service list -id * -host *` command on a host where the service has not started, a service with a duplicate service ID will appear in the *Service Name* column.

  For details on the `jpctool service list` command, see the chapters that

describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

- When you stopped the PFM - Agent and changed the PFM - Agent host name while the PFM - Agent was not connect to PFM - Manager.

  Each Performance Management service registers its own service information (IP address, host name, and port number) in PFM - Manager when it is starting and deletes the information when it is stopping. If a service is not able to delete its service information when it was stopping because it could not communicate with PFM - Manager for some reason, the service information remains on the PFM - Manager side. Then, if the service tries to start using the same service information it used the previous time it started, the attempt will fail. This is because Performance Management does not allow a duplicate service instance to be started. (`KAVE00133-E` is output to the common message log on the host where the attempt to start the service failed.) In such a case, perform the following procedure to change the service information:

  1. Execute the `jpcconf port define` command to unlock the PFM - Agent port (if it is locked).
  2. Restart the PFM - Agent service.
  3. Execute the `jpcconf port define` command again to relock the PFM - Agent port (if necessary).

  For details on the `jpcconf port define` command, see the chapters that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

- A previously started process still exists.

  If a previously started process still exists, the service of the process cannot be started, because Performance Management does not allow a duplicate service instance to be started. Use Task Manager (for Windows) or the `ps` command (for UNIX) to check whether a process exists for a service that could not start successfully. If such a process exists, terminate it.

- An error has occurred in the service control manager.

  When the `jpcspm start` command is executed in Windows, the `KAVE05163-E` message is output and the service might not start. If this occurs, re-execute the `jpcspm start` command. If the same problem frequently occurs, edit the `jpccomm.ini` file and change the retry interval and the number of retries of the service startup processing performed when executing the `jpcspm start` command. For details on changing the retry interval and the number of retries, see *1.8.3 Starting on a Windows machine*.

(2) A service takes a long time for to start once startup is requested.

It might take a long time for service to actually start once you execute the `jpcspm start` command or start a service by choosing the Services icon. If the following factors are the reason for this, subsequent service startups should take less time.

- Starting a service in standalone mode might slow down the startup of the service.
- During initial startup after the Store database is restored, the indexes of the Store database must be rebuilt. This might slow startup of the service.
- During initial startup after an Agent is newly added, the indexes of the Store database must be created. This might slow startup of the service.
- If normal end processing for the Store service cannot be performed due to a power interruption or other reason, the indexes of the Store database are rebuilt at restart; therefore, it might take a long time for the Store service to start.

(3) Immediately after a Performance Management program service is stopped, another program starts service and communication is not performed properly.

Immediately after stopping a Performance Management program service, another program service might start that uses the same port that the stopped service was using. In this case, communication might not be performed properly. You can use either of the following techniques to avoid this problem:

- Fix the port numbers to be allocated to the Performance Management program services.

  Allocate a fixed port number to each Performance Management program service. For details on how to set a port number, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- Set the `TCP_TIMEWAIT` value.

  Use the `TCP_TIMEWAIT` value to set a connection wait time.

  For HP-UX or AIX, specify a connection wait time of at least 75 seconds, as follows:

  - In HP-UX: `tcp_time_wait_interval:240000`
  - In AIX: `tcp_timewait:5`

  In Windows or Solaris, use the default connection wait time setting. The default settings are:

  - In Solaris: 4 minutes
  - In Windows Server 2003, Windows Server 2008: 2 minutes

  In Linux, you cannot change the connection wait time setting from the default of

60 seconds. If this problem occurs in Linux, use the technique to fix the port numbers of the Performance Management program services.

(4) After the message "The disk capacity is insufficient" is output, the Master Store service or Agent Store service stops.

If there is insufficient space on the disk used by the Store database, the storing of data to the Store database is cancelled. In this case, after the message `The disk capacity is insufficient` is output, the Master Store service, Agent Store service, or Remote Monitor Store service stops.

If this message appears, use either of the following techniques to solve this problem.

- Allocate sufficient disk space.

  Estimate the disk usage of the Store database and change the storage location of the Store database to a disk with sufficient space. For details on how to estimate the disk usage of the Store database, see the system requirements in an appendix of each PFM - Agent or PFM - RM manual.

  For details on how to change the storage location of the Store database for event data, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*. For details on how to change the storage location of performance data, see each PFM - Agent or PFM - RM manual.

- Modify the data retention conditions of the Store database.

  Modify the data retention conditions of the Store database and adjust the upper limit for the amount of data in the Store database. For details on how to change the retention conditions of the Store database, see *4.1.2 Modifying the retention conditions for performance data (in Store 2.0)*, *4.1.3 Modifying the retention conditions for performance data (in Store 1.0)*, or *4.2.1 Changing the maximum number of records for event data*.

If the Master Store service, the Agent Store service, or the Remote Monitor Store service does not start even after taking these actions, there may be some unrecoverable logical errors in the Store database. In this case, you must restore the Store database from the backup data, and then restart the Master Store service, the Agent Store service, or the Remote Monitor Store service. If you have no backup data, you must initialize the Store database, and then start the Master Store service, the Agent Store service, or the Remote Monitor Store service. To initialize the Store database, delete all of the following files in the installation directories of the Store database:

- Files with the extension `.DB`
- Files with the extension `.IDX`

The following shows the default installation directories of the Store database.

Store database installation directory for performance data:

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

Store database installation directory for event data:

- In Windows:

  installation-folder\mgr\store

- In UNIX:

  /opt/jp1pc/mgr/store/

14.2.2 Connecting to agents

If an error such as Cannot connect to an agent is output on PFM - Web Console, check the following:

1. From the PFM - Manager host, execute ping *PFM-Agent-host* to check the following:

   - Whether it is possible to communicate with the PFM - Agent host
   - If it is possible to communicate, whether the IP address matches that used by the PFM - Agent or PFM RM host
   - If the jpchosts or hosts file is used, whether the IP address is correctly set in the file on PFM - Manager and PFM - Agent or PFM - RM hosts

   Performance Management performs name resolution in the order of jpchosts, hosts, and DNS.

2. From the PFM - Agent or PFM - RM host, execute ping *PFM-Manager-host* to check the following:

   - Whether it is possible to communicate with the PFM - Manager host
   - If it is possible to communicate, whether the IP address matches the address used by the PFM - Manager host
   - If the jpchosts or hosts file is used, whether the IP address is correctly set in the file on the PFM - Manager and PFM - Agent or PFM - RM hosts

   Performance Management performs name resolution in the order of jpchosts, hosts, and DNS.

3. If there is a firewall between PFM - Manager and PFM - Agent or PFM - RM, whether the ports used by PFM - Manager and PFM - Agent or PFM - RM are locked and whether the system is configured to allow communication through the firewall.

   For details on firewall routing, see the manual *Job Management Partner 1/ Performance Management Reference*.

4. If jpctool service list -id * -host * is executed on the PFM - Manager

host, whether the information that existed before the host name was changed is displayed

If it is displayed, execute the `jpctool service delete` command on the PFM - Manager host to delete the information.

14.2.3 Logging on to PFM - Web Console

This subsection describes how to handle errors related to logging on to PFM - Web Console.

(1) The specified Performance Management user name is not recognized during logon.

A specified Performance Management user account might not exist. Use the user name `ADMINISTRATOR` to log on to PFM - Web Console from the monitoring console, and then use the Users window to confirm whether a Performance Management user account has been created. If no Performance Management user account has been created, create one now. For details on how to create a Performance Management user account, see *2. Managing User Accounts*.

(2) A connection from PFM - Web Console to the View Server service cannot be established.

Possible causes and solutions:

- There is an error in the host name or port number specified in the Windows initialization file (`config.xml`).

  Confirm whether the host name and port number are correct. Correct any incorrect settings, restart PFM - Web Console, and then re-execute the operation.

- The View Server service has not been initialized.

  The services or processes required to start the View Server service might not have been started. Wait a moment and then re-execute the operation.

- The PFM - Manager host is using an IP address that does not enable a connection from the PFM - Web Console host.

  When multiple IP addresses are set for the PFM - Manager host or an IP address translation (such as NAT) is performed between PFM - Manager and PFM - Web Console, a connection might not be established. In this case, the host name must be for with PFM - Manager. For details on how to set host names, see the list of port numbers in an appendix of the manual *Job Management Partner 1/ Performance Management Reference*.

- PFM - Web Console is connected to a PFM - Manager that has a function enabled on it that PFM - Web Console does not support.

  If the version of the connected PFM - Manager is newer than that of PFM - Web

Console, check that there are no functions enabled on the PFM - Manager that are not supported by PFM - Web Console.

If such a function is enabled, disable the function or consider upgrading the PFM - Web Consoler to a newer version.

The following table lists the corresponding functionality and PFM - Web Console versions that support the functionality.

Functionality	Supported in
Functionality for binding multiple alarm tables	PFM - Web Console 09-00 or later

14.2.4 Executing commands

This subsection describes how to handle errors related to executing Performance Management commands.

(1) When the jpctool service list command is executed, the names of services that are not operating are output.

Possible causes and solutions:

- A Performance Management program was uninstalled without its service information being deleted.

  Service information for a Performance Management program remains in the database even after the program is uninstalled. Execute the `jpctool service delete` command to delete the service information. For details on the `jpctool service delete` command, see the chapter that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

- The host name was changed without deleting the service information for a Performance Management program.

  If the host name is changed without deleting the service information for a Performance Management program, the service information for the service ID with the previous host name added remains in the database managed by the Master Manager service. Execute the `jpctool service delete` command to delete the service information. For details on the `jpctool service delete` command, see the chapter that describe commands in the manual *Job Management Partner 1/Performance Management Reference*. For details on how to change the host name, 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, the output data does not match the data in the specified Store database

Specifying the same export file name for the same Store service in multiple executions

of the `jpctool db dump` command causes the initial output results to be overwritten with the subsequent output results. Each time you execute the `jpctool db dump` command for the same Store service, specify a different export file name. For details on the `jpctool db dump` command, see the chapter that describe commands in the manual *Job Management Partner 1/Performance Management Reference*.

14.2.5 Agent management

This subsection describes how to handle errors related to Performance Management agent management.

(1) No agent is displayed in the Agents window of PFM - Web Console.

Agents to be monitored might not be defined. Use PFM - Web Console to define the agents to be monitored. For details on defining agents, see *3. Monitoring Agents*.

(2) The operating status of a server or agent is Unconfirmed or Not Supported

If a PFM - Web Console Summary View reports the operating status of a server or agent as `Unconfirmed` or `Not Supported`, select the appropriate action to take according to the procedure described below.

Before taking the action, check the operating status of each agent displayed in the navigation frame of the Agents window to identify which agent has an operating status of `Unconfirmed` or `Not Supported`.

The following table lists the locations to check for taking actions for each operation status.

Table 14-2: Locations to check for each operating status

Agent type	Operating status	Window type	
		Server Operational Status window	Agent Operational Status window
PFM - Agent or Remote Monitor Collector service	Unconfirmed	N/A	See *(a)*.
	Not Supported	N/A	See *(b)*.
Remote agent	Unconfirmed	See *(c)*.	
	Not Supported	See *(d)*.	

Legend:

N/A: Not applicable

(a) If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as "Unconfirmed"

If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as `Unconfirmed` in the Agent Operational Status window, the Status Server service is not running on the host that is running the identified agent. Start the Status Server service.

(b) If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as "Not Supported"

If there is a PFM - Agent or Remote Monitor Collector service whose operating status is shown as `Not Supported` in the Agent Operational Status window, the identified agent does not support the status management function. Consider upgrading the agent to a newer version that supports the status management function.

(c) If there is a remote agent whose operating status is shown as "Unconfirmed"

If there is a remote agent whose operating status is shown as `Unconfirmed` in the Server Operational Status window or the Agent Operational Status window, follow the procedure below.

1. Identify the Remote Monitor Collector service that corresponds to the identified remote agent.
2. Check whether the identified Remote Monitor Collector service is running.

   If the service is not running, start the Remote Monitor Collector service.

   For details on how to check the operating status of services, see *1.6 Checking the status of service operations*. For details on how to start the services, see *1.2.1 Starting services on the monitoring manager or the monitoring agent*.

   If the service is running or if the operating status of the remote agent is still shown as `Unconfirmed`, it is likely that the Remote Monitor Collector cannot communicate with the monitored host. Proceed to step 3.

   If the operating status changes to `Not Supported` after starting the Remote Monitor Collector service, proceed to *(d) If there is a remote agent whose operating status is shown as "Not Supported"*.
3. Check the communication settings for the Remote Monitor Collector service and the monitored host.

   A Remote Monitor Collector service polls its monitored host to check the operating status. If the system is configured to communicate from behind a firewall, check the firewall configuration. For details on the configuration

required to allow polling communication, see the applicable appendix in the appropriate PFM - RM manual.

Check the settings for host name resolution.

(d) If there is a remote agent whose operating status is shown as "Not Supported"

If there is a remote agent whose operating status is shown as `Not Supported` in the Server Operational Status window or the Agent Operational Status window, follow the procedure below.

1. Identify the Remote Monitor Collector service corresponding to the identified remote agent.
2. Select the identified Remote Monitor Collector service in the navigation frame of the Services window.
3. Click **Properties** in the method frame and select **Health Check Configurations** from the tree area of the Service Properties window.
4. Change the value of **Health Check for Target Hosts** to **Yes** and click the **OK** button.
5. Wait until polling is performed again.

   The default polling interval is five minutes.

   If the operating status changes to `Unconfirmed` after the time indicated by the polling interval is reached, proceed to *(c) If there is a remote agent whose operating status is shown as "Unconfirmed"*.

14.2.6 Report definition

This subsection describes how to handle errors related to a Performance Management report definition.

(1) There is a time period not indicated on the history report.

If the current time of the machine where PFM - Agent or PFM - RM is installed is changed to a time in the future, the history information from before the change to after the change is not saved.

(2) The View Server service can run out of memory when a large number of reports are displayed simultaneously.

(a) Windows

If you use PFM - Web Console to collect a large amount of report data, a memory shortage can occur with the View Server service. If this occurs, the `KAVJS5001-I` message is output.

By default, the View Server service runs with a fixed maximum memory size of 256

MB. For this reason, a memory shortage can occur with the service according to the amount of data to be processed, regardless of how much memory is available in the system. (If this error occurs, the View Server service might output a KAVE00104-E message.)

You can avoid this problem by shortening the report data collection period or decreasing the number of reports for which data is to be simultaneously collected. Alternatively, you can increase the maximum size of the memory that can be used by the View Server service to increase the amount of report data that can be processed at one time.

To increase the maximum size of the memory that can be used by the View Server service:

1. Stop PFM - Manager.
2. Create an empty file as the name of jvmopt.ini in *installation-directory*\mgr\viewsvr.
3. Use a text editor to add the following two lines in jvmopt.ini:
   -Xmx*maximum-memory-size-to-be-used-by-the-View-Server-service*
   -Djava.rmi.dgc.leaseValue=172800000
4. Save and update jvmopt.ini.
5. Restart PFM - Manager.

Example

The following example increases the maximum size of the memory that can be used by the View Server service to 354 MB:

```
-Xmx384M
-Djava.rmi.dgc.leaseValue=172800000
```

Note 1

The value specified with the -Xmx option indicates the maximum size of the memory that can be used by the View Server service.

Note 2

The -Xmx option indicates only the maximum size of the memory that can be used by the View Server service. This amount of memory is not always used by the service.

Note 3

You cannot specify a value greater than 385 MB as the maximum size of the memory that can be used by the View Server service.

Note 4

If PFM - Manager is running in a logical host environment, change the `jvmopt.ini` file in the installation directory of both the executing node and the standby node.

(b) In UNIX:

If you use PFM - Web Console to collect a large amount of report data, a memory shortage can occur with the View Server service. If this occurs, the `KAVJS5001-I` message is output.

By default, the View Server service runs with a fixed maximum memory size of 256 MB. For this reason, a memory shortage can occur with the service according to the amount of data to be processed, regardless of how much memory is available in the system. (If this error occurs, the View Server service might output a `KAVE00104-E` message.)

You can avoid this problem by shortening the report data collection period or decreasing the number of reports for which data is to be simultaneously collected. Alternatively, you can increase the maximum size of the memory that can be used by the View Server service to increase the amount of report data that can be processed at one time.

To increase the maximum size of the memory that can be used by the View Server service:

1. Stop PFM - Manager.
2. Use a text editor to search the following line in `/opt/jp1pc/mgr/viewsvr/jpcvsvr`:
   `-Xmx`*maximum-memory-size-to-be-used-by-the-View-Server-service*`\`
3. Save and update `/opt/jp1pc/mgr/viewsvr/jpcvsvr`.
4. Restart PFM - Manager.

Example

The following example increases the maximum size of the memory that can be used by the View Server service to 354 MB:

```
-Xmx384m \
```

Note 1

The value specified with the `-Xmx` option indicates the maximum size of the memory that can be used by the View Server service.

Note 2

The -Xmx option indicates only the maximum size of the memory that can be used by the View Server service. This amount of memory is not always used by the service.

Note 3

When you perform an installation, the /opt/jp1pc/mgr/viewsvr/jpcvsvr file is overwritten. If you increase the maximum size of the memory that can be used by the View Server service, back up the above file before overwriting the installation, and then overwrite the file with the backup.

Note 4

You cannot specify a value greater than 385 MB as the maximum size of the memory that can be used by the View Server service.

Note 5

If PFM - Manager is used in a logical host environment, edit /opt/jp1pc/mgr/viewsvr/jpcvsvr for both the active and standby servers.

14.2.7 Alarm definition

This subsection describes how to handle errors related to a Performance Management alarm definition.

(1) The program defined to be executed as an action does not work properly.

Possible causes and solutions:

- The machine's login environment does not match the execution environment for the program defined to be executed as an action.

  If the login environment does not match the execution environment for the program defined to be executed as an action, execution of the program might be not be possible. Determine whether the defined program can be executed as a Performance Management action. The following table lists the execution environment for a program defined to be executed as a Performance Management action.

  Table 14-3: Execution environment when a program is executed as a Performance Management action

Execution environment	Windows	UNIX
Account	System account	root user permission
Environment variables	System environment variables when a Performance Management program service starts	root user environment variables when Performance Management starts

Execution environment	Windows	UNIX
Current directory	Folder of the Action Handler service	Directory of the Action Handler service
Shell at startup	(Not applicable)	Login shell with root user permission

- You do not have permissions to execute the defined program.

  When the following programs are defined as Performance Management actions, execution of the program might not be possible depending on the restrictions of the execution permissions:

  - Programs in an NFS mount directory
  - Programs for viewing or updating files in an NFS mount directory

  Confirm whether the defined program can be executed as a Performance Management action. The table above lists the execution environment when the program is executed as a Performance Management action.

- PFM - Manager or the Action Handler service of PFM - Agent or PFM - RM of the destination host for performing the action has not started.

  If the PFM - Manager or the Action Handler service of PFM - Agent or PFM - RM of the destination host for performing the action is stopped, the action cannot be performed. To perform the action, start PFM - Manager and the Action Handler service of PFM - Agent or PFM - RM of the destination host for performing the action.

(2) No alarm event is displayed.

Possible causes and solutions:

- PFM - Manager has not started.

  When PFM - Manager is stopped, alarm events from PFM - Agent or PFM - RM might not be issued correctly. To monitor alarm events, start PFM - Manager.

14.2.8 Collecting and managing performance data

This subsection describes how to handle errors related to collecting and managing Performance Management performance data.

(1) Even if the data storage time is set for a shorter period, the size of the Store database for Agent Store does not become smaller.

If the file capacity of the Store database is already at its limit in Store version 1.0, the file size will not become smaller even if a shorter data retention period is set. In this case, set a shorter retention period, back up the Store database, and then restore it.

For details on how to set the data retention period, see *4.1.2 Modifying the retention conditions for performance data (in Store 2.0)* or *4.1.3 Modifying the retention conditions for performance data (in Store 1.0)*. For details on how to back up and restore the Agent Store and Remote Monitor Store databases, see *8.4.2 Backing up and restoring the performance data*.

(2) The message "Illegal data was detected in the Store database." is output to the common message log.

Invalid data in the Store database might have resulted due to an unexpected service halt or machine shutdown. To recover from this error:

- If the Store database has been backed up, restore it.
- If the Store database has not been backed up, stop the Master Store service, the Agent Store service, or Remote Monitor Store service, delete the corresponding database files (`*.DB` files or `*.IDX` files), and then restart the service.

14.2.9 Linking with other programs

(1) A server request error occurs and no connection is established when linking with an ODBC-compliant program.

Possible causes and solutions:

- PFM - Manager has not started.

  Confirm whether PFM -Manager has started. If PFM - Manager has not started, start it.

- There is an error in the setting of PFM - Manager for the connection destination.

  If PFM - Manager set to the connection destination has an error, correct it.

(2) A status change event is not displayed in the event browser when linking with NNM.

Possible causes and solutions:

- PFM - Manager has not started.

  Confirm whether PFM -Manager has started. If PFM - Manager has not started, start it.

- The Trap Generator service of PFM - Manager has not started.

  If the Trap Generator service of PFM - Manager has not started, start it.

- There is an error in the Trap Destination setting of the Trap Generator service of PFM - Manager.

  Confirm whether the host on which the linked NNM is installed is set as the Trap Destination.

- NNM linking is not set in PFM - Web Console.

  Confirm whether NNM linking is set in PFM - Web Console.

- There is an error in the path name specified in the NNM registration file.

  In Windows, makes sure that the path name in the NNM registration file is correct.

- The NNM ovtrapd service has not started.

  Execute the `ovstatus` command and confirm whether the ovtrapd service is running.

- There is an error in the SNMP setting of NNM.

  Confirm whether the community is set to `public` and the SNMP port is blank or set to `162`.

(3) No symbol appears in ovw when linking with NNM.

Possible causes and solutions:

- No status change event occurred.

  Confirm whether a status change event appears in the alarm browser.

- The NNM JPCObjMgr service has not started.

  Execute the `ovstatus` command and confirm whether the JPCObjMgr service is running.

(4) JP1 events are not reported when linking with JP1/IM.

Possible causes and solutions:

- There is an error in the settings for enabling JP1 events to be issued.

  Confirm whether the settings for issuing JP1 events are correct with PFM - Web Console.

- There is an error in the alarm setting.

  Confirm whether the alarm setting is correct with PFM - Web Console.

- JP1/Base is not installed or set up.

  Confirm whether JP1/Base is installed and set up.

(5) Monitored PFM - Agent or PFM - RM is not displayed in the monitoring tree window when linking with a monitored object function of JP1/IM.

Possible causes and solutions:

- The monitored PFM - Agent or PFM - RM has never been started.

  If PFM - Agent or PFM - RM has never been started, it is not displayed in the monitoring tree. Start PFM - Agent or PFM - RM and then redisplay the

monitoring tree.

- PFM - Agent and PFM - Manager are not connected, or PFM - RM and PFM - Manager are not connected.

  If PFM - Agent and PFM - Manager, or PFM - RM and PFM - Manager are not connected, establish a connection.

- The monitored object linkage function of JP1/IM is not set up.

  If the monitored object linkage function of JP1/IM is not set up, set it up.

(6) The display color of the monitored object does not change when linking with a monitored object function of JP1/IM.

Possible causes and solutions:

- A JP1 event has not been issued.

  Use the Event Monitor window to make sure that a JP1 event has been issued. If a JP1 event has not been issued, make sure that the alarm definition is correct.

- There is an error in the JP1/Base settings.

  Confirm that there are no errors in the JP1/Base settings. When the issuing of a JP1 event from the PFM - Agent or PFM - RM host is specified, confirm whether the transmission of a JP1 event from the PFM - Agent or PFM - RM host to the PFM - Manager host is set.

14.2.10 Other problems

Check the existing circumstances when errors occur. If a message is output, read its contents. For details on the log information output by Performance Management, see *14.3 Log information*.

If you cannot resolve an error by taking any of the steps described from *14.2.1 Setting up and starting a service* to *14.2.9 Linking with other programs*, or if an error occurs not described in these sections, collect the data needed to investigate the error, and then contact the system administrator.

For details on the data you need to collect and how to collect it, see *14.4 Data to be collected in the event of trouble* and *14.5 Data collection procedure*.

14.3 Log information

When an error occurs with Performance Management, check the log information and investigate the problem. The following four types of log information are output during operation of Performance Management:

- System log
- Common message log
- Operation status log
- Trace log

This section describes the four types of log information and the log options that can be set for each type.

14.3.1 Type of log information

(1) System log

The system log contains log information that reports the system status and errors that occurred. This log information is output to the following log file:

- In Windows

  Event log file

- In UNIX

  syslog file

For details on the output format, see the chapter explaining the log information in the manual *Job Management Partner 1/Performance Management Reference*.

Notes on logical host use:

To check the control of Performance Management by cluster software, the cluster software log is required in addition to the Performance Management system log.

(2) Common message logs

The common message logs contain log information that reports the system status and errors that have occurred. The information output to these logs is more detailed than the system log information. For details on the output destination file name and file size for common message logs, see *14.3.2 Log information files*. For details on the output format, see the chapter describing the log information in the manual *Job Management Partner 1/Performance Management Reference*.

Note:

The language of the common message log information is determined by the `LANG`

environment variable set when a service is started or a command is executed, therefore, the common message log might contain character strings with different language codes.

Notes on logical host use:

The common message logs are output to the shared disk when Performance Management is used on a logical host. The common message log information before and after a failover is recorded in the same log file, because the log file on the shared disk is inherited together with the system when a failover takes place.

(3) Operation status logs

The operation status logs contain the log information output by PFM - Web Console.

For details on the output destination file name and file size for operation status logs, see *14.3.2 Log information files*. For details on the output format, see the chapter describing the log information in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Trace logs

The trace logs contain log information needed, when an error occurs, to investigate the cause of the error or to determine the processing time required by each process.

The trace log information is output to a log file for each Performance Management service.

Notes on logical host use:

The trace logs are output to the shared disk when Performance Management is used on a logical host. The trace log information before and after a failover is recorded in the same log file, because the log file on the shared disk is inherited together with the system when a failover takes place.

14.3.2 Log information files

This section describes the log information output from Performance Management.

(1) Common message logs and operation status logs

The following tables list (by OS) the services or controls that are the output sources, the log file names, and the amount of disk space used for common message logs and operation status logs. The wrap-around file method is used to write data to the operation status log.

Table 14-4: File names of common message logs (in Windows)

Type of log information	Output source	File name	Disk space used[#1] (KB)
Common message log	Performance Management	*installation-folder*\log\jpclog{01|02}[#2]	2,048 (x 2)
		installation-folder\log\jpclogw{01|02}[#2]	2,048 (x 2)
Common message log (for logical host use)	Performance Management for logical host use	*environment-directory*[#3]\jplpc\log\jpclog{01|02}[#2]	2,048 (x 2)
		environment-directory[#3]\jplpc\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, 256 (x 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

The value 01 or 02 is appended to the file name of the common message log.

For the sequential file method (jpclog)

This method always writes the newest log information to the jpclog01 file (whose name ends with 01).

When the log file size reaches the set value, jpclog01 is renamed and saved as jpclog02, the contents of jpclog01 are cleared, and then the newest log information is written.

For the wrap-around file method (jpclogw)

When the log file size reaches the set value, the next log file contents are cleared, and the newest log information is written in the next log file. The file to be written to changes in the following manner: the file after jpclogw01 is jpclogw02 and the file after jpclogw02 is jpclogw01.

#3

The environment directory is a folder on the shared disk specified at the time the logical host is created.

Table 14-5: File names of operation status logs

Type of log information	Output source	File name	Disk space used#1 (KB)
Operation status log	PFM - Web Console	*installation-folder*\log\jpcwtrace*log-file-number*#3.log	4,096 (x 10)
		For the jpcrpt command#2 *installation-folder*\log\jpcrpt_*process-ID-of-executed-command_log-file-number*#3.log For the jpcrdef, jpcasrec, or jpcaspsv command *installation-folder*\log*command-name_sub-command-name_log-file-number*#3.log For the jpcmkkey command *installation-folder*\log\jpcmkkey_*log-file-number*#3.log For all other commands *installation-folder*\log*command-name_log-file-number*#3.log	4,096 (x 10 x 9 (number of PFM - Console commands))

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 256 (x 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

To limit the amount of memory used to the value shown in the above table when the jpcrpt command is executed over 1,500 times per month (or on average 50 times per day), you must shorten the retention period of the log files.

The following shows an example setting:

If the command is executed 3,000 times per month (or on average 100 times per day)

Limit the retention period of the log files to a maximum of 15 days.

If the command is executed 6,000 times per month (or on average 200 times per day)

Limit the retention period of the log files to a maximum of seven days.

These examples are only a guide, because the retention period for the jpcrpt command log files has the following characteristics.

About the retention period of jpcrpt command log files

If the total file size for the log files exceeds the value of logFileNumber x logFileSize specified in the initialization file (config.xml), the jpcrpt command deletes log files until the total file size is below the specified value.

In this case, only the files updated earlier than the number of days specified by logFileRetention in the initialization file (config.xml) are deleted.

Below are examples of how to calculate the retention period.

Example 1:

This example assumes that logFileRetention is set to 3 days (= 72 hours) and the following 6 files remain.

```
jpcrpt_3509_log1.log   9 MB  100 hours before
jpcrpt_3510_log1.log   9 MB   80 hours before
---<Reference time (= 72 hours before)>---
jpcrpt_3511_log1.log   9 MB   60 hours before
jpcrpt_3512_log1.log   9 MB   40 hours before
jpcrpt_3513_log1.log   9 MB   20 hours before
jpcrpt_3514_log1.log   9 MB     Several minutes before
```

When the jpcrpt command is executed in this situation, the files updated earlier than the reference time are deleted in chronological order until the total size of the log files is below 40 MB. This is because the current total size for the 6 log files is 54 MB, which is greater than 40 MB.

In this example, jpcrpt_3509_log1.log and jpcrpt_3510_log1.log would be deleted. The total file size becomes 36 MB and 4 files remain.

Example 2:

This example assumes that logFileRetention is set to 3 days (= 72 hours) and the following 6 files remain.

```
jpcrpt_3509_log1.log   7 MB  100 hours before
jpcrpt_3510_log1.log   7 MB   80 hours before
---<Reference time (= 72 hours before)>---
jpcrpt_3511_log1.log   7 MB   60 hours before
jpcrpt_3512_log1.log   7 MB   40 hours before
jpcrpt_3513_log1.log   7 MB   20 hours before
jpcrpt_3514_log1.log   7 MB   Several minutes before
```

When the jpcrpt command is executed in this situation, the files updated earlier than the reference time are deleted in chronological order until the total size of the log files is below 40 MB. This is because the current total

size for the 6 log files is 42 MB, which is greater than 40 MB.

In this example, `jpcrpt_3509_log1.log` would be deleted. The total file size becomes 35 MB and 5 files remain including `jpcrpt_3510_log1.log`, which is updated earlier than the reference time.

Example 3:

This example assumes that `logFileRetention` is set to 3 days (= 72 hours) and the following 6 files remain.

```
jpcrpt_3509_log1.log   1 MB  100 hours before
jpcrpt_3510_log1.log   1 MB   80 hours before
---<Reference time (= 72 hours before)>---
jpcrpt_3511_log1.log   1 MB   60 hours before
jpcrpt_3512_log1.log   1 MB   40 hours before
jpcrpt_3513_log1.log   1 MB   20 hours before
jpcrpt_3514_log1.log   1 MB   Several minutes before
```

Even if the `jpcprt` command is executed in this situation, none of the files are deleted, including those updated earlier than the reference time, because the total log file size is 6 MB, which is smaller than 40 MB.

Example 4:

This example assumes that `logFileRetention` is set to 30 days (= 720 hours) and the following 6 files remain.

```
---<Reference time (= 720 hours before)>---
jpcrpt_3509_log1.log   9 MB  100 hours before
jpcrpt_3510_log1.log   9 MB   80 hours before
jpcrpt_3511_log1.log   9 MB   60 hours before
jpcrpt_3512_log1.log   9 MB   40 hours before
jpcrpt_3513_log1.log   9 MB   20 hours before
jpcrpt_3514_log1.log   9 MB    Several minutes before
```

When the `jpcprt` command is executed in this situation, the current total size for the 6 files would be 54 MB, which is greater than 40 MB. However, because none of the retention times for the files exceeds 30 days (= 72 hours) from the time they were saved, as set in `logFileRetention`, none of the files would be deleted.

#3

The log file number is the number of output log files, starting from `1`.

Operation status log output

The output size of the operation status log (excluding the log for the `jpcrpt` command) can be set by using `logFileSize` x `logFileNumber` in the initialization file (`config.xml`).

Table 14-6: File names of common message logs (in UNIX)

Type of log information	Output source	File name	Disk space used[#1] (KB)
Common message log	Performance Management	`/opt/jp1pc/log/jpclog{01|02}`[#2]	2,048(x 2)
		`/opt/jp1pc/log/jpclogw{01|02}`[#2]	2,048(x 2)
Common message log (for logical host use)	Performance Management for logical host use	*environment-directory*[#3]`/jp1pc/log/jpclog{01|02}`[#2]	2,048(x 2)
		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, 256 (x 2) indicates that up to two log files, each using 256 KB of disk space, can be created. In this case, a total of 512 KB of disk space will be used.

#2

The value `01` or `02` is appended to the file name of the common message log.

For the sequential file method (`jpclog`)

This method always writes the newest log information to the `jpclog01` file (whose name ends with `01`).

When the log file size reaches the set value, `jpclog01` is renamed and saved as `jpclog02`, the contents of `jpclog01` are cleared, and then the newest log information is written.

For the wrap-around file method (`jpclogw`)

When the log file size reaches the set value, the next log file contents are cleared, and the newest log information is written in the next log file. The file to be written to changes in the following manner: the file after `jpclogw01` is `jpclogw02` and the file after `jpclogw02` is `jpclogw01`.

#3

The environment directory is a directory on the shared disk specified at the time the logical host is created.

(2) Trace log

The following tables list (by OS) the services or controls that are the output sources and the installation directories for trace logs.

Table 14-7: Installation folder names of trace logs (in Windows)

Type of log information	Output source	Folder name
Trace log	Action Handler	*installation-folder*\bin\action\log\
	Agent Collector and Remote Monitor Collector	*installation-folder**xxxx*[#1]\agent*instance-name*[#2]\log\
	Agent Store and Remote Monitor Store	*installation-folder**xxxx*[#1]\store*instance-name*[#2]\log\
	Correlator	*installation-folder*\mgr\clator\log\
	Agent Collector (health check agent)	*installation-folder*\agt0\agent\log\
	Agent Store (health check agent)	*installation-folder*\agt0\store\log\
	Master Store	*installation-folder*\mgr\store\log\
	Master Manager	*installation-folder*\mgr\manager\log\
	Name Server	*installation-folder*\mgr\namesvr\log\
	Performance Management command	*installation-folder*\tools\log\
	Status Server	*installation-folder*\bin\statsvr\log\
	Trap Generator	*installation-folder*\mgr\trapgen\log\
	View Server	*installation-folder*\mgr\viewsvr\log\
Trace log (for logical host use)	Action Handler	*environment-directory*[#3]\jp1pc\bin\action\log\
	Agent Collector and Remote Monitor Collector	*environment-directory*[#3]\jp1pc*xxxx*[#1]\agent*instance-name*[#2]\log\

Type of log information	Output source	Folder name
	Agent Store and Remote Monitor Store	*environment-directory*#3\jp1pc*xxxx*#1\store*instance-name*#2\log\
	Correlator	*environment-directory*#3\jp1pc\mgr\clator\log\
	Agent Collector (health check agent)	*environment-directory*#3\jp1pc\agt0\agent\log\
	Agent Store (health check agent)	*environment-directory*#3\jp1pc\agt0\store\log\
	Master Store	*environment-directory*#3\jp1pc\mgr\store\log\
	Master Manager	*environment-directory*#3\jp1pc\mgr\manager\log\
	Name Server	*environment-directory*#3\jp1pc\mgr\namesvr\log\
	Performance Management command	*environment-directory*#3\jp1pc\tools\log\
	Trap Generator	*environment-directory*#3\jp1pc\mgr\trapgen\log\
	View Server	*environment-directory*#3\jp1pc\mgr\viewsvr\log\

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a folder for each instance.

#3

The environment directory is a folder on the shared disk specified at the time the logical host is created.

Table 14-8: Installation directory names of trace logs (in UNIX)

Type of log information	Output source	Directory name
Trace log	Action Handler	/opt/jp1pc/bin/action/log/
	Agent Collector and Remote Monitor Collector	/opt/jp1pc/*xxxx*[#1]/agent/*instance-name*[#2]/log/
	Agent Store and Remote Monitor Store	/opt/jp1pc/xxxx[#1]/store/*instance-name*[#2]/log/
	Correlator	/opt/jp1pc/mgr/clator/log/
	Agent Collector (health check agent)	/opt/jp1pc/agt0/agent/log/
	Agent Store (health check agent)	/opt/jp1pc/agt0/store/log/
	Master Store	/opt/jp1pc/mgr/store/log/
	Master Manager	/opt/jp1pc/mgr/manager/log/
	Name Server	/opt/jp1pc/mgr/namesvr/log/
	Performance Management command	/opt/jp1pc/tools/log/
	Status Server	/opt/jp1pc/bin/statsvr/log/
	Trap Generator	/opt/jp1pc/mgr/trapgen/log/
	View Server	/opt/jp1pc/mgr/viewsvr/log/
Trace log (for logical host use)	Action Handler	*environment-directory*[#3]/jp1pc/bin/action/log/
	Agent Collector and Remote Monitor Collector	*environment-directory*[#3]/jp1pc/*xxxx*[#1]/agent/instance name[#2]/log/
	Agent Store and Remote Monitor Store	*environment-directory*[#3]/jp1pc/*xxxx*[#1]/store/instance name[#2]/log/

Type of log information	Output source	Directory name
	Correlator	*environment-directory*#3`/jp1pc/mgr/clator/log/`
	Agent Collector (health check agent)	*environment-directory*#3`/jp1pc/agt0/agent/log/`
	Agent Store (health check agent)	*environment-directory*#3`/jp1pc/agt0/store/log/`
	Master Store	*environment-directory*#3`/jp1pc/mgr/store/log/`
	Master Manager	*environment-directory*#3`/jp1pc/mgr/manager/log/`
	Name Server	*environment-directory*#3`/jp1pc/mgr/namesvr/log/`
	Performance Management command	*environment-directory*#3`/jp1pc/tools/log/`
	Trap Generator	*environment-directory*#3`/jp1pc/mgr/trapgen/log/`
	View Server	*environment-directory*#3`/jp1pc/mgr/viewsvr/log/`

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a directory for each instance.

#3

The environment directory is a directory on the shared disk specified at the time the logical host is created.

14.4 Data to be collected in the event of trouble

If the actions described in *14.2 Troubleshooting* are not successful in correcting the error, collect the necessary data, and then contact the system administrator to determine the cause of the error. This subsection describes the data that you need to collect in the event of an error.

Performance Management provides commands for collecting the needed data in one operation. To collect PFM - Manager, PFM - Agent, and PFM - RM data, use the `jpcras` command. To collect PFM - Web Console data, use the `jpcwras` command. The following tables indicate the data that can be collected by the `jpcras` or `jpcwras` command.

Note:

The data collected by the `jpcras` or `jpcwras` command depends on the options you specify when you execute the command. For details on the options specified in the command and the data that can be collected, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

Notes on logical host use:

Note the following when using a logical host.

- The logs for Performance Management for logical host use are stored on the shared disk. When the shared disk is online (in Windows) or mounted (in UNIX), the `jpcras` command can be used to collect all logs on the shared disk at once.
- To determine the cause of any problems at the time of a failover, the data before and after the failover is required. Therefore, the data of both the executing and standby nodes is required.
- To investigate Performance Management for logical host use, the cluster software data is required. Because the starting and stopping of Performance Management for logical host use are controlled by the cluster software, investigate Performance Management by comparing the operations of the cluster software and Performance Management.

14.4.1 Data to be collected in the event of an error (in Windows)

(1) Log information about the OS

The following table lists the log information about the OS to be collected.

Type of information	Outline	Default file name	Collected by the jpcras command	Collected by the jpcwras command
System log	Windows event log	N/A	Y	Y
Process information	List of processes	N/A	Y	Y
System file	hosts file	*system-folder*\system32\drivers\etc\hosts	Y	Y
	services file	*system-folder*\system32\drivers\etc\service	Y	Y
OS information	System information	N/A	Y	Y
	Network status	N/A	Y	Y
	Host name	N/A	Y	Y
Dump information	Dr. Watson log file#1	*system-drive*\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwtsn32.log#2 *system-drive*\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dump#2	Y	Y

Legend:

Y: Can be collected

N/A: Not applicable

#1

Windows Server 2008 provides Problem Reports and Solutions, which replace Dr. Watson.

#2

If your setup provides for output of log files to a different folder, be sure that you collect the data from the correct folder.

(2) Performance Management information

You need to collect the information about Performance Management listed below. In

the case of a network error, you also need to collect applicable files from the connection-destination machine. The Performance Management information required to be collected is shown below.

Type of information	Outline	Default file name	Collected by the `jpcras` command
Common message log	Message log output from Performance Management (sequential file method)	*installation-folder*`\log\jpclog{01|02}`[#1]	Y
	Message log output from Performance Management (wrap-around file method)	*installation-folder*`\log\jpclogw{01|02}`[#1]	Y
Configuration information	Each configuration information file	N/A	Y
	Output results of the `jpctool service list` command	N/A	Y
Version information	Product version	N/A	Y
	History information	N/A	Y
Database information	Name Server	*installation-folder*`\mgr\namesvr\*.DB` *installation-folder*`\mgr\namesvr\*.IDX`	Y
	Master Manager	*installation-folder*`\mgr\manager\*.DB` *installation-folder*`\mgr\manager\*.IDX`	Y
	Master Store	*installation-folder*`\mgr\store\*.DB` *installation-folder*`\mgr\store\*.IDX`	Y
	View Server	*installation-folder*`\mgr\viewsvr\data\*` *installation-folder*`\mgr\viewsvr\Reports\*`	Y
	Agent Store and Remote Monitor Store	*installation-folder*`\`*xxxx*[#2]`\store\`*instance-name*[#3]`\*.DB` *installation-folder*`\`*xxxx*[#2]`\store\`*instance-name*[#3]`\*.IDX`	Y

Type of information	Outline	Default file name	Collected by the `jpcras` command
	Agent Store (health check agent)	*installation-folder*`\agt0\store\*.DB` *installation-folder*`\agt0\store\*.IDX`	Y
Trace log	Trace information of each service in the Performance Management program	N/A[#4]	Y
Install log[#5]	Message log at the time of installation (in Windows Server 2003)	*TEMP-folder*`\pfm_inst.log`	N
	Message log at the time of installation (in Windows Server 2008)	Following files in the *system-folder*`\TEMP\HCDINST` folder: • `HCDMAIN.LOG` and `HCDMAIN`*n*`.LOG`[#4] • `HCDINST.LOG` and `HCDINST`*n*`.LOG`[#4] • *product-model-name*`.LOG`	N
	Install log[#6]	*system-folder*`\TEMP\HCDINST\`*product-model-name*`.LOG`	N
	Integrated installer log	*system-folder*`\TEMP\HCDINST\HCDMAIN.LOG` *system-folder*`\TEMP\HCDINST\HCDMAIN#.LOG` (# indicates a number)	N

Legend:

Y: Can be collected

N: Cannot be collected

N/A: Not applicable

#1

For details on the output format of the log files, see *13.5 Detecting problems by linking with the integrated system monitoring product*.

#2

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming

rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#3

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a folder for each instance.

#4

For details on the trace log storage destination, see *14.3.2 Log information files*.

#5

Collect this information if the installation fails.

#6

This is only applicable for Windows Server 2008.

(3) PFM - Web Console information

You need to collect the information about PFM - Web Console listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The PFM - Web Console information required to be collected is shown below.

Type of information	Outline	Default file name	Collected by the `jpcwras` command
Web server information	Server log of Web server or Web container	N/A	Y
Registry information	Product registry information	N/A	Y
Operation status log[#1]	Message log output from PFM - Web Console	*installation-folder*`\log\jpcwtrace1`[#2]`.log`	Y

Type of information	Outline	Default file name	Collected by the jpcwras command
	Message log output from a PFM - Web Console command	For the jpcrpt command *installation-folder*\log\jpcrpt_*process-ID-of-executed-command*_log1[#2].log For the jpcrdef, jpcasrec, or jpcaspsv command *installation-folder*\log*command-name_sub-command-name*_log1[#2].log For the jpcmkkey command *installation-folder*\log\jpcmkkey_log1[#2].log For all other commands *installation-folder*\log*command-name*_log1[#2].log	Y
File information	List of PFM - Web Console installation files	N/A	Y
Configuration Info	PFM - Web Console configuration information	*installation-folder*\config*.* *installation-folder*\sample\config*.*	Y
PFM - Web Console log information	(Un)installer log file	*system-drive*\pfmwebconuninst.log[#3] *system-drive*\pfmwebconinst.rtn[#3] *system-drive*\pfmwebconinst.log[#3] *system-drive*\pfmwebconuninst.rtn[#3]	Y
		system-folder\TEMP\HCDINST*product-model-name*.LOG[#4]	N

Legend:

Y: Can be collected

N: Cannot be collected

N/A: Not applicable

#1

For details on the output format of the operation status log, see the chapter explaining the log information in the manual *Job Management Partner 1/ Performance Management Reference*.

#2

The value `1` is appended to the file name of the operation status log.

#3

In Windows Server 2003 only

#4

In Windows Server 2008 only

(4) Operation information

You need to collect the following information about the operation being performed when an error occurs:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon

(5) Error information on window displays

Obtain printouts of the following:

- The Web browser
- The window operation when the application error occurred
- The error message dialog box (including the contents displayed if there is a **Details** button)
- The Command Prompt window or the Administrator Console window, if the error occurred during command execution

(6) User dumps (Windows Server 2008)

If a Performance Management process stops due to an application error under Windows Server 2008, collect the user dumps.

(7) Problem reports (Windows Server 2008)

If a Performance Management process stops due to an application error under Windows Server 2008, collect the problem reports.

(8) Other information

You also need to collect the following information:

- The contents of **System Information**, which is displayed by choosing **Accessories** and then **System Tools** (applicable in Windows 2003 and Windows Server 2008)
- The command arguments that were specified, if the error occurred during command execution
- Java VM thread dump

  When collecting PFM - Web Console information, collect the Java VM thread dump.

To collect the Java VM thread dump:

1. Execute the following command ten times at three-second intervals.

   `#` *installation-directory*`/CPSB/CC/web/bin/cjdumpweb PFMWebConsole`

2. Execute the `jpcwras` command.

Note:

Because the operation of Java VM becomes unstable when collecting a thread dump, restart the PFM - Web Console service.

14.4.2 Data to be collected in the event of an error (in UNIX)

(1) Log information about the OS

The following table lists the log information about the OS to be collected.

Type of information	Outline	Default file name	Collected by the `jpcras` command	Collected by the `jpcwras` command
System log	syslog	• In HP-UX `/var/adm/syslog/syslog.log` • In Solaris `/var/adm/messages*` • In AIX `/var/adm/syslog*` • In Linux `/var/log/messages*`	Y[#1]	Y[#1]
Process information	List of processes	N/A	Y	Y
System file	`hosts` file	`/etc/hosts`	Y	Y

Type of information	Outline	Default file name	Collected by the jpcras command	Collected by the jpcwras command
		/etc/inet/ipnodes[#2]	Y[#3]	N
	services file	/etc/services	Y	Y
OS information	Patch information	N/A	Y	Y
	Kernel information	N/A	Y	Y
	Version information	N/A	Y	Y
	Network status	N/A	Y	Y
	Environment variables	N/A	Y	Y
	Host name	N/A	Y	Y
Dump information	core file[#4]	N/A	Y	N

Legend:

Y: Can be collected

N: Cannot be collected

N/A: Not applicable

#1

This cannot be collected in a system where output is not set to the default path or file name. In this case, use a different method to collect this information.

#2

The /etc/inet/ipnodes file is available only under Solaris. Collect it together with the /etc/hosts file.

#3

This file can only be collected with the jpcras command included in PFM - Manager 09-00 or PFM - Base 09-00 or later.

#4

Under HP-UX 11i V3 (IPF), you can use the coreadm command to rename the core file. If the core file is renamed to a file name that does not start with core, the jpcras command cannot collect it. In this case, collect the file manually.

(2) Performance Management information

You need to collect the information about Performance Management listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The Performance Management information required to be collected is shown below.

Type of information	Outline	Default file name	Collected by the `jpcras` command
Common message log	Message log output from Performance Management (sequential file method)	`/opt/jp1pc/log/jpclog{01|02}`[#1]	Y
	Message log output from Performance Management (wraparound file method)	`/opt/jp1pc/log/jpclogw{01|02}`[#1]	Y
Configuration information	Each configuration information file	N/A	Y
	Output results of the `jpctool service list` command	N/A	Y
Version information	Product version	N/A	Y
	History information	N/A	Y
Database information	Name Server	`/opt/jp1pc/mgr/namesvr/*.DB` `/opt/jp1pc/mgr/namesvr/*.IDX`	Y
	Master Manager	`/opt/jp1pc/mgr/manager/*.DB` `/opt/jp1pc/mgr/manager/*.IDX`	Y
	Master Store	`/opt/jp1pc/mgr/store/*.DB` `/opt/jp1pc/mgr/store/*.IDX`	Y
	View Server	`/opt/jp1pc/mgr/viewsvr/data/*` `/opt/jp1pc/mgr/viewsvr/Reports/*`	Y
	Agent Store and Remote Monitor Store	`/opt/jp1pc/`*xxxx*[#2]`/store/`*instance-name*[#3]`/*.DB` `/opt/jp1pc/`*xxxx*[#2]`/store/`*instance-name*[#3]`/*.IDX`	Y

Type of information	Outline	Default file name	Collected by the `jpcras` command
	Agent Store (health check agent)	`/opt/jp1pc/agt0/store/*.DB` `/opt/jp1pc/agt0/store/*.IDX`	Y
Trace log	Trace information of each service in the Performance Management program	N/A[#4]	Y

Install log[#5]	Standard log of Hitachi Program Product Installer	`/etc/.hitachi/.hitachi.log`
		`/etc/.hitachi/.hitachi.log{01|02|03|04|05}`
		`/etc/.hitachi/.install.log`
		`/etc/.hitachi/.install.log{01|02|03|04|05}`
			N

Legend:

Y: Can be collected

N: Cannot be collected

N/A: Not applicable

#1

For details on the output format of the log files, see *13.5 Detecting problems by linking with the integrated system monitoring product*.

#2

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on the service keys of each PFM - Agent or PFM - RM, see the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#3

For a PFM - Agent or PFM - RM monitoring an application program which can start multiple service sets on a single host, there is a directory for each instance.

#4

For details on the trace log destination directory, see *14.3.2 Log information files*.

#5

Collect this information if the installation fails.

(3) PFM - Web Console information

You need to collect the information about PFM - Web Console listed below. In the case of a network error, you also need to collect applicable files from the connection-destination machine. The PFM - Web Console information that needs to be collected is shown below.

Type of information	Outline	Default file name	Collected by the `jpcwras` command
Web server information	Server log of Web server or Web container	N/A	Y
Operation status log[#1]	Message log output from PFM - Web Console	`/opt/jp1pcwebcon/log/jpcwtrace1`[#2]`.log`	Y

	Message logs output from PFM - Web Console commands	For the `jpcrpt` command
		`/opt/jp1pcwebcon/log/jpcrpt_`*process-ID-of-executed-command*`_log1`[#2]`.log`
		For the `jpcrdef`, `jpcasrec`, or `jpcaspsv` command
		`/opt/jp1pcwebcon/log/`*command-name_sub-command-name*`_log1`[#2]`.log`
		For the `jpcmkkey` command
		`/opt/jp1pcwebcon/log/jpcmkkey_log1`[#2]`.log`
		For all other commands
		`/opt/jp1pcwebcon/log/`*command-name*`_log1`[#2]`.log`
			Y

File information	List of PFM - Web Console installation files	N/A	Y
Configuration Info	PFM - Web Console configuration information	`/opt/jp1pcwebcon/conf/*.*/opt/jp1pcwebcon/sample/conf/*.*`	Y

Legend:

Y: Can be collected

N/A: Not applicable

#1

For details on the output format of the operation status log, see the chapter describing the log information in the manual *Job Management Partner 1/ Performance Management Reference*.

#2

The value `1` is appended to the file name of the operation status log.

(4) Operation information

You need to collect the following information about the operation being performed when an error occurs:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon

(5) Error information

You need to obtain the following error information:

- Messages output to the console, if the error occurred during command execution

(6) Other information

You also need to collect the following information:

- The command arguments that were specified, if the error occurred during command execution

14.5 Data collection procedure

This subsection describes how to collect data in the event of an error.

14.5.1 Data collection procedure (in Windows)

(1) Collecting dump information (Windows Server 2008)

To collect dump information in Windows Server 2008:

1. Open Task Manager.
2. Select the **Processes** tab.
3. Right-click the name of the process for which you want to collect dump information and select **Create Dump File**.

   Dump files are stored in the following folder:
   system-drive`\Users\`*user-name*`\AppData\Local\Temp`

4. Collect the dump files from the folder given in step 3.

   If the setting of an environment variable was changed so that the dump files are directed to a folder other than that given in step 3, collect the dump files from the new folder.

(2) Executing the data collection command

Use the `jpcras` or `jpcwras` command to collect the data needed to determine the cause of an error. Note that the user who executes the procedures described below must have Administrators permissions.

To execute the data collection command:

1. Log on to the host where the service subject to this data collection is installed.
2. At the command prompt, execute the following command to enable the extended command facility of the command interpreter:
   ```
   cmd /E:ON
   ```
3. Specify in the `jpcras` or `jpcwras` command the data to be collected and the storage folder for the data, and then execute the command.

   The following shows an example of specifying the command when all information that can be obtained by the `jpcras` command is to be stored in the `c:\tmp\jp1pcc\mgr` folder:

   ```
   jpcras c:\tmp\jp1pc\mgr all all
   ```

The following shows an example of specifying the command when all information that can be obtained by the `jpcwras` command is to be stored in the `c:\tmp\jp1pc\WebCon` folder:

```
jpcwras c:\tmp\jpc1pcWebCon
```

When the `jpcras` command is executed, the `jpctool service list -id * -host *` command is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take some time to complete the `jpctool service list -id * -host *` command. In such a case, by setting the value of the `JPC_COLCTRLNOHOST` environment variable to `1`, you can suppress the `jpctool service list -id * -host *` command, to reduce the time required to complete the command.

For details on the `jpcras` and `jpcwras` commands, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

Note on command execution under Windows Server 2008:

If the user account control function (UAC) of the OS is enabled, a dialog box for user account control may appear during command execution. If this occurs, click the **Continue** button to proceed with data collection. Clicking the **Cancel** button stops data collection.

(3) Executing the data collection command (for logical host use)

The data of Performance Management for logical host use exists on the shared disk, and this data must be collected from both the executing node and standby node.

Use the `jpcras` or `jpcwras` command to collect the data needed to determine the cause of an error. The following describes the procedure for executing the data collection command. Note that the user who executes the procedure described below must have Administrators permissions.

To execute the data collection command for logical host use:

1. Make the shared disk available online.

   The data of the logical host is stored on the shared disk. For the executing node, make sure that the shared disk is online and then collect the data.

2. For both the executing and standby nodes, specify in the `jpcras` or `jpcwras` command the data to be collected and the storage folder for the data, and then execute the command.

   The following shows an example of specifying the command when all information that can be obtained by the `jpcras` command is to be stored in the

c:\tmp\jp1pcc\mgr folder:

```
jpcras c:\tmp\jp1pc\mgr all all
```

When the jpcras command is executed without specifying the lhost argument, all the Performance Management data of the physical host and logical host of that node is collected.

The following shows an example of specifying the command when all information that can be obtained by the jpcwras command is to be stored in the c:\tmp\jp1pc\WebCon folder:

```
jpcwras c:\tmp\jpc1pcWebCon
```

If Performance Management exists in the logical host environment, the log files on the shared disk are acquired. In addition, when the jpcras command or jpcwras command is executed on a node in which the shared disk is offline, files on the shared disk cannot be acquired, but the command ends normally without an error.

Note:

Execute the command to collect the data on both the executing node and standby node. To investigate the conditions before and after a failover, the data of both the executing node and standby node is required.

3. Collect the cluster software data.

   This data is required to investigate whether an error occurred in either the cluster software or Performance Management. Collect the data to enable an investigation of the control request, such as a start or stop request from the cluster software to Performance Management, and the results.

When the jpcras command is executed, the jpctool service list -id * -host * command is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take a long time to complete the jpctool service list -id * -host * command. In such a case, by setting the value of the JPC_COLCTRLNOHOST environment variable to 1, you can suppress the jpctool service list -id * -host * command, to reduce the time required to complete the command.

For details on the jpcras and jpcwras commands, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

(4) Collecting Windows event logs

Use the Windows Event Viewer window to output Windows event logs to a file.

(5) Checking information about the operation

Check the information about the operation when an error occurs and record the information. You also need to check the following information:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon

(6) Collecting error information on window displays

Obtain printouts of the following:

- The Web browser
- The window operation, if an application error occurred
- The error message dialog box

  Also print a copy of any detailed information.
- The Command Prompt window or the Administrator Console window, if the error occurred during command execution

  To obtain a printout of the Command Prompt window or the Administrator Console window in Windows Server 2003 or Windows Server 2008, perform the following settings in the Command Prompt Properties window:

  - **Edit Options** on the **Options** tab

    Select the **Quick Edit mode** checkbox.
  - The **Layout** tab

    Under **Screen buffer size**, set **Height** to `500`.

(7) Collecting other information

You also need to collect the following information:

Common to all OSs

- The command arguments that were specified, if the error occurred during command execution

- The contents of **System Information**, which is displayed by choosing **Accessories** and then **System Tools**

In Windows Server 2003

- Information displayed in **System** and **Applications** of the Windows System Event Viewer window

In Windows Server 2008

- Information displayed in **System** and **Applications** in the left pane titled **Windows logs** in the Windows System Event Viewer window

14.5.2 Data collection procedure (in UNIX)

(1) Executing the data collection command

Use the `jpcras` command to collect the data needed to determine the cause of an error. Note that the user who executes the procedures described below must be a root user.

To execute the data collection command:

1. Log on to the host where the service subject to this data collection is installed.
2. Specify in the `jpcras` command the data to be collected and the storage directory for the data, and then execute the command.

   The following shows an example of specifying the command when all information that can be obtained by the `jpcras` command is to be stored in the `/tmp/jp1pc/mgr` directory:

   ```
   jpcras /tmp/jp1pc/mgr all all
   ```

   The data collected by the data collection command can be stored in the specified directory in a compressed format by using either the `tar` or `compress` command. Example of the file name:

   Data collected by the `jpcras` command: `jpcras`*YYMMDD*`.tar.Z`

   YYMMDD represents the year, month, and date.

When the `jpcras` command is executed, the `jpctool service list -id "*" -host "*"` command is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take an extended period to complete the `jpctool service list -id "*" -host "*"` command. In such a case, by setting the value of the `JPC_COLCTRLNOHOST` environment variable to `1`, you can suppress the `jpctool service list -id "*" -host "*"` command, to reduce the time required to complete the command.

For details on the `jpcras` command, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

(2) Executing the data collection command (for logical host use)

The data of Performance Management for logical host use exists on the shared disk, and this data must be collected from both the executing node and standby node.

Use the `jpcras` command to collect the data needed to determine the cause of an error. The following describes the procedure for executing the data collection command. Note that the user who executes the procedure described below must be a root user.

To execute the data collection command for logical host use:

1. Mount the shared disk.

   The data of the logical host is stored on the shared disk. For the executing node, make sure that the shared disk is mounted and then collect the data.

2. For both the executing and standby nodes, specify in the `jpcras` command the data to be collected and the storage directory for the data, and then execute the command.

   The following shows an example of specifying the command when all information that can be obtained by the `jpcras` command is to be stored in the `/tmp/jp1pc/mgr` directory:

   ```
   jpcras /tmp/jp1pc/mgr all all
   ```

   The data collected by the data collection command can be stored in the specified directory in a compressed format by using either the `tar` or the `compress` command. Example of the file name:

   Data collected by the `jpcras` command: `jpcras`*YYMMDD*`.tar.Z`

   YYMMDD represents the year, month, and date.

   When the `jpcras` command is executed without specifying the `lhost` argument, all the Performance Management data of the physical host and logical host of that node is collected. If Performance Management exists in the logical host environment, the log files on the shared disk are acquired.

   If the `jpcras` command is executed on a node in which the shared disk is not mounted, files on the shared disk cannot be acquired, but the command ends normally without an error.

   Note:

   > Execute the command to collect the data on both the executing node and standby node. To investigate the conditions before and after a failover, the data of both the executing node and standby node is required.

3. Collect the cluster software data.

   This data is required to investigate whether an error occurred in either the cluster software or Performance Management. Collect the data to enable an investigation of the control request, such as a start or stop request from the cluster software to Performance Management, and the results.

When the `jpcras` command is executed, the `jpctool service list -id "*" -host "*"` command is executed internally to collect a list of PFM services and check their operating status. If there is a firewall between the host executing the command and a host on a different PFM system, or if the system is large, it may take an extended period to complete the `jpctool service list -id "*" -host "*"` command. In such a case, by setting the value of the `JPC_COLCTRLNOHOST` environment variable to `1`, you can suppress the `jpctool service list -id "*" -host "*"` command, to reduce the time required to complete the command.

For details on the `jpcras` command, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

(3) Checking information about the operation

Check the information about the operation when an error occurs and record the information. You also need to check the following information:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, the OS version, host name, and PFM - Manager and PFM - Agent or PFM - RM configuration)
- Whether the error is replicable
- When logged on from PFM - Web Console, the Performance Management user name at logon

(4) Collecting error information

You need to obtain the following error information:

- Messages output to the console, if the error occurred during command execution

(5) Collecting other information

You also need to collect the following information:

- The command arguments that were specified, if the error occurred during command execution

14.5.3 Data collection procedure (in PFM - Web Console)

(1) Executing the data collection command

Use the `jpcwras` command to collect the data needed to determine the cause of an error. Note that the user who executes the procedures described below must be a root user.

To execute the data collection command:

1. Log on to the host where the service whose data you want to collect is installed.
2. Execute the `jpcwras` command, specifying the data to be collected and the storage directory for the data.

   The following shows an example of specifying the command when all information that can be obtained by the `jpcwras` command is to be stored in the `/tmp/jp1pcwebcon` directory:

   ```
   jpcwras /tmp/jp1pcwebcon
   ```

   To gather together the data collected by the data collection command, you can use an archiving tool (such as the `tar` command) and compression tool (such as `gzip` or `compress`) available on the host where the data is collected to archive or compress the specified directory in its entirety.

   For details on the `jpcwras` command, see the chapter explaining the commands in the manual *Job Management Partner 1/Performance Management Reference*.

(2) Collecting error information on the screen

When using a browser with PFM - Web Console, collect hard copies of the following:

- The content of the Web browser window
- Windows on the screen when the application error occurred
- The error dialog boxes

  Also copy the detailed information if the dialog box contains a **Details** button.
- The command line of the terminal when an error occurs during command execution.

14.6 Restoring the Performance Management system

This subsection describes the procedure for using the backup file to restore Performance Management to its normal status when an error occurs in the Performance Management server.

Note:

When restoring from a backup file, make sure that you use the same version of the product.

There are two methods for restoring Performance Management to its status before an error occurred.

- For an error related to changes in the configuration

  This procedure is used when an error occurs after changing the parameters or configuration, or when inconsistencies occur in the database storing the performance data or event data.

  Restore the system by restoring, from the backup file, the definition information for the service where the error occurred, and the data model definition file for the performance data or event data.

- For a serious error such as disk failure

  This procedure is used when there is a possibility of wide-ranging damage to the Performance Management files due to a physical disk failure, or when the procedure for an error related to changes in the configuration fails to restore the Performance Management system.

  Reinstall or set up Performance Management again.

  Next, restore the system by restoring, from the backup file, all definition information, performance data, and event data for Performance Management.

Point:

When changing the system configuration or updating the Performance Management version, it is recommended that a backup of the various definition information be obtained. Because performance data and event data are constantly updated, we recommend that you make regular backups in case of a disk failure. Performance Management provides commands for backing up performance data and event data.

For details on obtaining backups, see *8. Backing Up and Restoring Data*.

14.6.1 Restore procedure for an error related to changes in the configuration

Use the following procedure to restore Performance Management when there is an error related to changes in the configuration.

(1) Stopping services

Stop all Performance Management program services.

For details on stopping a service, see *1.3 Stopping services*.

(2) Checking the consistency of and restoring the service definition information

Compare the service definition information on the target host and the backed-up service definition information to check for any inconsistencies. Save any files on the target host that are different, and then restore the backed-up service definition information.

For details on the service definition information to be restored, see *8.3.3 Backing up and restoring service definition information*.

(3) Checking the consistency of and restoring the performance data and event data

Compare the data model definition files on the target host and the backed-up data model definition files to check for any inconsistencies. Save any files on the target host that are different, and then restore the backed-up data model definition files.

The following table shows the data model definition files that must be compared and restored.

OS	Type	File name
In Windows	PFM - Manager	*installation-folder*\mgr\store*.DAT
		installation-folder\agt0\store*.DAT
	PFM - Agent and PFM - RM	*installation-folder**xxxx*[#1]\store*.DAT
		*installation-folder**xxxx*[#1]\store*instance-name*[#2]*.DAT
In UNIX	PFM - Manager	/opt/jp1pc/mgr/store/*.DAT
		/opt/jp1pc/agt0/store/*.DAT

OS	Type	File name
	PFM - Agent and PFM - RM	/opt/jp1pc/*xxxx*#1/store/*.DAT
		/opt/jp1pc/*xxxx*#1/store/*instance-name*#2/*.DAT

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

Folders when running in an instance environment. One folder is created for each instance.

Note:

If the Master Store, Agent Store, or Remote Monitor Store service is started when the comparison check reveals an inconsistency, the Store database becomes invalid. In this case, use the following procedure to fix the Store database.

1. Stop the Master Store, Agent Store, or Remote Monitor Store service.
2. Delete all of the following files in the installation directory of the Store database.

   - Files with the extension .DB

   - Files with the extension .IDX
3. Restore the Store database.

   For details on restoring the Store database, see *8.4 Backing up and restoring operation-monitoring data*.

(4) Reconstructing the index file

Execute the following command to reconstruct the index file of the Store database:

In Windows

installation-folder\bin\jpcmkindex *xxxx*#1 [-lhost *logical-host-name*#2]

In UNIX

/opt/jp1pc/bin/jpcmkindex *xxxx*#1 [-lhost *logical-host name*#2]

#1

xxxx indicates the service key of each PFM - Agent or PFM - RM. For details on service keys of each PFM - Agent or PFM - RM, see the description of the naming rules in an appendix of the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

#2

To specify the service of the logical host environment, specify the `-lhost` option. If this option is omitted, the physical host is temporarily set.

The following table lists the command return values. If the command does not terminate normally, follow the solutions in the table to review the command, and then reconstruct the index file again.

Return value	Command execution result	Solution
0	Terminated normally.	N/A
1	There is an error in the argument setting.	Check, and if necessary, revise the command arguments.
2	You do not have permissions to execute the command.	Check, and if necessary, revise the permissions to execute command.
4	The specified service is not stopped.	Perform the following procedure: 1. Stop the specified service. 2. Delete all of the following files in the installation directory of the Store database. Files with the extension `.DB` Files with the extension `.IDX` 3. Restore the Store database.
5	The specified service is not installed.	Install the specified service.
100	The Performance Management environment is invalid.	Restore the Store database.
102	The specified logical host name is not set up.	Set up the specified logical host name.

Return value	Command execution result	Solution
230	Execution of an internal command failed.	Check for the following problems: • The memory or hard drive size is insufficient • The limit on the number of processes has been exceeded Note: If the return value is 230 even after checking and re-executing the command, the Store database must be restored.
255	An index creation error occurred.	Delete all of the following files in the installation directory of the Store database: • Files with the extension `.DB` • Files with the extension `.IDX`

Legend:

N/A: Not applicable

Note:

For details on restoring the Store database, see *8.4 Backing up and restoring operation-monitoring data*.

(5) Starting services

Start the Performance Management program services and confirm that the service starts normally.

For details on starting the services, see *1.2 Starting services*. Use the `jpctool service list` command to check the service status. For details on checking the service status, see *1.6 Checking the status of service operations*.

(6) Checking operations

Lastly, make sure that the trouble has been resolved. Check whether the following items are normal:

- Check whether performance data can be collected

  Run Performance Management for more than twice the length of the collection interval for performance data to confirm that performance data can be collected without a problem.

  For details on the collection interval of performance data, see *4.1.1 Modifying the recording options for performance data*.

- Check whether there is a problem with the data in the Store database

  Export the data of the Store database to a text file and check whether there is a

problem with the data. Use the `jpctool db dump` command to export the data in the Store database to a text file.

For details on the `jpctool db dump` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

- Check the report and alarm definitions

  Check whether there is a problem with the report or alarm definitions. Use PFM - Web Console to check the report and alarm definitions.

  For details on the report definition, see *5. Creation of Reports for Operation Analysis*. For details about the alarm definition, see *6. Monitoring Operations with Alarms*.

14.6.2 Restore procedure for a serious error related to a disk failure

Use the following procedure to restore Performance Management when there is a serious error related to a disk failure.

(1) Uninstallation

Uninstall the Performance Management program.

For details on how to uninstall the Performance Management program, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Reinstallation

Reinstall the Performance Management program.

For details on how to reinstall the Performance Management program, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(3) Setup

Set up the Performance Management program again. During setup, use the instance name and physical host name used in the environment before the error occurred.

For details on how to set up the Performance Management program, see the chapter that describes installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(4) Restoring definition information

Restore the backed-up service definition information.

For details on the service definition information to be restored, see *8.3.3 Backing up and restoring service definition information*.

(5) Restoring performance data and event data

Restore the backed-up Store database that contains performance data and event data.

For details on restoring the Store database, see *8.4 Backing up and restoring operation-monitoring data*.

(6) Starting services

Start the Performance Management program services and confirm that the services start normally.

For details on starting the services, see *1.2 Starting services*. Use the `jpctool service list` command to check the service status. For details on checking the service status, see *1.6 Checking the status of service operations*.

(7) Restoring the report and alarm table definition information

Restore the backed-up report and alarm table definition information.

For details on restoring the report definition information, see *8.3.1(2) Restoring report definition information*. For details on restoring the alarm definition information, see *8.3.2(2) Restoring alarm definition information*.

(8) Checking operations

Lastly, make sure that the trouble has been resolved. Check whether the following items are normal:

- Check whether performance data can be collected

  Run Performance Management for more than twice the length of the collection interval for performance data to confirm that performance data can be collected without a problem.

  For details on the collection interval of performance data, see *4.1.1 Modifying the recording options for performance data*.

- Check whether there is a problem with the data in the Store database

  Export the data of the Store database to a text file and check whether there is a problem with the data. Use the `jpctool db dump` command to export the data in the Store database to a text file.

  For details on the `jpctool db dump` command, see the chapter that describes commands in the manual *Job Management Partner 1/Performance Management Reference*.

- Check the report and alarm definitions

  Check whether there is a problem with the report and alarm definitions. Use PFM - Web Console to check the report and alarm definitions.

  For details on the report definition, see *5. Creation of Reports for Operation*

Analysis. For details about the alarm definition, see *6. Monitoring Operations with Alarms*.

- Check the binding of the alarm table

  Check the binding of the alarm table and bind it as necessary.

  For details on binding the alarm table, see *6.6.1 Changing the association between an alarm table and a monitoring agent*.

Appendixes

A. Version Changes
B. Glossary

A. Version Changes

A.1 Changes in 09-00

- PFM - RM has been added to the Performance Management product to support remote monitoring.
- Events that occur in a Performance Management service can now be reported as JP1 system events or agent events.
- The product name display function has been added. Service keys and IDs can now be displayed and specified in a new format.
- A new command syntax compatible with pre-08-11 commands has been added. A unified option specification format has been introduced.
- Summaries of the entire system status and the latest operating status of services can now be checked in the Summary View.
- The tiling display function has been added. Multiple historical report graphs can now be displayed as thumbnails.
- The search fields function has been added. Information on an item to be monitored can now be found by searching for a keyword when setting an alarm or report.
- The Quick Guide function has been added. Reports can now be displayed without performing a conventional report definition procedure. The alarm definition procedure has been simplified.
- A definition for displaying a report can now be edited from the report display window.
- The procedure for changing the name of a host running a Performance Management product has been simplified.
- PFM - Manager, PFM - Base, and PFM - Web Console services can now be started and stopped in a synchronized manner.
- Internet Explorer 7.0 and Firefox 3 have been added as monitoring console browsers.
- Mozilla has been removed as a monitoring console browser.
- An agent for monitoring a virtual environment has been added.
- Remote monitors for Windows, UNIX, Oracle, and Microsoft SQL Server have been added.
- The name *solution set* has been changed to *monitoring template*.

- The alarm table version in the monitoring template for the health check agent has been changed from 8.11 to 8.50 and 09.00.
- The alarm table in the monitoring template for the health check agent has been renamed to the following:

  `PFM Health Check Template Alarms`
- Windows Server 2008 is now supported.
- A report graph can now be displayed with time adjustment.
- A bookmark or combination bookmark can now be specified for the `jpcbdef` command.
- A PFM service that has stopped abnormally can now be restarted automatically.
- More than one alarm table can now be bound to a monitoring agent.
- Performance Management can now be used in an environment where there are multiple hosts with the same name.
- The Performance Management setup procedure has been simplified.
- PFM - Web Console can now be used in a UNIX environment.
- A description required for installing a Solaris patch for version 09-00 has been added.
- The number 4.0 has been added to the data model version of the health check agent. Accordingly, the `PI_HAVL`, `PD_HOST`, and `PI_SYS` records have been added.
- The number 8.50 has been added as the alarm table version in the monitoring template of the health check agent. Accordingly, the `Host Status Change` and `Host Not Available` alarms have been added.
- `Host Availability (4.0)`, `Hosts Availability (4.0)`, `Hosts Status (Real-Time) (4.0)`, and `System Summary (4.0)` have been added as reports in the monitoring templates of the health check agent.

A.2 Changes in 08-11

- The health check function now supports monitoring of the operation status of a monitoring agent and the host running the monitoring agent.
- The tree view of PFM - Web Console has been improved.
- Reports can now be output in HTML format from the GUI.
- Firefox is now available as a monitoring console browser.
- A timeout time can now be specified for automatic logout, which occurs if no user operation or automatic update occurs within a specific time interval.

- PFM - Agent-specific properties can now be distributed as a batch.
- A registered report in the bookmarks and a combination report in the combination bookmarks can now be output from a command.
- Store version 2.0 is now supported.
- The `jpcrpt` command can now output a report in HTML format.
- Multiple reports can now be displayed in the same window.
- The operation log can now be output.
- File permissions have been enhanced under Windows.
- PFM - Manager is now available for HP-UX (IPF).
- PFM - Web Console is now available for Linux.
- UTF-8 can be specified in the LANG environment variable for Linux.
- Properties can now be distributed to agents.
- Reports registered in bookmarks and combination bookmarks can now be displayed as a drilldown report.
- A report definition can now be displayed from the Reports tree.
- A report can now be registered in a bookmark from the Agents tree.
- A monitoring agent associated with an alarm table can now be displayed.

A.3 Changes in 08-00

- PFM - Base has been added as the monitoring base.
- PFM - Web Console has been added as the monitoring console server.
- The status management function (Status Server service) has been added. This function manages the statuses of Performance Management services.
- The log file trapping function has been added. This function can convert the common message logs for Performance Management to JP1 events.
- The wrap-around file (`jpclogw`) method has been added as a storage method for common message logs output by Performance Management. The user can select one of the following two methods:
  - Sequential file (`jpclog`) method (conventional method)
  - Wrap-around file (`jpclogw`) method
- The Windows event log can be logged using the `jpcras` command.

A.4 Changes in 07-10

- For the JRE for the PFM-Manager's View Server, you can now specify a JRE installed in a location of your choosing.

A.5 Changes in 07-00

- Cluster systems are now supported.
- The OSs supported by PFM - Manager and PFM - View have been changed as follows:

Program name	Changes
PFM - Manager	Windows NT and Windows Server 2003 have been added.
PFM - View	Windows NT and Windows Server 2003 have been added.

- Operations in a network environment connected to multiple LANs are now supported.
- Starting of PFM - Agent in stand-alone mode is now supported.
- The installation log file to which installation failures are output has been added.
- The settings for specifying whether to collect PI records, and for specifying the collection interval, can now be changed.
- Index file creation processing for Store databases running during service startup is now performed during upgrade installation and database restoration.
- The monitoring time can now be set for report output processing.

B. Glossary

action

An action is something that is automatically executed by Performance Management when monitored data reaches a threshold. An action might be any of the following:

- Sending one or more emails
- Executing one or more commands
- Issuing one or more SNMP traps
- Issuing one or more JP1 events

Action Handler

One of the services provided by PFM - Manager or PFM - Base. This service executes an action.

administrative tools

Various commands or functions in the GUI that are used to verify the service status or perform operations on performance data. The following can be done:

- Configuring a service and displaying the status
- Backing up and restoring performance data
- Exporting performance data to a text file
- Deleting performance data

Administrator Console

A command prompt provided by Performance Management to execute commands that require administrator privileges when the UAC feature is enabled in Windows Server 2008.

agent

A PFM - Agent or PFM - RM service that collects performance data.

Agent Collector

One of the services provided by PFM - Agent. This service collects or evaluates performance data by using thresholds set in alarms.

agent monitoring

An operating style in which the operating status of a server is monitored after an agent is installed on the server. You must install an agent on the target server, but you can monitor the operating status of the server by using a rich range of items.

Agent Store

One of the services provided by PFM - Agent. This service stores performance data. The Agent Store service uses a database to record performance data. Each Agent Store service corresponds to a PFM - Agent.

alarm

Information that defines an action or event message executed when monitored data reaches a threshold.

alarm table

A table that includes one or more alarms for which the following information is defined:

- Object to be monitored (for example, process, TCP, or Web service)
- Information to be monitored (for example, CPU usage or number of received bytes per second)
- Conditions to be monitored (threshold)

baseline

An object that serves as historical reference data for a report. You can display a baseline as reference data on the same graph as a combination report.

binding

To associate an alarm with an agent. When an alarm and agent are bound, a user can be notified when performance data collected by the agent reaches the threshold defined in the alarm.

cluster system

Cluster systems are used to link multiple servers and run them as a single system. There are two types of cluster systems: HA (High Availability) cluster systems, and load-balancing cluster systems.

HA cluster systems are cluster systems that provide high availability. The objective of an HA cluster system is to be able to continue operations even if a failure occurs. If a failure occurs on a server that is executing a job, a different server that has been standing by can continue the job processing. This can prevent the transaction from being suspended when a failure occurs, and improves availability.

Load-balancing cluster systems balance and execute the processing load among multiple nodes. The objective is to increase the processing performance by balancing and executing the processing load among multiple nodes. Even if a failure occurs and the node stops, the availability of the system can be enhanced by switching processes to a different node.

This manual uses the term *cluster system* (by itself) to refer to an HA cluster system.

combination bookmark

An object that stores and manages multiple registered reports and baselines. You can display a combination report from a combination bookmark.

combination report window

A report window in which a registered report in a combination bookmark is displayed together with a baseline.

Correlator

One of the services provided by PFM - Manager. This service controls event sending between services. The service evaluates alarm statuses and, if a status exceeds a threshold, sends an alarm to the Trap Generator service and PFM - Web Console.

data group

A data collection that collects records at one time. One or more records exist in a single data group.

data model

A generic term for records or fields that each PFM - Agent or PFM - RM has. Data models are managed by version.

database ID

An ID, given to each record in PFM - Agent and PFM - RM, that indicates the database where records are stored. A database ID indicates the type of record stored in the appropriate database. The database IDs are as follows:

- PI

  Database for records of the PI record type.

- PD

  Database for records of the PD record type.

device ID

An identifier containing characters (1-255 bytes) that indicate the host on which this service has been started in the Performance Management system. A device ID is one part of a service ID.

drilldown report

Report that is associated with a report or a field of a report. A drilldown report is used to display detailed or related information for a particular report.

executing node

The node that is executing jobs in each server system that makes up the cluster system (a node whose logical host is active).

failover

To take over server job-execution processing from the executing node to the standby node when a failure occurs in the cluster system.

field

An item (a column) in a record related to one type of performance data (such as the CPU usage percentage), which can have one or more pieces of performance data associated with it.

function ID

A one-byte identifier that indicates the function type for services of Performance Management programs. A device ID is one part of a service ID.

HA cluster system

A cluster system that provides high availability. The objective of an HA cluster system is to be able to continue operations even if a failure occurs. If a failure occurs in a server that is executing a job, a different server that has been standing by can continue the job processing. This can prevent the transaction from being suspended when a failure occurs, and improves availability.

This manual uses the term *cluster system* (by itself) to refer to an HA cluster system.

health check

A function that monitors the operating status of the following services and hosts:

- PFM - Agent or PFM - RM services
- Hosts where PFM - Agent or PFM - RM is running
- Hosts monitored by PFM-RM

This function is provided by PFM - Manager.

health check agent

An agent that monitors the operating status of the following services and hosts:

- PFM - Agent or PFM - RM services
- Hosts where PFM - Agent or PFM - RM is running
- Hosts monitored by PFM-RM

historical report

This type of reports display the operating status of the monitored target from past to present.

instance

This manual uses the term *instance* as follows:

- To indicate the format of a record

  A record that is recorded in a single line is called a *single-instance record*, a record that is recorded in multiple lines is called a *multi-instance record*, Each line in a multi-instance record is called an *instance*.

- To indicate the startup method of PFM - Agent and PFM - RM

  An agent monitoring a monitoring target on the same host by using a single agent is called a *single-instance agent*. An agent monitoring a monitoring target on the same host by using multiple agents is called a *multi-instance agent*, Each agent service of the multi-instance agent is called an *instance*.

instance number

An identifier that is a one-byte control number used by internal processing. A device ID is one part of a service ID.

lifetime

The period in which the integrity of performance data collected in each record is assured.

load-balancing cluster system

A system that balances and executes the processing load among multiple nodes. The objective is to increase processing performance by balancing and executing the processing load among multiple nodes. Even if a failure occurs and the node stops, the availability of the system can be enhanced by switching processes to a different node.

logical host

A logical server that is the execution environment for JP1 during operation on a cluster system. A system is switched between logical hosts when a failure occurs. A logical host has a dedicated IP address, and that IP address is taken over when failover occurs. Therefore, even if the physical server is switched due to a failure, clients can continue to access the same IP address and the system appears as if a single server were always working.

Master Manager

One of the services provided by PFM - Manager. This is the main service PFM - Manager provides.

Master Store

One of the services provided by PFM - Manager. This service manages the alarm events issued from each PFM - Agent. The Master Store service uses a database to hold the event data.

monitoring template

Defined alarms and reports prepared for PFM - Agent and PFM - RM. By using a

monitoring template, you can easily monitor the operation status of PFM - Agent and PFM - RM without using complex definitions.

multi-instance agent

An Agent using a method that monitors monitoring targets on the same host by using multiple agents.

-> See *Instance*

multi-instance record

A record recorded in multiple lines. This record has a unique ODBC key field.

-> See *Instance*

Name Server

One of the services provided by PFM - Manager. This service manages service configuration information in a system.

ODBC key field

The ODBC key field is required when you use SQL to utilize the record data stored in the Store database in PFM - Manager or PFM - Base. For the ODBC key field, there are two types of keys; one is common to all records and the other is unique to each record.

open interface

A function that can link with JP1/IM or with a product compliant with ODBC or SNMP.

PD record type

-> See *Product Detail record type*

performance data

Operation status data for the resources collected from the system being monitored.

Performance Management

A generic term for the set of software required for monitoring and analyzing problems regarding system performance. Performance Management consists of the following five program products:

- PFM - Manager
- PFM - Web Console
- PFM - Base
- PFM - Agent
- PFM - RM

Performance Management ODBC driver

By including this driver, you can access the data of the Agent Store and Remote Monitor Store services from Microsoft ODBC-compliant application programs.

PFM - Agent

One of the Performance Management program products. PFM - Agent corresponds to the agent monitoring function. There is a different type of PFM - Agent for applications, databases, and OSs. PFM - Agent has the following functions:

- Monitoring performance of the monitoring target
- Collecting and logging data about the monitored target

PFM - Base

One of the Performance Management program products. This provides base functions for monitoring operations in Performance Management. PFM - Base is a prerequisite product for running PFM - Agent and PFM - RM. PFM - Base has the following functions:

- Management tools such as various commands
- Common functions required for linking Performance Management with other systems

PFM - Manager

One of the Performance Management program products. PFM - Manager corresponds to the manager function. PFM - Manager has the following functions:

- Managing program products of Performance Management
- Managing events

PFM - Manager name

A name for identifying a field stored in the Store database. A PFM - Manager name is used in cases such as specifying a field by using a command.

PFM - RM

One of the Performance Management program products. PFM - RM corresponds to the remote monitoring function. There is a different type of PFM - RM for applications, databases, and OSs. PFM - RM has the following functions:

- Monitoring performance of the monitored target
- Collecting and logging data about the monitored target

PFM - View name

A synonym for PFM - Manager name. This name is more intuitive than the PFM - Manager name. For example, the PFM - View name `Record Type` is used for the

PFM - Manager name `INPUT_RECORD_TYPE`. A PFM -View name is used in cases such as specifying a field on the PFM - Web Console GUI.

PFM - Web Console

One of the Performance Management program products. PFM - Web Console provides Web application server functionality to centrally monitor a Performance Management system by using a browser. PFM - Web Console has the following functions:

- GUI display
- Integrated monitoring and management function
- Defining reports and alarms

physical host

The environment specific to each server that makes up a cluster system. The physical host environment cannot be taken over to another server when failover occurs.

PI record type

-> See *Product Interval record type*

primary host name

The name of the host running the group agent. A group agent monitors multiple objects as a batch, so the name of the host where the object representing the group agent is located is used as the agent name.

The name of the host running PFM - RM is used as the agent name for the default `All` group agent.

Product Detail record type

A record type that stores the performance data indicating the system status at a certain point, such as detailed information on currently running processes. The PD record type is used to display the following system statuses at a certain point:

- Operating status of the system
- Currently used file system space

product ID

A one-byte identifier that indicates which Performance Management program product provides the appropriate Performance Management program service is. The product ID is one part of a service ID.

Product Interval record type

A record type that stores performance data covering a certain time (interval), such as the number of processes per minute. The PI record type is used to analyze the following system statuses or system trends that change over time:

- Changes in the number of system calls that occurred within a certain time
- Changes in used file system space

realtime report

A report that indicates the current status of a monitoring target.

record

The format in which the collected performance data is stored. The type of record depends on each database of the Store database.

registered report

A report registered together with display conditions and agent information using the bookmark function. Once a report is registered, it is a straightforward process to display it.

Remote Monitor Collector

One of the services provided by PFM - RM. This service collects or evaluates performance data by using thresholds set in alarms.

Remote Monitor Store

One of the services provided by PFM - RM. This service stores performance data. The Remote Monitor Store service uses a database to record performance data. Each Remote Monitor Store service corresponds to each PFM - RM.

remote monitoring

An operating style in which operating status of a server is monitored from a remote host without installing an agent on the server. Installation of an agent on the server is not necessary, so it is convenient when you start operation monitoring for already running systems. Items to be monitored are relatively fewer than agent monitoring, but you can collect and manage performance data of multiple monitored systems by using one instance of PFM - RM.

report

Definitions that define the information when the performance data collected by PFM - Agent or PFM - RM is graphically displayed. The following information is defined:

- Records to be displayed in the reports
- Items of performance data
- Display format of the performance data (for example, a table or graph)

series group

A way of grouping the objects in a combination bookmark by their display format. You can assign series groups when editing a combination bookmark.

service ID

A unique ID given to the service of a Performance Management program. When you use a command to verify the system configuration of Performance Management or to back up the performance data of an individual agent, specify the service ID for the Performance Management program that will execute the command. The service ID format differs depending on the settings of the product name display function. For details on the service ID format, see the chapter that describes the Performance Management functions in the manual *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

single-instance agent

An agent using a method that monitors a monitoring target on the same host by using a single agent.

-> See *Instance*.

single-instance record

A record that is recorded in one line. This record does not have a unique ODBC key field.

-> See *Instance*.

stand-alone mode

A state in which PFM - Agent or PFM - RM starts by itself. You can still collect the performance data by starting only PFM - Agent or PFM - RM even when the Master Manager service and the Name Server service of PFM - Manager cannot run due to an error or other reasons.

standby node

A node that is standing by to be able to take over a job if the executing node fails, in each server system that makes up a cluster system.

Store database

A database that stores performance data collected by the Agent Collector and Remote Monitor Collector services.

Trap Generator

One of the services provided by PFM - Manager. This service issues SNMP traps.

UAC

UAC stands for User Account Control. In Windows Server 2008, even if you log on as a management user, administrator privileges are not granted. If you try to execute a program that requires administrator privileges, the UAC pop-up window is displayed asking you to elevate the privileges.

UAC pop-up

A pop-up window asking you to elevate the privileges when the UAC feature is enabled in Windows Server 2008. If you elevate the privileges, the program you tried to execute will start, having administrator privileges.

View Server

One of the services provided by PFM - Manager. This service connects PFM - Web Console and PFM - Manager.

WRP

WRP stands for Windows Resource Protection. Files protected by WRP cannot be deleted or modified. WRP is a feature independent from UAC, so even if you have administrator privileges, you cannot delete or modify the files.

Index

Symbols

<ex-product-detail> tag 139
<ex-product-interval> tag 138
<ex-product-log> tag 139

A

abbreviations defined v
abnormal status 86
Action Handler 800
Action Handler label 332, 334
actions 278
    glossary definition 800
    notes on executing 298
    possible when alarm status changes 294
    setting 294
adjusting time 685
administrative tool 800
Administrator Console 800
administrator user permission 46
Agent Collector 800
Agent Collector service startup initialization file 155
agent event 386, 389
agent for PFM - Agent 72
agent monitoring 800
Agent Store 801
Agent Store service
    notes on abnormal stops 168
agents 800
    Agent for PFM - Agent 72
    associating with alarm 346
    changing association with alarm table 314
    checking agent status 81
    checking connection to alarm table 354
    component of agent tree 71
    displaying properties 98
    displaying those bound to alarm table 318
    distributing properties in batch 100
    editing properties 100
    errors related to connections 741
    integrated management 594
    monitoring 69
    PFM - RM group agent 72
    PFM - RM remote agent 72
    properties 98
    types 72
    types supporting summary display 87
    unbinding alarm tables 350
    usable types 72
agents tree 70
    component 71
    creating 73
alarm condition-dependent alarm evaluation 379
alarm created by using Quick Guide
    default values 312
alarm damping 363
alarm damping setting-dependent alarm evaluation 383
alarm definition
    backing up and restoring 415
    checking file 337
    creating file 324
    modifying 338
Alarm Definition File Code label 326
Alarm Definition File Version label 326
alarm events
    monitoring via JP1/IM integrated console 631
alarm tables
    associating with monitoring agent 346
    changing association with monitoring agent 314
    checking connection to monitoring agent 354
    checking properties 359
    copying 302, 340
    deleting 305, 342
    displaying bound monitoring agents 318
    exporting 306

glossary definition 801
importing 307
unbinding with monitoring agent 350
alarms 278
Alarm Name label 327
Alarm Table Name label 327
associating with report 301
checking status 84
condition 292
copying 302
creating 288
creating using Quick Guide 309
deleting 305, 343
displaying associated reports 393
displaying properties (definition) 320
editing 304
event 278
events 386, 389
glossary definition 801
message 288
name 288, 391
notes on creating 362
notes on evaluating 378
property 393
starting monitoring by using 355
status 85
table 278
table name 287
troubleshooting definitions 749
using to start monitoring 319
using to stop monitoring 319, 357
associating
alarm table with monitoring agent 346
associating report with alarm 301
attributes
of JP1 events 633
authentication mode
user account 58
automatic refresh interval 32
automatic restart functionality 720
configuring 722
service startup units 721
using 726
automatic service restart
prerequisite conditions 720

B

backing up 408
event data 448
info. to back up 408
methods 408
performance data 451
performance data, partial (Store 2.0) 454
backing up and restoring
alarm definition information 415
cluster system 596
performing 596
report definition information 414
backup data
converting data model (Store 2.0) 159
importing (Store 2.0) 158
baseline 180, 801
registering in combination bookmark 251
batch distribution of properties 100
binding 278, 314, 801
bookmark folder
deleting 227
renaming 225
bookmark properties
checking 228
bookmarks
adding folder 224
backing up and restoring definitions 438
creating 220
deleting 227
renaming 225, 226
term defined xv
browser
operating alarm by using 314

C

changing
cluster system configuration (UNIX) 567
cluster system configuration (Windows) 510
password 64
permissions of user account 66
changing configuration
NNM linkage 659

Check Value Exist label 328
checking
    agent status 81
    alarm status 84
    alarm table properties 359
    bookmark properties 228
    service operating status by browser 31
    service operating status by command 28
cluster configuration
    designing 463
cluster software 546
cluster system 460, 589, 593, 594, 595, 801
    backup and restore 596
    configuration 474
    configuration (UNIX) 531
    configuration changing (UNIX) 567
    configuration changing (Windows) 510
    failover 597
    failure recovery 603
    note 605
    operation 589
    operation design 473
    overview 460
    realtime monitoring by alarm 596
    status management 716
collecting
    dump (Windows Server 2008) 778
collecting and managing
    operation management 595
Collection Interval property 120
Collection Offset property 121
columns
    specification rules for ODBC driver 682
combination bookmark 802
    registering baseline in 251
combination report window 802
combination reports
    displaying 247, 253
    examples of real-world use 254
    notes on 271
    preparing to display 250
    whether displayable 247
Command label 330
commands
    operating alarm by using 346
    setting alarm by using 324
    troubleshooting 743
common message log 754
component
    agents tree 71
component version 190
condition
    alarms 292
Condition label 329
config.xml 270
configuration
    cluster system 474
    cluster system (in UNIX) 531
    MIB object 665
configuring
    health check function 691
    log output method 729
    status management function 711
content
    MIB object 665
control command
    PFM - Manager 546
    PFM - Web Console registered in cluster software 555
conventions
    abbreviations v
    diagrams xi
    fonts and symbols xii
    KB, MB, GB and TB xv
    mathematical expressions xiv
    meaning of bookmark xv
    meaning of directory xv
    meaning of installation directory xv
    version numbers xvi
copying
    alarm 303
    alarm table 302, 340
    reports 205
Correlator 802
counting range for summary display 95
counting unit for summary display 95
creating
    alarm definition file 324

alarm tables 287
alarms 288
new report 184
notes on creating reports 269
report 595
report by using browser 187
report by using command 217
report by using existing report 184
report by using Quick Guide 212
report, process flow 184
CSV format 264
outputting event history 404

D

data collection procedure 778
data configuration
designing 472
data group 802
data model 802
converting for backup data (Store 2.0) 159
performance data stored after upgrade 176
version 190
data to be collected in event of trouble 765
database ID 802
default values
for reports with Quick Guide 215
of alarm created by using Quick Guide 312
definition information that needs to be backed up 413
deleting
alarm 306, 343
alarm tables 305, 342
bookmark 227
bookmark folder 227
folders, bookmarks, reports 227
report folder 209
report from bookmark 228
reports 209
unnecessary reports 218
user account 67
deleting and setting
properties 120
Description property 120
designing
cluster configuration 463
data configuration 472
failover policy 473
network configuration 470
Detail Records 119
detecting problems by linking with the integrated system monitoring product 729
device ID 802
diagram conventions xi
directory
term defined xv
disabling alarm 357
disk failure
restoration procedure 791
disk space 153, 164
checking for event data 164
for performance data 153
notes when insufficient 168
display condition for event monitor window
setting 395
display conditions
setting for report 240
display format 198
reports 181
display format of combination report
setting 251
display item
event monitor window 389
display period 195
displaying
agent properties 98
alarm properties (definition) 320
combination report 247
displaying agents bound to alarm table 318
drilldown reports 243
event history 397
events 385
info. about Store services (Store 2.0) 160
latest event 386
latest event info. 386
list of alarm tables 359
New Report window 188
notes on displaying reports 269
reports 235
distributing

agent properties in batch 100
drilldown reports 201
displaying 243
glossary definition 802
dump
collecting (Windows Server 2008) 778

E

E-mail Address label 332
E-mail label 330
editing
agent properties 100
alarms 304
reports 205
enabling alarm 355
environment directory 472
erasing
event data 165
performance data 155
errors
data to collect (UNIX) 772
data to collect (Windows) 765
handling 734
list of different types 735
related to alarm definitions 749
related to collecting and managing performance data 750
related to commands 743
related to lining to other programs 751
related to Performance Management 744
related to report definitions 746
related to setup or starting services 736
relating to agent connections 741
restoration for disk failure 791
event data
backing up and restoring 448
checking disk space 164
erasing 165
exporting 163
managing 162
event history
displaying 397
outputting in CSV format 404
event history window 397, 400
Event ID label 334
event log file 754
event monitor window 386
display item 389
events
alarms 278, 386, 389
changing max. num of records 162
displaying 385
displaying latest info. 386
JP1 event types 612
example
creating definition file for log file trapping 731
detecting problem in PFM - Agent 689
detecting problem in PFM - RM 690
graph 183
list 182
operation monitoring by Performance Management with JP1/IM 609
settings in jpcnnm.ini 654
table 182
using combination reports in real world 254
using health check function 705
Excel 677
executing node 460, 802
execution procedure of data collection command 778
existing report
creating report by using 184
export 152
exporting
alarm tables 306
event data 163
performance data 152
reports 210
reports in CSV or HTML by browser 262
reports in CSV or HTML by command 263

F

failover 460, 803
cluster system 597
failover policy
designing 473
failure recovery
cluster system 603

field 803
field-level drilldown report 201
fields
    filter conditions for report 193
    searching 214
    searching for 192, 293
    setting for a report 190
filter condition 193
folders
    component of agents tree 71
    deleting 227
    for alarms 278
    renaming for bookmarks 225
font conventions xii
function ID 803
functionality for binding multiple alarm tables 314, 346

G

GB meaning xv
general user permission 46
glossary 800
GMT_ADJUST 685
graph 183
    example 183
    rearranging (tiling display) 233
group agent 71

H

HA cluster system 460, 803
health check 803
health check agent 803
health check function 688
    configuring 691
    examples of using 705
historical (multiple agents) 189
historical (single agent) 189
historical report 180, 803
Host Name
    output by jpctool service list command 29
Host Not Available 701, 703, 704
how to check service status 714
how to start 7
how to stop 15
HTML format 265
    outputting event history 404

I

importing
    alarm tables 307
    backup data (Store 2.0) 158
    reports 210
Incomplete 700, 704
information that needs to be backed up 408
inherited information 245
initializing
    settings for Store database 155
inittab 10
installation
    JP1/IM linkage 614
    NNM linkage 648
installation directory
    term defined xv
installing
    PFM ODBC driver 672
instance 803
instance number 804
integrated console
    displaying reports 631
    monitoring with 610
integrated management
    agents 594
integrated scope
    monitoring 631
    monitoring with 610
interval for evaluating alarm 379
Interval Records 119

J

JP/IM
    displaying reports with integrated console 631
JP1 authentication mode 46
JP1 Event label 331
JP1 events 298
    attribute list 633
    prerequisite conditions 613
    types of 612

JP1 system event 612
JP1 user 46
JP1 user event 612
JP1/Base 729
    example of definition file for log file trapping 731
    starting log file trapping function 731
JP1/IM 608, 610
    linking with Performance Management 611
    monitoring with integrated scope 631
JP1/IM integrated console
    alarm event monitoring 631
JP1/IM linkage
    installation 614
    operation monitoring 607
    setup 615
    unsetup 630
jpc_start 10
jpc_start.model 10
jpc_stop 18
jpc_stop.model 18
jpcagt.ini 156
jpcagt.ini.model 155
jpcaspsv output 145
jpcaspsv update 145
jpcasrec output 123
jpcasrec update 123
jpccomm.ini 730
jpcconf db display 160
jpcrdef create 218
jpcrdef delete 219
jpcrdef output 217
jpcspm start 7
jpcspm stop 15
jpctool alarm active 355
jpctool alarm bind 346
jpctool alarm check 337
jpctool alarm copy 340
jpctool alarm delete 342, 343
jpctool alarm export 324, 338, 359
jpctool alarm import 338
jpctool alarm inactive 357
jpctool alarm list 354
jpctool alarm unbind 350
jpctool db clear 155, 165
jpctool db dmconvert 159
jpctool db dump 152, 163
jpctool db import 158
jpctool service list 28
jpcvsvr.ini 58
jpcwstart 12
jpcwstop 19

K

KAVE00182-E 167
KB meaning xv
key fields
    specifying for ODBC key fields 684

L

LANG environment variable 755
language of common message log 754
latest event
    displaying 386
lifetime 804
limitation on number of alarms 362
limitation on number of instances evaluated in alarm 378
linking
    to other programs, troubleshooting 751
list 182
    example 182
load-balancing cluster system 462, 804
local action 283
local disk 472
log file trap 729
log information 754
Log property 120
Log Records 119
logging on
    errors for PFM - Web Console 742
logical host 471, 472, 804
    changing name during operation 517, 574
    name 532
    names 475
logical IP address 475, 532
LOGIF property 121
<logif> tag 128

logoff 26
logon 24
logs
configuring output method 729
example for JP1/Base log file trapping function 731
JP1/Base log file trapping function, starting 731
log information files 755
type of log information 754

M

managing
event data 162
operation monitoring data 115
performance data 116
user account 593
Master Manager 804
Master Store 804
mathematical expressions
conventions xiv
MB meaning xv
message
alarms 288
Message label 334
Message Text label 328
Message Text sub-subsection 332
messages
KAVE00105-E 168
MIB object
configuration 665
content 665
model file 155
modifying
alarm definition 338
monitored object 610
monitoring
agent status 81
agents 69
alarm events from NNM 660
alarm events via JP1/IM integrated console 631
by agents tree 70
by using alarms 314
by using integrated console 610
by using integrated scope 610
for a set value 291
operating status of host running monitoring agent 691
operating status of monitoring agent service 691
starting by using alarm 319
stopping by using alarm 319
stopping by using alarm (command) 357
monitoring template 804
multi-instance agent 805
multi-instance record 805
multi-row record 191

N

name
alarms 288, 391
Name Server 805
network configuration
designing 470
new report
creating 184
New Report window
displaying 188
NNM
term defined 646
NNM linkage
changing configuration 659
installation 648
monitoring alarm events 660
operation monitoring 644
OSs supported 647
setting up 649
unsetup 656
node that can be modified
properties 120
non stand-alone mode
overview 36
normal status 86
Not supported 702, 703, 704
note
cluster system 605
number of alarms that can be registered 362

number of events to be displayed
setting 396
number of records 140

O

ODBC 670
expressions supported by driver 681
OSs for linking 672
using from MS Excel 686
ODBC driver
glossary definition 806
ODBC key field 805
ODBC-compliant operation analysis application 670
open interface 805
OpenView
starting and terminating service for linkage 660
operating alarm
using browser 314
using command 346
operating status of server or agent is Unconfirmed or Not Supported 744
operating statuses
checking 697
operation
cluster system 589
operation design
cluster system 473
operation management data
collecting and managing 595
operation monitoring
linking with Network Node Manager (NNM) 644, 645
linking with the Integrated Management Product JP1/IM 607
operation status log 755
order to start 2
order to stop 5
overview
cluster system 460

P

password 61
changing 64
PD record type 805
performance data 116, 805
backing up and restoring 451
checking disk space for 153
erasing 155
exporting 152
modifying for performance data (Store 1.0) 140
modifying for performance data (Store 2.0) 130
modifying recording options 116
partial backups (Store 2.0) 454
stored after data model upgrade 176
troubleshooting 750
Performance Management 805
linking with JP1/IM 611
ODBC driver (glossary definition) 806
start and stop sequences 2
starting and stopping 589
user 46
Performance Management operation monitoring data that must be backed up 446
performing
backup and restore 596
permission level
selecting 61
permissions
changing for user account 66
for administrators 46
for ordinary users 46
PFM - Agent 806
adding in cluster 510, 567
deleting in cluster 515, 573
installing upgrade in cluster 556
installing upgrade in logical host environment 499
PFM - Base 806
PFM - Manager 806
control command 546
installing and setting up in cluster 476, 533
name (glossary definition) 806
unsetup and uninstallation in cluster 499, 556
PFM - RM 806
adding in cluster 510, 567

deleting in cluster 515, 573
installing upgrade in cluster 556
installing upgrade in logical host environment 499
PFM - RM group agent 72
PFM - RM remote agent 72
PFM - View name 806
PFM - Web Console 807
error data collection 785
installing and setting up in cluster 490, 547
logoff 26
logon 24
logon errors 742
starting from JP1/IM integrated management menu 631
unsetup and uninstallation in cluster 507, 564
PFM authentication mode 46
PFM ODBC driver 670, 672, 673
PFM service automatic restart functionality 720
physical host 471, 807
PI record type 807
PID
output by jpctool service list command 29
Port
output by jpctool service list command 29
prerequisite (health check function) 691
prerequisite conditions
for issuing JP1 events 613
primary host name 807
printing
summary display 97
procedure before setting alarm 282
procedure for creating report
using Quick Guide 212
process flow
for creating report 184
Product Alarm - PA 163
Product Detail record type 807
product ID 807
Product Interval - Day Drawer 143
Product Interval - Hour Drawer 143
Product Interval - Minute Drawer 143
Product Interval - Month Drawer 144
Product Interval - Week Drawer 144
Product Interval - Year Drawer 144
Product Interval record type 807
Product label 327
<product-detail> tag 150
<product-interval> tag 149
<product-log> tag 151
properties 98
agents 98
batch distribution 100
description, setting, and node that can be modified 120
displaying agent properties 98
displaying alarm properties (definition) 320
editing agent properties 100
of bookmarks 228
property
alarms 393

Q

query
executing among multiple agents 685
Quick Guide
creating report 212
creating report by using 212
default values for reports 215
procedure for creating alarm by using 309
procedure for creating report by using 212
setting alarm by using 309
window 310

R

rc.jp1_pc 10
rc.shutdown 19
realtime (single agent) 189
realtime monitoring by alarm
cluster system 596
realtime report 180, 808
rearranging
graphs (tiling display) 233
record 808
<record> tag 126
record type 130
recording options 116
modifying for performance data 116

records
changing max. num. for event data 162
refresh interval 32, 195
registered report 808
displaying in tiling display 229
registering
baseline in combination bookmark 251
remote action 283
remote agent 71
Remote Monitor Collector 808
Remote Monitor Collector service 71
Remote Monitor Collector service startup initialization file 155
Remote Monitor Store 808
Remote Monitor Store service
notes on abnormal stops 168
remote monitoring 808
renaming
bookmark 226
bookmark folder 225
folders and bookmarks 225
report folder 207
reports 208
report definition information
backing up and restoring 414
report folder
deleting 209
renaming 207
report properties
checking 240
report type 189
report-level drilldown report 201
reports 180
associating with alarm 301
associating with another (drilldown) 201
combination reports, display preparation 250
combination reports, displaying 253
copying 205
creating 595
creating bookmarks 220
creating report folder 187
creating with Quick Guide 212
creating, by using browser 187
creating, by using command 217
creating, by using Quick Guide 212
default values for Quick Guide 215
definition troubleshooting 746
deleting 209, 227
deleting from bookmark 228
deleting if unnecessary 218
display format 181
displaying 235
displaying those associated with alarm 393
editing 205
exporting 210
exporting in CSV or HTML by browser 262
exporting in CSV or HTML by command 263
general comments 180
glossary definition 808
importing 210
notes on creation 269
notes on displaying 269
output and customize 217
process flow for creation 184
renaming 207, 208
setting display conditions 240
setting display conditions for fields 193
setting display format 198
setting fields displayed in 190
setting name and type for 188
types of 180
restore procedure for serious error related to disk failure 791
restoring 408
configuration-change error 787
event data 448
performance data 451
restoring system 786
retention conditions 140
modifying for performance data (Store 1.0) 140
modifying for performance data (Store 2.0) 130
retention period 140
default in Store 2.0 175
if files or folders are not deleted 174
root 71
Running 700, 703, 704

S

saving of record to be evaluated in alarm 362
scheduled restart functionality 720
searching fields 214
searching for
    field 293
    fields 192
selecting
    permission level 61
sequential file 760
series group 252, 808
service automatic start script file 9
service automatic stop script file 18
service definition information
    backing up and restoring 415
service ID 809
Service Name
    output by jpctool service list command 29
ServiceID
    output by jpctool service list command 29
services
    checking operating statuses by browser 31
    checking operating statuses by command 28
    error in setup or starting 736
    how to check status 714
    prerequisites for automatic restart 720
    starting 7
    stopping 15
setting
    display condition for event monitor window 395
    display format of combination report 251
    name and type of report 188
    number of events to be displayed 396
setting alarm
    using command 324
    using Quick Guide 309
setting PFM - RM polling 695
setting prior to setting associated report 301
setting up
    JP1/IM linkage 615
    NNM linkage 649
    PFM ODBC driver 673
shared disk 472
single-instance agent 809
single-instance record 809
single-row record 191
size limit
    Store database 167
SNMP trap 298
specification rules for names of columns and tables 682
specifying common key fields 684
SQL
    supported functions 680
stand-alone mode 809
    overview 33
standby node 460, 809
starting
    cautionary notes 33
    JP1/Base log file trapping function 731
    monitoring by using alarm 319, 355
    PFM - Web Console from JP1/IM 631
    sequence for Performance Management system 2
    services 7
    Status Server service 41
    synchronizing PFM Manager, Base, Web Console 22
starting and stopping
    Performance Management 589
Status
    output by jpctool service list command 30
status
    alarms 85
status indicated by agent icon 83
status indicated by folder icon 82
status management function 711
    troubleshooting 718
Status Server service
    starting 41
Stopped 700
stopping
    cautionary notes 33
    monitoring by alarm (command) 357
    monitoring by using alarm 319
    sequence for Performance Management system 2

services 15
synchronizing PFM Manager, Base, Web Console 22
Store database 809
checking size and reorganizing 173
initializing 155
size limit 167
store database storage method 408
summary display 87
counting unit and range 95
printing 97
supported agent types 87
use to check operating status 87
supported expressions 681
supported OS 672
supported SQL functions 680
Switch Alarm Level label 334
symbol conventions xii
Sync Collection With property 121
synchronizing service starting and stopping
PFM - Manager or PFM - Base and PFM - Web Console 22
syntax conventions xiii
syslog file 754
system log 754

T

table 181
alarm 801
alarms 278
example 182
specification rules for ODBC driver 682
table name
alarms 287
TB meaning xv
tiling display 229
registered report 229
time
adjusting 685
for evaluating alarm 362
timing of reporting alarm 384
trace log 755
Trap Generator 809
troubleshooting 735
detecting problems by linking with integrated system monitoring product 729

U

UAC 809
UAC pop-up 810
ulimit 167
unbind alarm table 351
unbinding 314
alarm table bound to monitoring agent 350
Unconfirmed 701, 702, 703, 704
UNIX
data to collect when error occurs 782
unsetup
JP1/IM linkage 630
NNM linkage 656
URL to log on to PFM - Web Console 24
user accounts 46
authentication mode 58
copying and customizing 62
creating for Performance Management 60
deleting 67
editing 64
management method 46
managing 593
setting authentication mode 58
user name 61

V

version changes 796
version number conventions xvi
View Server 810

W

warning status 86
wrap-around file 760
WRP 810

X

XML declaration 125, 147

Reader's Comment Form

We would appreciate your comments and suggestions on this manual. We will use these comments to improve our manuals. When you send a comment or suggestion, please include the manual name and manual number. You can send your comments by any of the following methods:

- Send email to your local Hitachi representative.
- Send email to the following address:
  WWW-mk@itg.hitachi.co.jp
- If you do not have access to email, please fill out the following information and submit this form to your Hitachi representative:

Manual name:	
Manual number:	
Your name:	
Company or organization:	
Street address:	
Comment:	

(For Hitachi use)