

JP1 Version 11

**JP1/Performance Management - Agent Option for
Service Response Description, User's Guide and
Reference**

3021-3-A53-10(E)

Notices

■ Relevant program products

JP1/Performance Management - Manager (For Windows Server 2008 R2, Windows Server 2012 and Windows Server 2016):

P-2A2C-AABL JP1/Performance Management - Manager version 11-10

The above product includes the following:

P-CC2A2C-5ABL JP1/Performance Management - Manager version 11-00

P-CC2A2C-5RBL JP1/Performance Management - Web Console version 11-10

JP1/Performance Management - Manager (For CentOS 6 (x64), CentOS 7, Linux 6 (x64), Linux 7, Oracle Linux 6 (x64), Oracle Linux 7 and SUSE Linux 12):

P-812C-AABL JP1/Performance Management - Manager version 11-10

The above product includes the following:

P-CC812C-5ABL JP1/Performance Management - Manager version 11-10

P-CC812C-5RBL JP1/Performance Management - Web Console version 11-10

JP1/Performance Management - Manager (For AIX V6.1, AIX V7.1 and AIX V7.2):

P-1M2C-AABL JP1/Performance Management - Manager version 11-10

The above product includes the following:

P-CC1M2C-5ABL JP1/Performance Management - Manager version 11-10

P-CC1M2C-5RBL JP1/Performance Management - Web Console version 11-10

JP1/Performance Management - Agent Option for Service Response (For Windows Server 2008 R2, Windows Server 2012 and Windows Server 2016):

P-2A2C-ASBL JP1/Performance Management - Agent Option for Service Response version 11-10

The above product includes the following:

P-CC2A2C-AJBL JP1/Performance Management - Base version 11-10

P-CC2A2C-5SBL JP1/Performance Management - Agent Option for Service Response version 11-10

These products include the parts developed under licenses from other companies.

■ Export restrictions

If you export this product, please check all restrictions (for example, Japan's Foreign Exchange and Foreign Trade Law, and USA export control laws and regulations), and carry out all required procedures.

If you require more information or clarification, please contact your Hitachi sales representative.

■ Trademarks

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

IBM, AIX, DB2, DB2 Universal Database, Lotus and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

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

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

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

Microsoft and Hyper-V are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Microsoft Exchange server is a product name of Microsoft Corporation in the U.S. and other countries.

ODBC is Microsoft's strategic interface for accessing databases.

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

RC4 is either a registered trademark or a trademark of EMC Corporation in the United States and/or other countries.

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

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

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

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

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

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

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

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

2. This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

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

OpenSSL License

/* =====

* Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

*

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

* OF THE POSSIBILITY OF SUCH DAMAGE.

* =====

*

* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

*

* This package is an SSL implementation written

* by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscapes SSL.

*

* This library is free for commercial and non-commercial use as long as

* the following conditions are aheared to. The following conditions

* apply to all code found in this distribution, be it the RC4, RSA,

* lhash, DES, etc., code; not just the SSL code. The SSL documentation

* included with this distribution is covered by the same copyright terms

* except that the holder is Tim Hudson (tjh@cryptsoft.com).

*

* Copyright remains Eric Young's, and as such any Copyright notices in

* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution

* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or

* in documentation (online or textual) provided with the package.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

* 1. Redistributions of source code must retain the copyright

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must display the following acknowledgement:

* "This product includes cryptographic software written by

* Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the routines from the library

* being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from

* the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND

* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or

* derivative of this code cannot be changed. i.e. this code cannot simply be

* copied and put under another distribution licence

* [including the GNU Public Licence.]

*/

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Internet Explorer		Windows(R) Internet Explorer(R)
.NET Framework 3.5		Microsoft(R) .NET Framework 3.5
MSCS		Microsoft(R) Cluster Server
		Microsoft(R) Cluster Service
Windows Server 2008 R2		Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard

Abbreviation	Full name or meaning
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
	Microsoft(R) Windows Server(R) 2016 Standard
Win32	Win32(R)

Windows is sometimes used generically, referring to Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016.

■ Restrictions

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

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

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

■ Issued

Jan. 2017: 3021-3-A53-10(E)

■ Copyright

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

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

Summary of amendments

The following table lists changes in this manual (3021-3-A53-10(E)) and product changes related to this manual.

Changes	Location
The subsection that provides an overview of pausing or resuming a measurement was added.	<i>2.1.6</i>
Windows Server 2016 is now supported as an OS for PFM - Agent Option for Service Response.	<i>3.1.2</i>
The <code>jpcvtaskctl</code> command was added.	<i>11</i>
The following messages have been added: KAVK08026-W, KAVK43000-E, KAVK43001-E, KAVK43002-E, KAVK43003-E, KAVK43004-I, KAVK43005-E, KAVK43006-E, KAVK43007-E, KAVK43008-E, KAVK43009-W, KAVK43010-E, KAVK43011-E, KAVK43015-E, KAVK43016-E, KAVK43017-E, KAVK43018-I, KAVK43019-W, KAVK43020-W, KAVK43021-E, AVK43023-E, KAVK43024-E, KAVK43025-E, KAVK43026-E	<i>12.2, 12.4</i>
The explanation of the following message was changed: KAVK08171-E	<i>12.4</i>
The actions the operator should take for the following messages were changed: KAVK08172-E, KAVK08302-E, KAVK10040-E	<i>12.4</i>
The section that describes how to troubleshoot some problems was added.	<i>13.8</i>

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

Preface

This manual describes the functionality and records of JP1/Performance Management - Agent Option for Service Response.

■ Intended readers

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

- Users who wish to design or construct an operation monitoring system.
- Users who wish to collect internet service performance data.
- Users who wish to define conditions for collecting performance data.
- Users who wish to define reports and alarms.
- Users who wish to use collected performance data to monitor a system.
- Users who wish to consider or take actions for a system based on monitoring results.

Readers of this manual must be familiar with the system being monitored and Internet service protocols, and must have a basic knowledge of the operating systems.

For details about how to design and run systems that use JP1/Performance Management, also see the following manuals:

- *JP1/Performance Management Planning and Configuration Guide*
- *JP1/Performance Management User's Guide*
- *JP1/Performance Management Reference*

■ Organization of this manual

This manual is organized into the parts listed below. This manual can be used as a common reference under the following condition: the host on which JP1/Performance Management - Agent Option for Service Response is installed runs on the Windows operating system. When there are differences in functionality between OSs, this manual provides a separate description for each OS.

Part 1. *Overview*

This part provides an overview of JP1/Performance Management - Agent Option for Service Response.

Part 2. *Configuration and Operations*

This part explains how to install and set up JP1/Performance Management - Agent Option for Service Response. It also explains the definitions for service measurement, starting and stopping, and how to perform operations in a cluster system.

Part 3. *Reference*

This part describes the windows, definition files, monitoring templates, records, commands, and messages of JP1/Performance Management - Agent Option for Service Response.

Part 4. *Troubleshooting*

This part describes the actions to be taken for errors that might occur during operation of JP1/Performance Management - Agent Option for Service Response.

■ Conventions: Fonts and symbols

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

Text formatting	Convention
Bold	<p>Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example:</p> <ul style="list-style-type: none"> • From the File menu, choose Open. • Click the Cancel button. • In the Enter name entry box, type your name.
<i>Italic</i>	<p>Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none"> • Write the command as follows: <code>copy source-file target-file</code> • The following message appears: <code>A file was not found. (file = file-name)</code> <p>Italic characters are also used for emphasis. For example:</p> <ul style="list-style-type: none"> • <i>Do not</i> delete the configuration file.
Monospace	<p>Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none"> • At the prompt, enter <code>dir</code>. • Use the <code>send</code> command to send mail. • The following message is displayed: <code>The password is incorrect.</code>

The following table explains the symbols used in this manual:

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

■ Conventions: Version numbers

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

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

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

Contents

Notices	2
Summary of amendments	8
Preface	9

Part 1: Overview

1	Overview of PFM - Agent for Service Response	21
1.1	Features of PFM - Agent for Service Response	22
1.1.1	Collecting Internet service performance data	22
1.1.2	Collecting performance data according to its characteristics	23
1.1.3	Saving performance data	24
1.1.4	Providing notification of problems in Internet service operations	24
1.1.5	Easily defining alarms and reports	25
1.1.6	Operation in a cluster system	25
2	Functions of PFM - Agent for Service Response	26
2.1	Functions of PFM - Agent for Service Response	27
2.1.1	Measurement of Internet services	27
2.1.2	Measurement of Web transactions	28
2.1.3	Web transaction measurement test	34
2.1.4	Measurement of IE scenarios	36
2.1.5	Measurement of user-defined services	40
2.1.6	Pausing and resuming a measurement	41
2.2	Selecting the type of measurement for Web server monitoring	43
2.3	Overview of collecting and managing performance data	44
2.4	Example of performance monitoring operation	45
2.4.1	Purpose of performance monitoring	45
2.4.2	Determining baselines	45
2.4.3	Definition examples (Measurement of Web transactions)	45
2.4.4	Definition examples (Measurement of IE scenarios)	62

Part 2: Configuration and Operations

3	Installation and Setup	68
3.1	Installation and setup	69
3.1.1	Installation and setup flow	69
3.1.2	Before installation and setup	70

3.1.3	Installation procedure	75
3.1.4	PFM - Agent for Service Response setup procedure	76
3.2	Uninstallation and unsetup	82
3.2.1	Before uninstallation	82
3.2.2	Unsetup procedures	83
3.2.3	Uninstallation procedure	83
3.3	Changing the PFM - Agent for Service Response system configuration	84
3.4	Changing the PFM - Agent for Service Response operation method	85
3.4.1	Changing the performance data storage destination	85
3.4.2	Updating the Store version to 2.0	88
3.4.3	Changing the integrated trace log function settings	90
3.4.4	Interpolating performance data	90
3.5	Backup and restoration	92
3.5.1	Backup	92
3.5.2	Restoration	93
3.6	Settings for browsing manuals in a Web browser	94
3.6.1	Setting required to view manuals	94
3.6.2	Viewing manuals	95

4 Definitions for Measuring Services 96

4.1	Definition procedure	97
4.2	Notes on service measurement definition	98
4.3	Definitions for measuring Internet services	99
4.3.1	Registering passwords	99
4.3.2	Defining measurement conditions	99
4.3.3	Registering certification files	102
4.3.4	Applying the definition information	102
4.4	Definitions for measuring Web transactions	103
4.4.1	Defining Web transactions (creating Web transaction files)	103
4.4.2	Registering passwords	111
4.4.3	Defining measurement conditions	111
4.4.4	Registering certification files	112
4.4.5	Applying the definition information	112
4.4.6	Defining settings for the dynamic session management	113
4.5	Definitions for measuring IE scenarios	116
4.5.1	Performing pre-measurement check on target Web pages	116
4.5.2	Defining IE scenarios (creating IE scenario files)	116
4.5.3	Defining measurement conditions	123
4.5.4	Applying the definition information	124
4.6	Definitions for measuring user-defined services	125
4.6.1	Defining a user-defined service	125
4.6.2	Defining measurement conditions	126

4.6.3	Applying the definition information	127
4.7	Defining measurement conditions in PFM - Web Console	128
4.7.1	Adding the Tasks	129
4.7.2	Deleting the Tasks	130
4.7.3	Setting the Task information	130
4.7.4	Applying the Task information	131
4.7.5	Distributing the Task information	133
5	Starting and Stopping	134
5.1	Starting and stopping PFM - Agent for Service Response	135
5.1.1	List of the PFM - Agent for Service Response services	135
5.1.2	Starting services	136
5.1.3	Stopping services	136
5.1.4	Using commands to start and stop services	137
5.1.5	Starting and stopping the IE probe service using the Windows services	137
5.1.6	Notes about starting the IE probe	139
5.2	Notes on operations	140
5.2.1	Notes on system operation	140
5.2.2	Notes about the functions of PFM - Agent for Service Response	141
5.2.3	Notes on IE scenarios	149
5.2.4	Notes on the navigation	166
6	Operation in a Cluster System	184
6.1	Overview of cluster systems	185
6.1.1	HA cluster systems	185
6.2	Processing at failover	186
6.2.1	Failover when an error occurs	186
6.2.2	Effects of PFM - Manager stopping	186
6.3	Installation and setup	188
6.3.1	Flow from installation to starting operation	188
6.3.2	Before installation	190
6.3.3	Installation	193
6.3.4	Setup	193
6.4	Uninstallation and unsetup	202
6.4.1	Flow of PFM - Agent for Service Response uninstallation and unsetup	202
6.4.2	Unsetting up PFM - Agent for Service Response	203
6.4.3	Uninstallation	206
6.5	Changing the PFM - Agent for Service Response operation method	207
6.5.1	Exporting and importing the logical host environment definition file	207
6.5.2	Changing the definition files of PFM - Agent for Service Response	207
6.6	Notes on operating PFM - Agent for Service Response in a cluster system	208
6.6.1	Notes on using the IE scenarios	208

Part 3: Reference

7 Windows 209

- 7.1 Basic window operations and window transitions 210
 - 7.1.1 Basic window operations 210
 - 7.1.2 Window transitions 210
- 7.2 Web Recorder windows 212
 - 7.2.1 Web Recorder (main) window 212
 - 7.2.2 Create New Web Transaction window 214
 - 7.2.3 Save As window 216
 - 7.2.4 Select Web Transaction window 217
 - 7.2.5 Select Scope window 218
 - 7.2.6 Set Web Transaction Conditions window 218
 - 7.2.7 Properties window 223
 - 7.2.8 Conditions of Variable String window 234
 - 7.2.9 Select Source of Variable String Settings window 237
 - 7.2.10 Conditions of Substitute String window 238
 - 7.2.11 Select Source of Substitute String Settings window 240
 - 7.2.12 Filtering Conditions window 241
- 7.3 IE Recorder windows 242
 - 7.3.1 IE Recorder (main) window 242
 - 7.3.2 Operation Settings window 250
 - 7.3.3 Change Password window 257
 - 7.3.4 IE Recorder Settings window 257
 - 7.3.5 Start Scope Settings window 258
 - 7.3.6 End Scope Settings window 259
 - 7.3.7 Scope List window 259
 - 7.3.8 Replay Report window 260

8 Definition Files 262

- 8.1 List of definition files 263
 - 8.1.1 About specification in XML format 264
 - 8.1.2 Editing the definition files after an upgrade installation to the multi-language edition 265
- 8.2 Probe action condition definition file (esp.conf) 266
 - 8.2.1 Format 266
 - 8.2.2 Definition 267
 - 8.2.3 Example 270
- 8.3 Measurement condition registration file (esptask.xml) 272
 - 8.3.1 Format and definition of the measurement condition registration file 273
 - 8.3.2 Format and definition of measurement conditions (common section) 274
 - 8.3.3 Format and definition of measurement conditions (service-specific condition sections) 275
 - 8.3.4 Example 287

8.4	Web Recorder action condition definition file (wr.conf)	289
8.4.1	Format	289
8.4.2	Definition	289
8.4.3	Example	290
8.5	Web transaction files	291
8.5.1	Format and definition of the overall Web transaction file	291
8.5.2	Format and definition of the Web transaction measurement conditions	292
8.6	Command registration file (espcommand.xml)	308
8.6.1	Format	308
8.6.2	Definition	308
8.6.3	Example	309
8.7	Measurement condition label definition file (esptasklabel.conf)	310
8.7.1	Format	310
8.7.2	Definition	310
8.7.3	Example	311
8.8	IE Recorder action condition definition file (jpcvierec.conf)	312
8.8.1	Format	312
8.8.2	Definition	312
8.8.3	Example	313
8.9	IE scenario files	315

9 Monitoring template 316

Overview of the monitoring template	317
Format of alarm explanations	318
List of alarms	319
FTP Failure	320
FTP Response Time	321
IES Failure	322
IES Replay Time	323
IMAP4 Failure	324
IMAP4 Response Time	325
POP3 Failure	326
POP3 Response Time	327
SMTP Failure	328
SMTP Response Time	329
TCP Failure	330
TCP Response Time	331
WT Failure	332
WT Response Time	333
Format of report explanations	334
Organization of report folders	335
List of reports	338
DHCP Response Time Status	342
DHCP Response Time Status (real-time report)	343

DHCP Response Time Summary	344
DHCP Response Time Trend	345
DNS Response Time Status	346
DNS Response Time Status (real-time report)	347
DNS Response Time Summary	348
DNS Response Time Trend	349
FTP Rate	350
FTP Response Time Status	351
FTP Response Time Status (real-time report)	352
FTP Response Time Summary	353
FTP Response Time Trend	354
FTP Top 10	355
HTTP Rate	356
HTTP Response Time Status	357
HTTP Response Time Status (real-time report)	358
HTTP Response Time Summary	359
HTTP Response Time Trend	360
HTTP Top 10	361
HTTPS Rate	362
HTTPS Response Time Status	363
HTTPS Response Time Status (real-time report)	364
HTTPS Response Time Summary	365
HTTPS Response Time Trend	366
HTTPS Top 10	367
IE Scenario Detail	368
IE Scenario Logged Message	369
IE Scenario Replay Time Status	370
IE Scenario Replay Time Status (real-time report)	371
IE Scenario Replay Time Summary	372
IE Scenario Replay Time Trend	373
IE Scenario Scope Detail	374
IE Scenario Scope Rate	376
IE Scenario Top 10	377
IMAP4 Rate	378
IMAP4 Response Time Status	379
IMAP4 Response Time Status (real-time report)	380
IMAP4 Response Time Summary	381
IMAP4 Response Time Trend	382
IMAP4 Top 10	383
POP3 Rate	384
POP3 Response Time Status	385
POP3 Response Time Status (real-time report)	386
POP3 Response Time Summary	387
POP3 Response Time Trend	388
POP3 Top 10	389
Scope Detail	390
SMTP Rate	391

- SMTP Response Time Status 392
- SMTP Response Time Status (real-time report) 393
- SMTP Response Time Summary 394
- SMTP Response Time Trend 395
- SMTP Top 10 396
- TCP Response Time Status 397
- TCP Response Time Status (real-time report) 398
- TCP Response Time Summary 399
- TCP Response Time Trend 400
- Transaction Detail 401
- User Defined Service Response Time Status 402
- User Defined Service Response Time Status (real-time report) 403
- User Defined Service Response Time Summary 404
- User Defined Service Response Time Trend 405
- Web Transaction Response Time Status 406
- Web Transaction Response Time Status (real-time report) 407
- Web Transaction Response Time Summary 408
- Web Transaction Response Time Trend 409
- Web Transaction Scope Detail 410
- Web Transaction Scope Rate 411
- Web Transaction Top 10 412

10

Records 413

- Data model 414
- Format of record explanations 415
- List of ODBC key fields 417
- Summary rules 418
- List of data types 420
- Field values 421
- Fields that are added only when a record is recorded in the Store database 423
- Common fields 424
- List of records 427
- DHCP (PI_DHCP) 428
- DNS (PI_DNS) 430
- FTP (PI_FTP) 432
- HTTP (PI_HTP) 435
- HTTPS(PI_HTTPS) 439
- IE Scenario(PI_IES) 445
- IE Scenario Overview(PI_IESO) 446
- IMAP4 (PI_IMP4) 449
- Logged Message for IE Scenario(PL_IESM) 452
- POP3 (PI_POP3) 454
- Service Summary Interval (PI_PI) 457
- SMTP (PI_SMTP) 458
- TCP (PI_TCP) 461
- User Defined Service (PI_UDEF) 463
- Web Transaction (PI_WT) 464

11 **Commands 469**

List of commands 470

Details of commands 471

esppasswd (registers, changes, and deletes passwords) 472

hntr2util (changes the integrated trace log settings) 475

jpcvtaskctl (pauses/resumes the measurement of a task) 476

jpcvtest (executes measurement tests) 482

12 **Messages 491**

12.1 Message format 492

12.1.1 Format of output messages 492

12.1.2 Format of message explanations 493

12.2 Message output destinations 494

12.3 List of messages output to the Windows event log 511

12.4 Messages 513

Part 4: Troubleshooting

13 **Error Handling Procedures 645**

13.1 Error handling procedures 646

13.2 Troubleshooting 647

13.2.1 Measuring Web transactions 648

13.2.2 Other problems 651

13.3 Log information to be collected upon troubleshooting 653

13.3.1 Types of log information to be collected upon troubleshooting 653

13.3.2 Lists of log files and folders accessed upon troubleshooting 654

13.4 Data to be collected when a problem occurs 657

13.4.1 In Windows 657

13.5 Data collection procedure 661

13.5.1 In Windows 661

13.6 Detecting problems within Performance Management 664

13.7 Performance Management system error recovery 665

13.8 Error handling procedure for each problem 666

13.8.1 PFM - Agent for Service Response service cannot be started 666

13.8.2 PFM - Agent for Service Response cannot perform measurements 667

13.8.3 Error and normal alarms are raised alternately in PFM - Agent for Service Response measurement 675

Appendixes 676

A Estimating System Requirements 677

A.1 Estimating memory requirements 677

A.2 Estimating disk space requirements 677

A.3	Disk space requirements for operation in a cluster system	677
B	List of Identifiers	678
C	List of Processes	679
D	List of Port Numbers	680
D.1	Port numbers of PFM - Agent for Service Response	680
D.2	Firewall passage directions	680
D.3	Notes on measurement in a firewall/NAT environment	681
E	Properties of PFM - Agent for Service Response	682
E.1	Agent Store service properties	682
E.2	Agent Collector service properties	685
F	List of Files and Folders	701
G	Migration Procedure and Notes on Migration	705
H	Version Compatibility	706
I	Outputting Action Log Data	707
I.1	Types of events output to the action log	707
I.2	Format for saving the action log files	707
I.3	Format of output action log data	708
I.4	Settings for outputting action log data	713
J	Linkage with JP1/SLM	715
K	About Communication in IPv4 Environments and IPv6 Environments	716
L	Version Changes	717
L.1	Changes in 11-10	717
L.2	Changes in 11-00	717
L.3	Changes in 10-50	718
L.4	Changes in 10-00	718
L.5	Changes in 09-00	719
M	Reference Material for This Manual	722
M.1	Related publications	722
M.2	Conventions: Abbreviations for product names	722
M.3	Conventions: Acronyms	724
M.4	Conventions: Product names, service IDs, and service keys	725
M.5	Conventions: Installation folder	726
M.6	Conventions: KB, MB, GB, and TB	726
N	Glossary	727

Index 735

1

Overview of PFM - Agent for Service Response

This chapter provides an overview of PFM - Agent for Service Response.

1.1 Features of PFM - Agent for Service Response

PFM - Agent for Service Response is a program that collects and manages performance data, enabling you to monitor the performance of Internet services.

PFM - Agent for Service Response has the following features:

- Ability to analyze the operating status of Internet services
PFM - Agent for Service Response enables you to easily analyze the operating status of Internet services by collecting and summarizing such performance data as response times obtained from the Internet services being monitored. You can also display trends and changes graphically.
- Ability to detect operational problems on the Internet and quickly provide information needed to identify the cause of a problem
In the event of a performance problem, such as a delay in response time on the Internet, PFM - Agent for Service Response helps the user become aware of the problem at an early stage by sending the user a notification, such as by email. PFM - Agent for Service Response also provides a graphic display of information useful in identifying the cause of a problem.

You must have PFM - Manager, PFM - Base, and PFM - Web Console to use PFM - Agent for Service Response.

The following subsections describe PFM - Agent for Service Response.

1.1.1 Collecting Internet service performance data

PFM - Agent for Service Response enables you to collect performance data, such as an Internet service's response times.

PFM - Agent for Service Response lets you collect and use performance data in the following ways:

- Collecting information about an Internet service's response performance
PFM - Agent for Service Response collects information about an Internet service's response performance by sending requests to the Internet service's server, and by measuring the amount of time it takes to receive a response and the data transfer throughput. The information collected by PFM - Agent for Service Response, such as response times and throughput, is called the *response performance information*. PFM - Agent for Service Response can monitor the following eight types of Internet services:
 - HTTP
 - HTTPS
 - SMTP
 - POP3
 - IMAP4
 - DNS
 - DHCP
 - FTP
 - TCP
- Measuring transactions

For measurement of the services of HTTP and HTTPS (abbreviated hereafter to *HTTP(S)*), PFM - Agent for Service Response supports not only measurement of a single request/response, but also a series of tasks consisting of multiple HTTP(S) requests/responses as a single Web transaction.

- Measuring the operations in the Internet Explorer

PFM - Agent for Service Response measures the time to finish displaying Web pages in the Internet Explorer and collects the approximate performance data close to the actual performance the users experience in the Internet Explorer. It enables you to define and measure an IE scenario on a series of tasks consisting of multiple sets of operations in Internet Explorer.

- Extending the target services

You can measure a service other than the standard services supported by PFM - Agent for Service Response by providing a program for measuring the target service's response times, and then registering your program as a user-defined command in PFM - Agent for Service Response.

With PFM - Agent for Service Response, you use the collected performance data as follows:

- By graphically displaying the Internet service's operating status

By using PFM - Web Console, you can process and display performance data in a graphical format called a *report*. A report facilitates analysis of the Internet service's operating status.

There are two types of reports:

- *Real-time reports*

A real-time report indicates the current status of an Internet service that is being monitored. A real-time report is used primarily to check the current status of the system and to detect problems in the system. To display real-time reports, PFM - Agent for Service Response uses current performance data that has just been collected.

- *Historical reports*

A historical report indicates the status over time of an Internet service that is being monitored from past to present. A historical report is used primarily to analyze trends in the system. To display a historical report, the system uses performance data that has been stored in a database for PFM - Agent for Service Response.

- Using performance data to determine whether a problem has occurred

If the performance data value collected indicates some sort of error, an action can be taken, such as notifying the user.

1.1.2 Collecting performance data according to its characteristics

PFM - Agent for Service Response collects performance data in *records*. Each record consists of smaller units called *fields*. Records and fields are referred to collectively as the *data model*.

Records are classified into three types according to their characteristics. The record types that are used to collect performance data are predefined in PFM - Agent for Service Response. The user simply uses PFM - Web Console to specify the performance data records to be collected.

PFM - Agent for Service Response supports the following three record types:

- Product Interval record type (referred to hereafter as the *PI record type*)

For records of the *PI* record type, the system collects performance data for a specified interval, such as the number of processes per minute. You can use these records to analyze changes or trends in the system status over time.

- Product Detail record type (referred to hereafter as the *PD record type*)

For records of the PD record type, the system collects performance data that indicates the system status at a specific point in time, such as detailed information about the currently active processing. You can use these records to obtain a snapshot of the system status at a particular time.

- Product Log record type (referred to hereafter as the *PL record type*)

For records of the PL record type, the system collects the log and the messages on applications that are being executed.

For details about each record type, see [10. Records](#).

1.1.3 Saving performance data

By storing collected performance data in a special database, you can save the performance data up to the current date and use it to analyze trends (from the past to the current date) in the Internet service's operating states. This special database is called the *Store database* of PFM - Agent for Service Response. You use historical reports for analysis of trends.

You use PFM - Web Console to select the performance data records to be stored in the Store database. For details about how to use PFM - Web Console to select records, see the chapter that describes management of operation monitoring data in the *JP1/Performance Management User's Guide*.

1.1.4 Providing notification of problems in Internet service operations

You can use performance data collected by PFM - Agent for Service Response not only to display Internet service performance as reports, but also to warn the user when problems and errors occur during operation of an Internet service.

For example, the user can be notified by email whenever it takes longer than 10 seconds to receive a response after a request has been sent to an Internet service's server. To achieve this, you would set *takes more than 10 seconds to receive response after request sent to Internet service's server* as the abnormal condition threshold, and you would set the system to send an email to the user when this threshold is reached. What the system is set to do when a threshold is reached is called an *action*. The following actions are available:

- E-mail transmission
- Command execution
- SNMP trap issuance
- JP1 event issuance

The definition of a threshold or action is called an *alarm*. A table of the defined alarms is called an *alarm table*. Once an alarm table is defined, it is associated with PFM - Agent for Service Response; this process is called *binding*. Once an alarm table has been bound to PFM - Agent for Service Response, whenever performance data collected by PFM - Agent for Service Response reaches a threshold defined as an alarm, the event is reported to the user.

By defining alarms and actions, you can be made aware of problems in Internet service operations at an early stage, and take appropriate action quickly.

For details about how to set alarms and actions, see the chapter that describes operation monitoring by alarms in the *JP1/Performance Management User's Guide*.

1.1.5 Easily defining alarms and reports

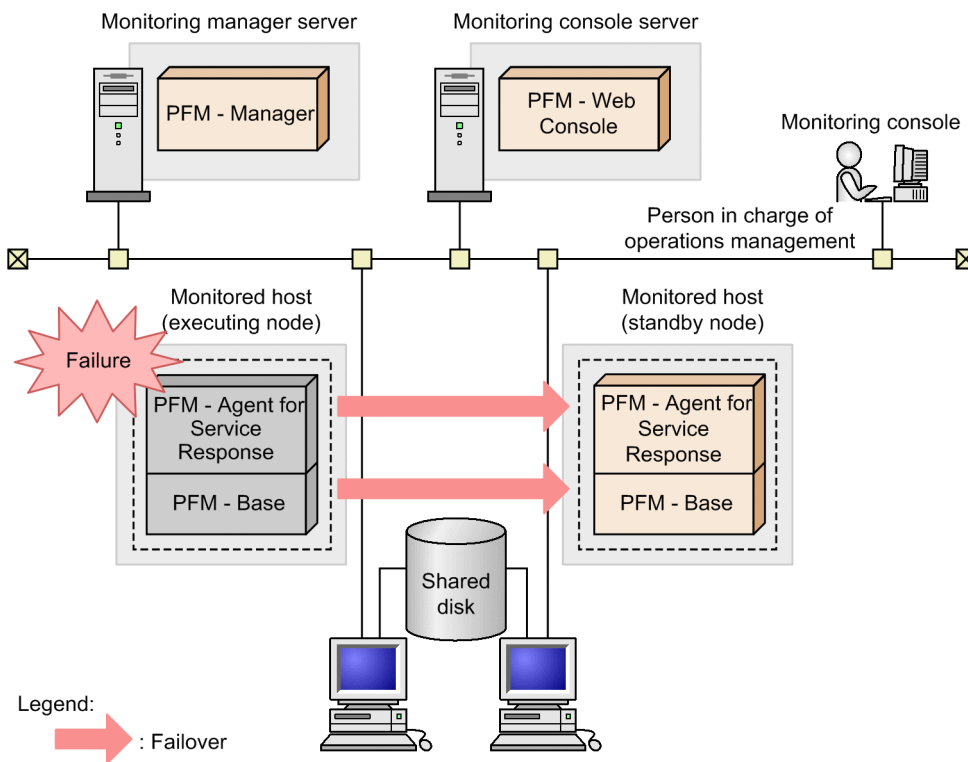
PFM - Agent for Service Response provides a *monitoring template*, in which the required information for standard reports and alarms is predefined. This monitoring template facilitates setup for monitoring the operating status of Internet services, because it does not require you to make complicated definitions. You can also customize the monitoring template for your environment. For details about how to use the monitoring template, see the chapter that describes report creation for operation analysis or for operation monitoring by alarms in the *JP1/Performance Management User's Guide*. For details about the monitoring template, see [9. Monitoring template](#).

1.1.6 Operation in a cluster system

Employment of a cluster system creates a highly reliable system that can continue job processing even in the event of a system failure, thereby achieving 24-hour operation and monitoring for Performance Management.

The following figure shows an example of operation in the event of a host failure in a cluster system.

Figure 1–1: Example of operation in a cluster system



Two environments with the same settings are created. Then the environment that is normally used for operations is defined as the *executing node*, and the other environment that will be used in the event of a failure is defined as the *standby node*.

For details about the operation of Performance Management in a cluster system, see [6. Operation in a Cluster System](#).

2

Functions of PFM - Agent for Service Response

This chapter describes functions of PFM - Agent for Service Response.

2.1 Functions of PFM - Agent for Service Response

PFM - Agent for Service Response is a program for measuring the performance of Internet services, such as their response times and data transfer throughputs. PFM - Agent for Service Response supports the following types of measurements for Internet services:

Table 2–1: Types of measurements for Internet services with PFM - Agent for Service Response

Types of measurements	Description	See
Measurement of Internet services	Response performance of Internet services can be measured. Data to be acquired includes response times after transmission of requests to HTTP, SMTP, and other servers and data transfer throughputs.	2.1.1
Measurement of Web transactions	Response performance of HTTP(S) services can be measured. You can not only measure a pair of request and response, but also define and measure as a Web transaction a series of tasks consisting of multiple HTTP(S) requests and responses. This measurement can be used to measure not only Web servers, but also Web applications that require logon.	2.1.2
Measurement of IE scenarios	Response performance of HTTP(S) services that users experience when using Internet Explorer can be measured. You can define a series of tasks consisting of multiple operations in Internet Explorer as an IE scenario and measure it. For details about the difference between measurement of Web transactions and measurement of IE scenarios, see 2.2 Selecting the type of measurement for Web server monitoring .	2.1.4
Measurement of user-defined services	Response performance of services other than the standard Internet services supported by PFM - Agent for Service Response can be measured. You must provide a program for measuring the response time or other measurements of the target service and register it as a user-defined command.	2.1.5

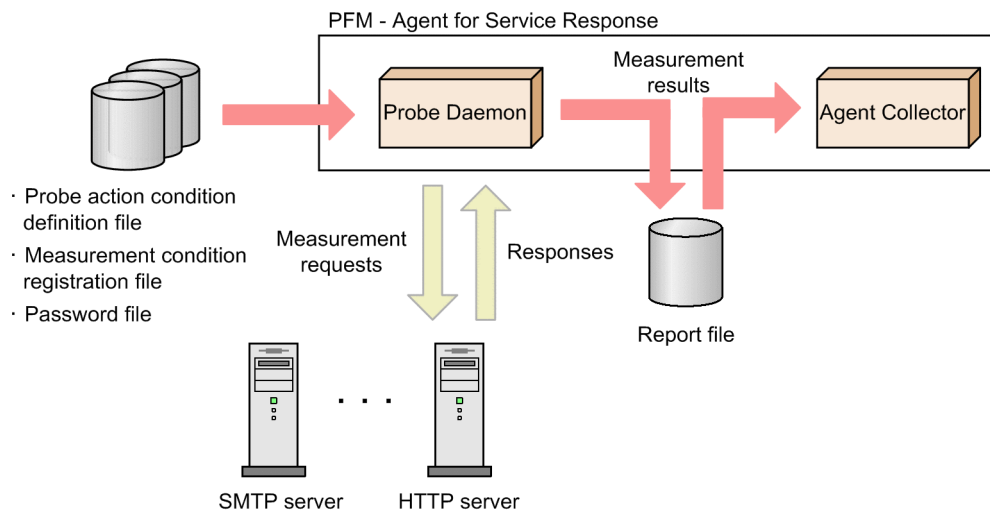
Each type is described below in terms of the mechanism of service measurement, the measurement items, and the measurement conditions.

2.1.1 Measurement of Internet services

PFM - Agent for Service Response measures an Internet service's response performance by acquiring data, such as the response times after transmission of requests and the data transfer throughputs. The function that measures an Internet service's response performance is called a *probe*. PFM - Agent for Service Response can measure an Internet service's response times down to thousandths of a second (3 decimal places).

The following figure provides an overview of measurement of an Internet service by PFM - Agent for Service Response.

Figure 2–1: Overview of measurement of an Internet service



At startup, PFM - Agent for Service Response's Probe Daemon reads the three files listed below. Measurement results for each measurement condition are output to a report file and then collected by Agent Collector at a specified interval.

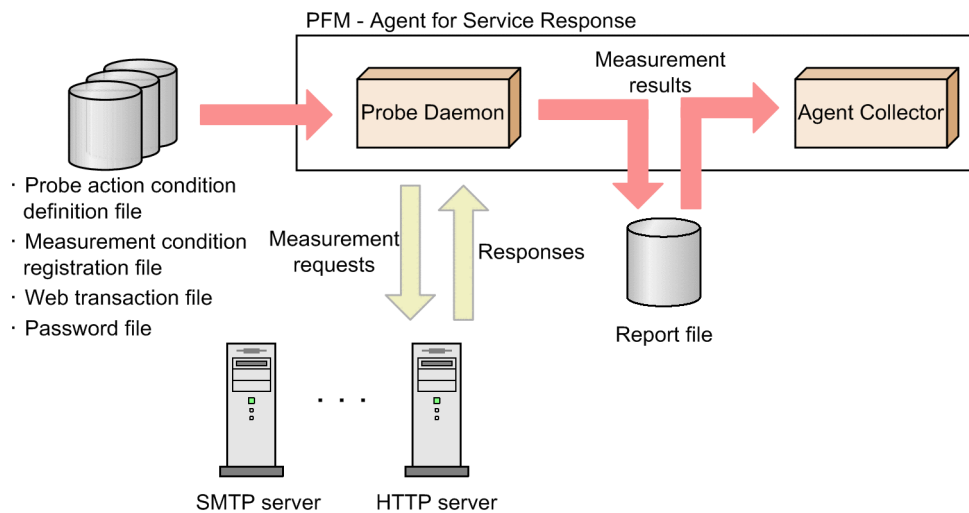
- Probe action condition definition file (`esp.conf`)
This file defines startup options, such as the maximum number of measurement conditions for a PFM - Agent for Service Response probe and the maximum size of a report file. For details, see [8.2 Probe action condition definition file \(`esp.conf`\)](#).
- Measurement condition registration file (`esptask.xml`)
This file defines the measurement conditions, such as a target's service type, host name, and measurement interval. You define the measurement conditions in PFM - Web Console (or you can define conditions by editing the measurement condition registration file directly). For details about defining conditions in PFM - Web Console, see [4.7 Defining measurement conditions in PFM - Web Console](#). For details about measurement condition registration file, see [8.3 Measurement condition registration file \(`esptask.xml`\)](#).
- Password file (`esp.pdb`)
This file registers and manages the passwords needed to log on to a target Internet service. For details, see [4.3.1 Registering passwords](#).

2.1.2 Measurement of Web transactions

When you obtain measurements of HTTP(S) services, PFM - Agent for Service Response enables you not only to measure a single set of a request and a response, but also to define and measure as a Web transaction a series of tasks consisting of multiple sets of an HTTP(S) request and a response. This makes it possible to measure not only Web servers, but also Web applications that require logon. PFM - Agent for Service Response can measure a Web transaction's response times down to thousandths of a second (3 decimal places).

The following figure provides an overview of measurement of a Web transaction.

Figure 2–2: Overview of measurement of a Web transaction



At startup, PFM - Agent for Service Response's Probe Daemon reads the four files listed below. Measurement results for each measurement condition are output to a report file and then collected by Agent Collector at a specified interval.

- Probe action condition definition file (`esp.conf`)
This file defines startup options, such as the maximum number of measurement conditions for a PFM - Agent for Service Response probe and the maximum size of a report file. For details, see [8.2 Probe action condition definition file \(`esp.conf`\)](#).
- Measurement condition registration file (`esptask.xml`)
This file defines the measurement conditions, such as a target's service type, host name, and measurement interval. You define the measurement conditions in PFM - Web Console (or you can define conditions by editing the measurement condition registration file directly). For details about defining conditions in PFM - Web Console, see [4.7 Defining measurement conditions in PFM - Web Console](#). For details about measurement condition registration file, see [8.3 Measurement condition registration file \(`esptask.xml`\)](#).
- Web transaction file
This file defines information such as a target Web transaction's access destination URL, Web authentication, and proxy. For details, see [8.5 Web transaction files](#).
- Password file (`esp.pdb`)
This file registers and manages the passwords needed to log on to a target Internet service. For details, see [4.3.1 Registering passwords](#).

When you measure a Web transaction, PFM - Agent for Service Response issues HTTP(S) requests according to the definition of the Web transaction, and measures data such as response times. The URL to be measured must be defined for each HTML frame. PFM - Agent for Service Response measures transactions by simulating a series of operations using a browser such as Internet Explorer. You can measure performance not only of the entire Web transaction, but also the following specific items:

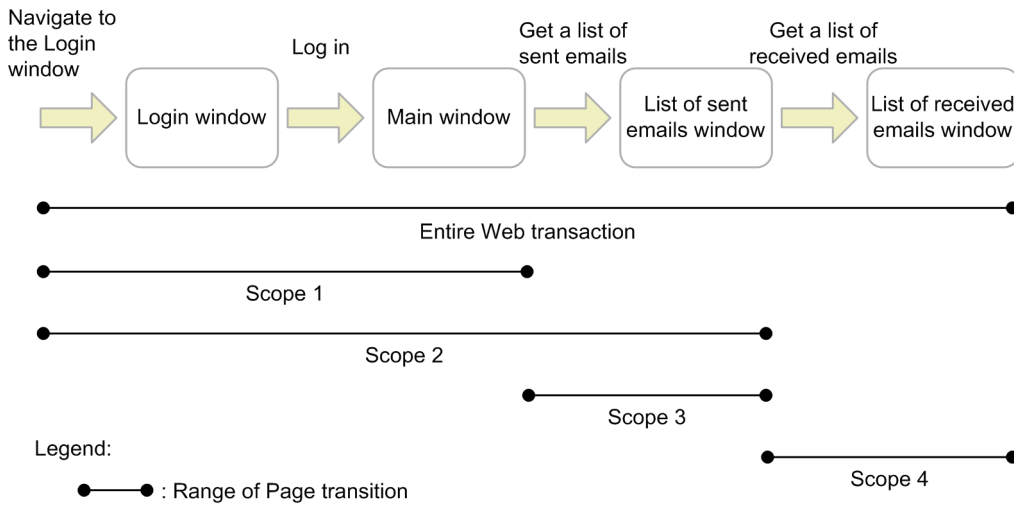
The measurement result of the entire Web transaction is output as the measurement result. You can define a series of page transitions as scope and the measurement result includes the measurement result of each scope. For details about performance data as measurement results, see [Web Transaction \(PI_WT\)](#) and [Web Transaction Overview \(PI_WTO\)](#) in [10. Records](#).

You can use Web Recorder to create Web transaction files. An Internet Explorer window is called from Web Recorder, which defines the Web transaction by recording the browser operations (navigations) performed in that window.

(1) Measurement of performance response for page transitions

You can measure the response performance for page transitions. To do this, you define as a *scope* a series (or range) of page transitions. You can define a maximum of 8 scopes. One range of page transitions defined as a scope may overlap another range. The following figure shows an example of scope definitions.

Figure 2–3: Example of scope definitions



In this example, the following measurement items were defined for each scope:

- Entire transaction
The time required to get to the point of being able to log in, the time that elapsed from display of the login window to getting a list of sent emails, and the time that elapsed from display of the login window to getting a list of received emails.
- Scope 1
Items such as the time required to get to the login window and log in
- Scope 2
Items such as the time required to get to the login window and get a list of sent emails
- Scope 3
Items such as the time required to get a list of sent emails
- Scope 4
Items such as the time required to get a list of received emails

As demonstrated in this example, you can measure the performance of each type of processing by defining scopes within a single Web transaction.

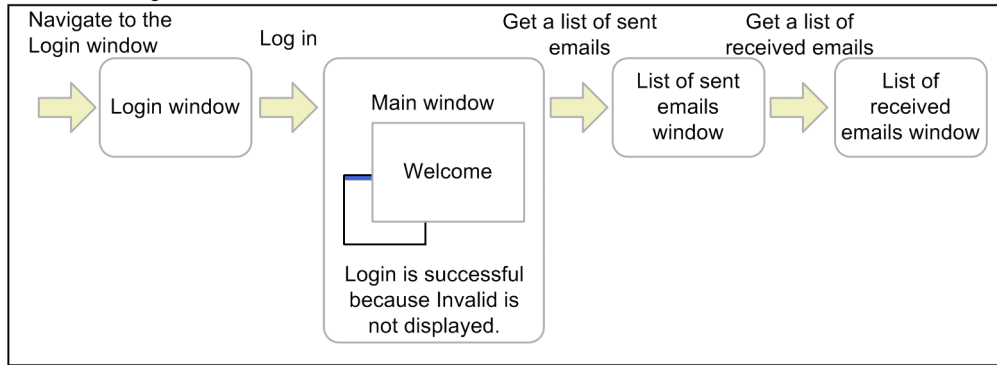
(2) Response determination

By defining response determination information, you can check the details of the HTML responses acquired from a defined URL and detect abnormalities at the measurement target.

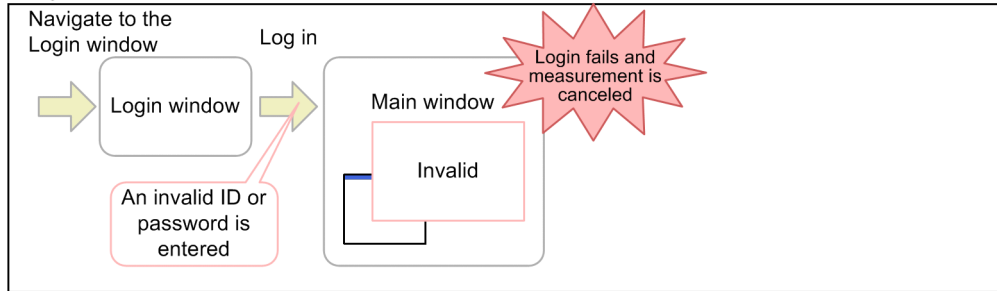
If you want to treat some successful event in the HTTP protocol level as evidence of an error in the Web transaction monitoring, such as when the login window is redisplayed because login has failed, you define the response determination information and then check the details of the response. The following figure shows an example of response determination definitions.

Figure 2–4: Example of response determination definitions (measurement of a Web transaction).

● Successful login



● Login failure



In this example, if the page after transition contains the word `Invalid`, login is determined to have failed. If this error is detected, measurement of the Web transaction is canceled.

(3) Acquisition of embedded resources

If you define acquisition of an embedded resource, you can acquire the embedded resource automatically during measurement. PFM - Agent for Service Response analyzes the HTML acquired during measurement, and obtains the resource specified by the values of a tag and an attribute name, as listed in the table below. If the response time is to include the acquisition time either for an embedded resource specified by a tag that is not an acquisition target for embedded resources, or for a resource embedded using a programming language such as JavaScript, then you must add the URL of that resource in the Web transaction definition.

Table 2–2: Acquisition targets of embedded resources

Tag name	Attribute name
applet	code
body	background
embed	src
img	src
object	data
script	src

Note:

Tag and attribute names are not case sensitive.

(4) Support for dynamic session management

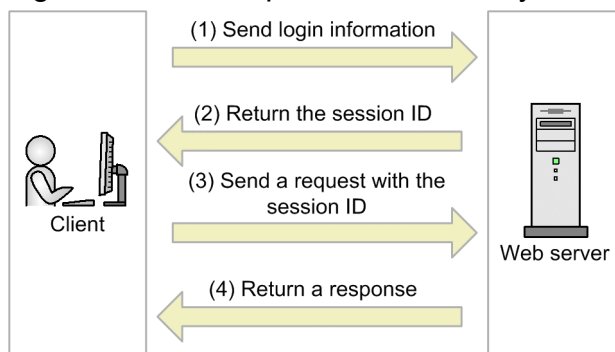
When PFM - Agent for Service Response conducts Web transaction monitoring, it can handle the dynamically changing HTTP requests so that PFM - Agent for Service Response can monitor the sites that manage the session using the session IDs.

Take the sites using the Web applications for example. These sites provide the log-in page using the form on the HTML. These sites assign the session IDs to its visitors when they log in to the sites and then identify its visitors by adding the session IDs to the requests.

To monitor these kind of sites, you must add the issued (obtained) session IDs to its requests thereafter.

The following figure shows an example of a site that manages sessions by dynamically issuing session IDs.

Figure 2–5: Example of a site that dynamically manages sessions



Yet, if you send requests with the recorded session IDs by the Web Recorder, the Web server judges the requests to be sent with the invalid session IDs and returns the HTML with error messages such as `Invalid Session ID` (although error messages appear, the HTTP requests itself do succeed).

To monitor these kind of sites properly, you must obtain the session IDs while you conduct a measurement of Web transactions and issue the requests with the obtained session IDs.

PFM - Agent for Service Response provides the setting of variable strings and substitute strings in order to support the dynamic session management. You specify the location of the string to contain the session IDs as the variable strings. To monitor the sites with the dynamic session management, you must define the Web transaction to output the HTML files. To do so, select the **Output the acquired HTML and HTTP header in a file** check box on the **Web Transaction Info** page in the Set Web Transaction Conditions window, or specify the `<HTML_OUT>` tag and measure the transaction. This is because PFM - Agent for Service Response looks up the session IDs in the output HTML files. As for the substitute string, you specify the location of the session IDs in the obtained HTML files.

Note that the HTTP Cookies generated through the Web transaction measurement issue the requests according to its conditions. If the sites implement the dynamic session management using HTTP Cookies and you do not need to edit the values of the Cookies in order to measure properly, you do not have to define variable strings and substitute strings. If you edit the values of the HTTP Cookies, prepare the commands to generate the substitute string, specify the value of the Cookie as the variable string and specify the commands as the substitute string.

For details about the definitions for supporting dynamic session management, see [4.4.6 Defining settings for the dynamic session management](#).

(5) Setting of the Character set

You can specify the following character sets for the Web transaction measurement. You specify the character set in the Web transaction file.

- The character set for the Web transaction file

You specify the character set of the Web transaction file in the XML declaration of the Web transaction file. The specifiable values are `Shift_JIS`, `EUC-JP`, `ISO-2022-JP`, `UTF-8`, `US-ASCII`, and `GB18030`.

You cannot use multiple character sets in a Web transaction file. Define Web transaction files for each character set if you use multiple character sets. If you specify `UTF-8`, do not add the BOM (Byte Order Mark) in the Web transaction file when editing and saving the file. If the BOM is added, the Web Recorder fails to read the Web transaction file.

- The character set for the acquired HTML file

You specify the character set of the character set is specified in the `<DEFAULT_CHARSET>` tag or the `<CHARSET>` tag of the Web transaction file. The specifiable values are `Shift_JIS`, `EUC-JP`, `ISO-2022-JP`, `UTF-8`, and `GB18030`. If the character set for the acquired HTML is `US-ASCII`, specify `Shift_JIS`, and you can use ASCII characters when you set response determinations and variable strings.

When you define response determinations and variable strings, specify this character set correctly.

- The character set for request information (URL, Message body, and Cookie) sent when measuring

You specify the character set for request information in the `<REQUEST_CHARSET>` tag of the Web transaction file.

The request information is sent using this specified character set, instead of the character set for the Web transaction files and the character set for the acquired HTML file. The specifiable values are `Shift_JIS`, `EUC-JP`, `ISO-2022-JP`, `UTF-8`, and `GB18030`. If the character set for request information is `US-ASCII`, specify `none` or `Shift_JIS`. If the value is `ISO-2022-JP`, do not include multi-byte characters in the URL strings and do not set variable strings.

If all request information (such as URL encoding strings) is defined using ASCII characters, it is not necessary to specify this character set.

The `UTF-8` supports only Japanese and Chinese. The `GB18030` supports only Chinese.

For details about setting, see [8.5 Web transaction files](#).

(6) URL encoded

The URL and the message body defined in the Web transaction file are URL encoded when issuing the requests, as listed in the table below.

Table 2–3: URL encoding process

Target URL encoded	Target string	URL encoding process
URL	<code>%xy#1</code>	Not encoded
	Alphanumeric characters	Not encoded
	The following symbols: ; / ? : @ & = + \$, - _ . ! ~ *	Not encoded
	Characters not listed above	Encoded into three-character string in the format of <code>%xy#1</code> .
Message body ^{#2}	Space	It is encoded into <code>+</code> .
	<code>%xy#1</code>	Not encoded
	Alphanumeric characters	Not encoded
	The following symbols:	Not encoded

Target URL encoded	Target string	URL encoding process
Message body#2	; / ? : @ & = + \$, - _ . ! ~ *	Not encoded
	Characters not listed above	Each byte is encoded into %xy#1.

#1

x and *y* are the hex numbers with each one representing 4-bit.

#2

Only the messages are sent for the `application/x-www-form-urlencoded` form.

The substitute strings are replaced with the variable strings through the encoding process described in the above table. If you use the characters such as delimiter (/ or =) in the variable string, you must force these characters to be URL encoded in the URL. In this case, specify the `<SUBSTITUTE_FORCE URLENCODE>` tag in the Web transaction file. For details about the `<SUBSTITUTE_FORCE URLENCODE>` tag, see [8.5.2 Format and definition of the Web transaction measurement conditions](#).

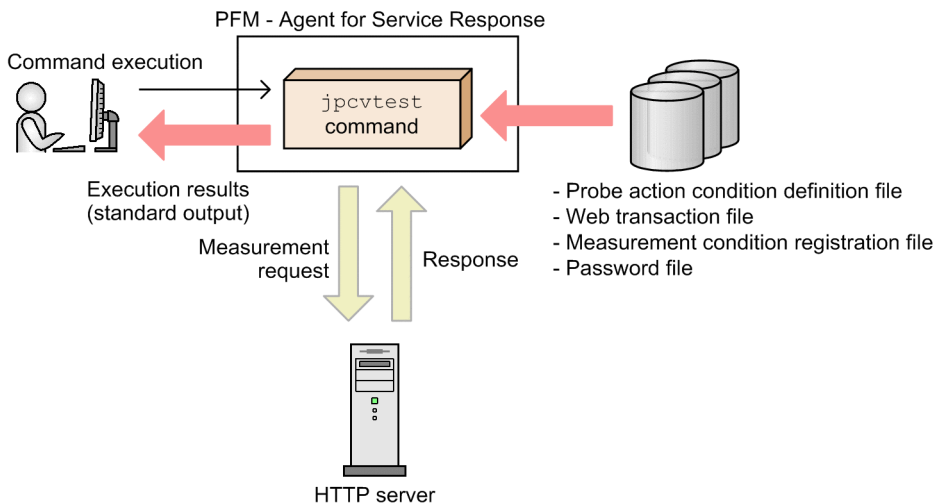
2.1.3 Web transaction measurement test

With PFM - Agent for Service Response, a predefined Web transaction measurement test can be executed.

Executing the measurement test command (`jpcvtest`) enables you to issue an HTTP(S) request according to the Web transaction definition and receive standard output that indicates whether a response to the request can be obtained. For details, see [jpcvtest \(executes measurement tests\)](#) in *II. Commands*.

The following figure shows an overview of a Web transaction measurement test.

Figure 2–6: Overview of a Web transaction measurement test



The measurement test command (`jpcvtest`) reads the following probe action condition definition file. The contents and creation method of the definition for the Web transaction to be measured are the same as those described in [2.1.2 Measurement of Web transactions](#).

- Probe action condition definition file (`esp.conf`)

This file defines startup options of PFM - Agent for Service Response. The following options are read and used when a Web transaction is measured with the measurement test command (`jpcvtest`).

Table 2–4: Probe action condition definition file used by the measurement test command "jpcvtest"

Section name	Key name
General	mode
	disable_ssl_protocol
	html_script_skip_flag
	enable_low_level_ssl_protocol
WEBTRANS Probe	max_keep_alive_session
	skip_emb_rsc_error
	post_redirect_method
Cluster	cluster_flag
	shared_directory

For details, see [8.2 Probe action condition definition file \(esp.conf\)](#).

- Measurement condition registration file (esptask.xml)

This file defines the measurement conditions, such as a target's service type, host name, and measurement interval. You define the measurement conditions in PFM - Web Console (or you can define conditions by editing the measurement condition registration file directly).

The definition for the Web transaction that undergoes a measurement test is read from this file.

For details about defining conditions in PFM - Web Console, see [4.7 Defining measurement conditions in PFM - Web Console](#). For details about measurement condition registration file, see [8.3 Measurement condition registration file \(esptask.xml\)](#).

- Web transaction file

This file defines information such as a target Web transaction's access destination URL, Web authentication, and proxy. For details, see [8.5 Web transaction files](#).

- Password file (esp.pdb)

This file registers and manages the passwords needed to log on to a target Internet service. For details, see [4.3.1 Registering passwords](#).

Web transaction measurement tests can be used in the following cases: when a new Web transaction that is created is checked before it is used for production operations, or when you need to check whether Web transactions can be measured after a monitored Web site is changed.

The following table describes measurement test usage patterns.

Table 2–5: Measurement test usage patterns

Usage patterns		Usage example
Checking when creating a new Web transaction	This assumes a situation in which PFM - Agent for Service Response is installed or Web transactions to be monitored are added.	Checking beforehand whether Web transactions can be monitored using a new Web transaction file that has been created
Checking after changing the settings on the monitored server	This assumes a situation in which Web content has been changed.	Checking whether Web transactions can be monitored even after components such as buttons or frames on the monitored page are changed

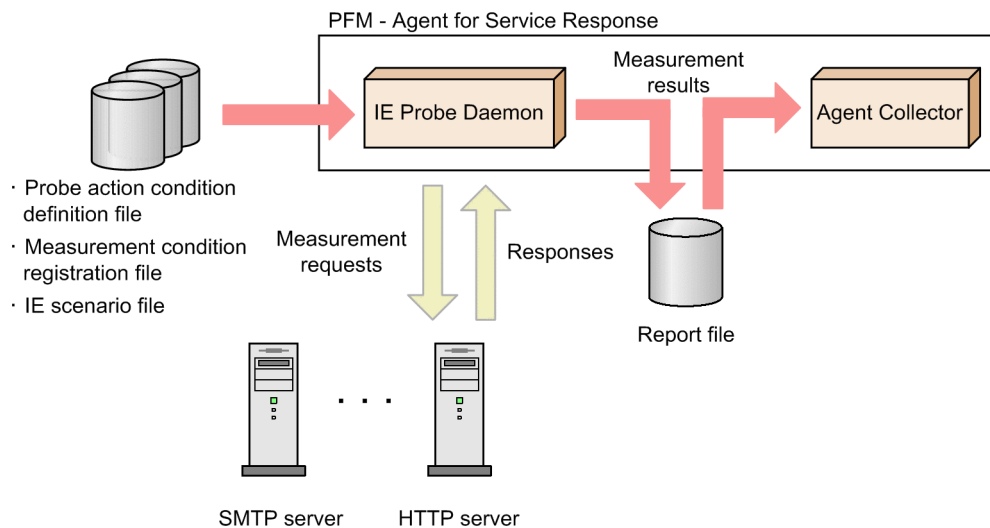
Usage patterns		Usage example	
Checking after changing the settings on the monitored server	This assumes a situation in which server settings have been changed.	Network configuration	Checking whether Web transactions can be monitored after server settings are changed, in the same way as before server settings are changed
		Security	
		Web server function settings (such as the number of simultaneous accesses)	
Checking after changing the definitions for PFM - Agent for Service Response	This assumes a situation in which the definitions for the monitored Web transaction have been changed.	Checking whether Web transactions can be monitored after the definitions in the Web transaction file are changed (the destination page, or the content of page operations is changed)	
	This assumes a situation in which measurement condition definitions have been changed.	Checking whether Web transactions can be measured correctly without measurement timeout after a timeout period is changed (shortened, for example)	
	This assumes a situation in which the password for a Web page that requires authentication has been changed.	Checking whether the Web page can be correctly authenticated with the new password and Web transactions can be monitored	
	This assumes a situation in which a certification file has been registered or replaced.	Checking whether the Web page can be correctly authenticated and Web transactions can be monitored	
Checking the Web server operating status	This assumes routine and maintenance tasks for system administrators.	Checking whether the Web server enters a running state after it is restarted.	

2.1.4 Measurement of IE scenarios

PFM - Agent for Service Response collects the time to complete displaying the Web pages in the Internet Explorer, measures the approximate performance response close to the actual performance the users experience in the Internet Explorer. You can define a series of tasks consisting of multiple sets of operations in Internet Explorer as an IE scenario and measure it. PFM - Agent for Service Response can measure IE scenarios response times down to thousandths of a second (3 decimal places).

The following figure provides an overview of measurement of an IE scenario.

Figure 2–7: Overview of measurement of an IE scenario



At startup, PFM - Agent for Service Response's IE Probe Daemon reads the three files listed below. Measurement results for each measurement condition are output to a report file and then collected by Agent Collector at a specified interval.

- Probe action condition definition file (*esp.conf*)
This file defines startup options, such as the maximum number of measurement conditions for a PFM - Agent for Service Response IE probe and the maximum size of a report file. For details, see [8.2 Probe action condition definition file \(esp.conf\)](#).
- Measurement condition registration file (*esptask.xml*)
This file defines the measurement conditions, such as a target's service type, host name, and measurement interval. You define the measurement conditions in PFM - Web Console (or you can define conditions by editing the measurement condition registration file directly). For details about defining conditions in PFM - Web Console, see [4.7 Defining measurement conditions in PFM - Web Console](#). For details about measurement condition registration file, see [8.3 Measurement condition registration file \(esptask.xml\)](#).
- IE scenario file
This file is used to record the operations in the Internet Explorer services as an IE scenario. You can use IE Recorder to create IE scenario files. An Internet Explorer window is called from IE Recorder, which defines the IE scenario by recording the operations performed in that window.

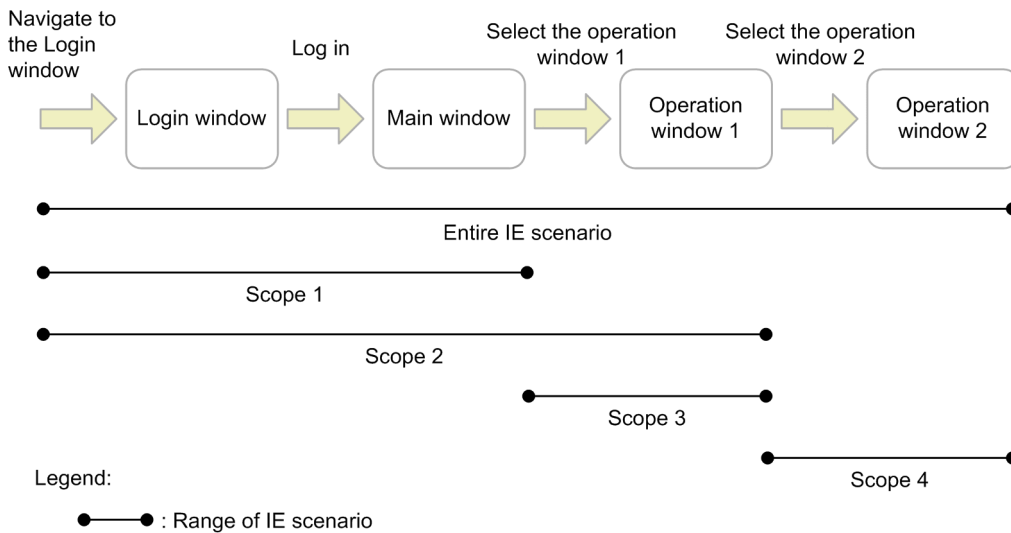
PFM - Agent for Service Response enables you to replay the Internet Explorer operations according to the IE scenario definitions and measure the required time to replay.

The measurement result of the whole IE scenario is output as the measurement result. You can define a series of operations as a scope and the measurement result includes the measurement result of each scope. For details about performance data as measurement results, see [IE Scenario \(PI_IES\)](#) and [IE Scenario Overview \(PI_IESO\)](#) in [10. Records](#).

(1) Measurement of performance response for operations in Internet Explorer

You can measure the response performance for operations in Internet Explorer. To do this, you define a series (or range) of operations in Internet Explorer. You can define a maximum of 16 scopes. One range of operations in Internet Explorer defined as a scope may overlap another range. The following figure shows an example of scope definitions.

Figure 2–8: Example of scope definitions



In this example, each scope is measured in terms of different measurement items described below:

- Entire IE scenario
The time for replaying the IE scenario required to get to the point of being able to log in, the time that elapsed from display of the login window to select the operation window 1, and the time that elapsed from display of the login window to select the operation window 2.
- Scope 1
The time for replaying the IE scenario required to get to the point of being able to log in, the time that elapsed from display of the login window to display of the main window.
- Scope 2
The time for replaying the IE scenario required to get to the point of being able to log in, the time that elapsed from display of the login window to select the operation window 1.
- Scope 3
The time for replaying the IE scenario required to select the operation window 1 in the main window that elapsed from display of the operation window 1.
- Scope 4
The time for replaying the IE scenario required to select the operation window 2 in the operation window 1 that elapsed from display of the operation window 2.

As demonstrated in this example, you can measure the performance of each type of processing by defining scopes within a single IE scenario.

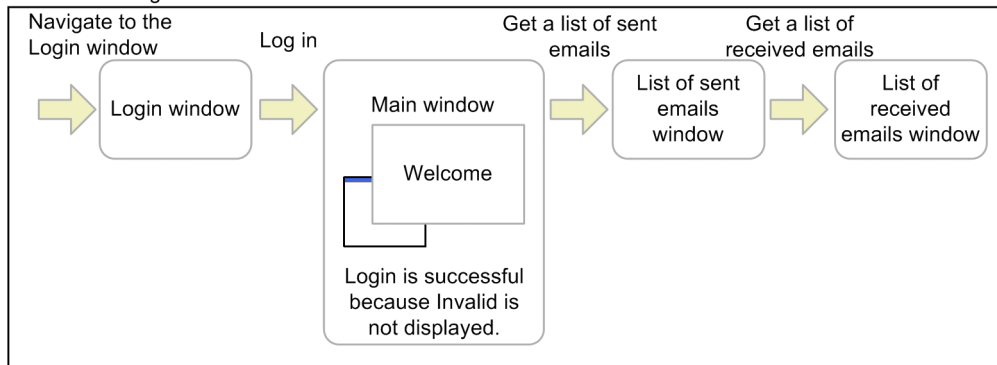
(2) Response determination

By defining response determination information, you can check the details of the HTML responses acquired from a defined IE scenario and detect abnormalities at the measurement target.

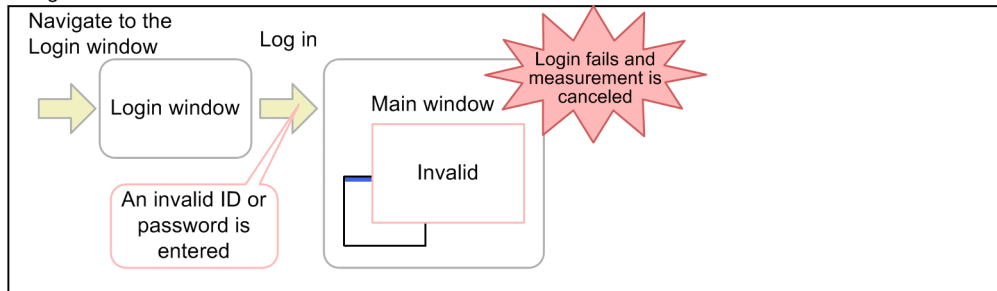
If you want to treat measurement tests as failure when the login failure page appears, define the response determination information and then check the details of the response. When PFM - Agent for Service Response checks the response, it only checks the strings of the obtained HTML file. The following figure shows an example of response determination definitions when login is successful and when login fails.

Figure 2–9: Example of response determination definitions (measurement of an IE scenario)

● Successful login



● Login failure



In this example, if the page after transition contains the word `Invalid`, login is determined to have failed. If this error is detected, measurement of the IE scenario is canceled.

(3) Identification of tags

After you record the IE scenario, the attributes or the positions of the operation target tags in the HTML file may change due to the layout change of the monitoring target site. In such a case, you can set a filtering condition to specify the monitoring target tag without re-recording the IE scenario.

The following describes how to identify the tags for operating targets.

Inner text:

Identifies the tags for operating targets by the inner text, which is surrounded by the start and end tags. If you specify the inner text, the tag that has the specified inner text is selected and operated during replaying the IE scenario. If there are multiple tags with the specified inner text, the tag that appears first in the HTML file is selected.

Attributes:

Identifies the tags for operating targets by the attribute value of the tag.

If you specify the attribute, the tag with the specified attribute value is selected and operated during replaying the IE scenario. If there are multiple tags with the specified attribute value, the tag that appears first in the HTML file is selected.

Tag position:

Identifies the tags for operating targets by the position of tag in the HTML file that has same inner text or attribute value. If you specify the tag position, the tag in the specified position is selected and operated during replaying the IE scenario.

For details about how to identify the tags for operating targets, see [7.3.2 Operation Settings window](#).

2.1.5 Measurement of user-defined services

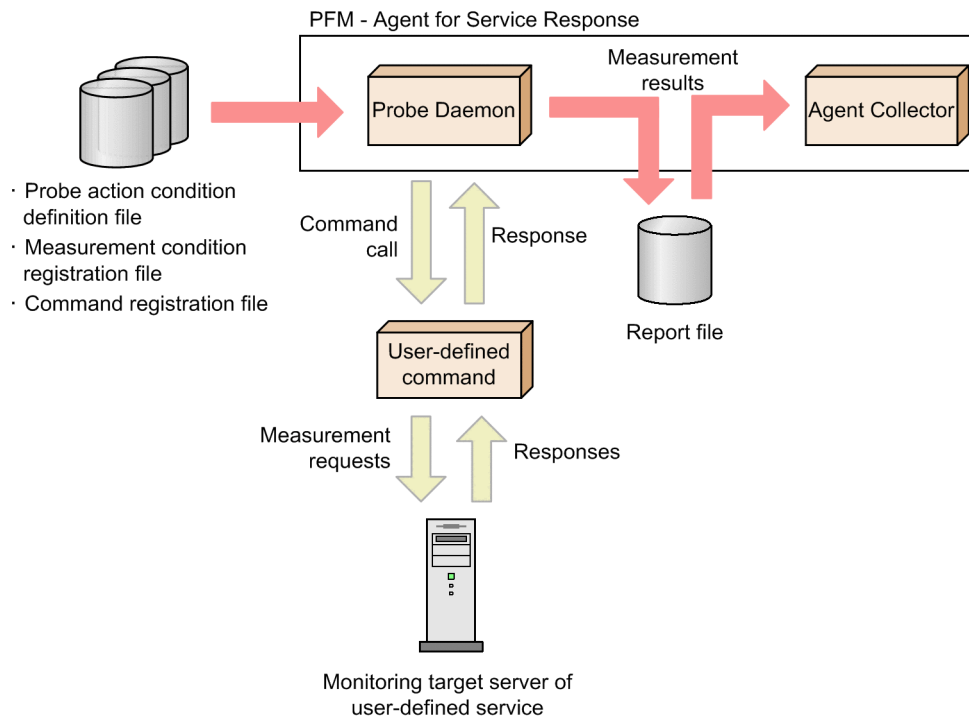
To measure a service other than the standard Internet services supported by PFM - Agent for Service Response, you must provide a program for measuring the target service's response times, and then register your program as a user command. In PFM - Agent for Service Response, such a program is called a *user-defined command*. A service that is measured by a user-defined command is called a *user-defined service*. PFM - Agent for Service Response can measure a user-defined service's response times down to thousandths of a second (3 decimal places).

There are two ways of performing measurement with a user-defined command:

- By using a numeric value output by the user-defined command as the measurement result
- By using the user-defined service's execution time as the measurement result

The following figure provides an overview of measurement of a user-defined service.

Figure 2–10: Overview of measurement of a user-defined service



At startup, PFM - Agent for Service Response's Probe Daemon reads the three files listed below. Measurement results are output to a report file for each measurement condition and then collected by Agent Collector at a specified interval.

- Probe action condition definition file (`esp.conf`)
This file defines start options, such as the maximum number of measurement conditions for a PFM - Agent for Service Response probe and the maximum size of a report file. For details, see [8.2 Probe action condition definition file \(`esp.conf`\)](#).
- Measurement condition registration file (`esptask.xml`)
This file defines the measurement conditions, such as the target's service type, host name, and measurement interval. You define the measurement conditions in PFM - Web Console (or you can define conditions by editing the measurement condition registration file directly). For details about defining conditions in PFM - Web Console, see [4.7 Defining measurement conditions in PFM - Web Console](#). For details about measurement condition registration file, see [8.3 Measurement condition registration file \(`esptask.xml`\)](#).
- Command registration file (`espcommand.xml`)

This file registers user-defined commands. For details, see [8.6 Command registration file \(espcommand.xml\)](#).

PFM - Agent for Service Response calls the user-defined command according to the defined measurement conditions at the defined measurement interval, and takes measurements consecutively in the same manner as when it measures the supported standard Internet services. However, only one item of a user-defined service can be measured. To measure additional item of a single user-defined service, you must create a user-defined command for each item.

2.1.6 Pausing and resuming a measurement

PFM - Agent for Service Response measures the time it takes to respond to a request issued to a monitoring target, and you can pause this measurement. This can be done while, for example, the HTTP or SMTP server monitored by PFM - Agent for Service Response is stopped due to maintenance. You can also resume the paused measurement.

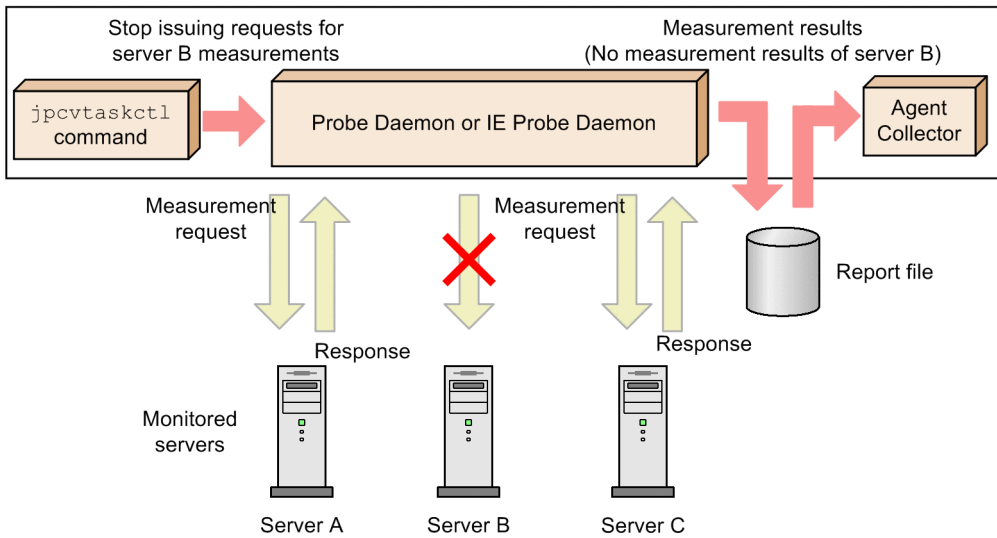
To pause or resume a measurement, execute the `jpcvtaskctl` command on a measurement-condition basis. For details about the command, see [jpcvtaskctl \(pauses/resumes the measurement of a task\)](#) in *11. Commands*.

The following figure provides an overview of how to pause or resume a measurement in PFM - Agent for Service Response.

Figure 2–11: Overview of how to pause or resume a measurement in PFM - Agent for Service Response

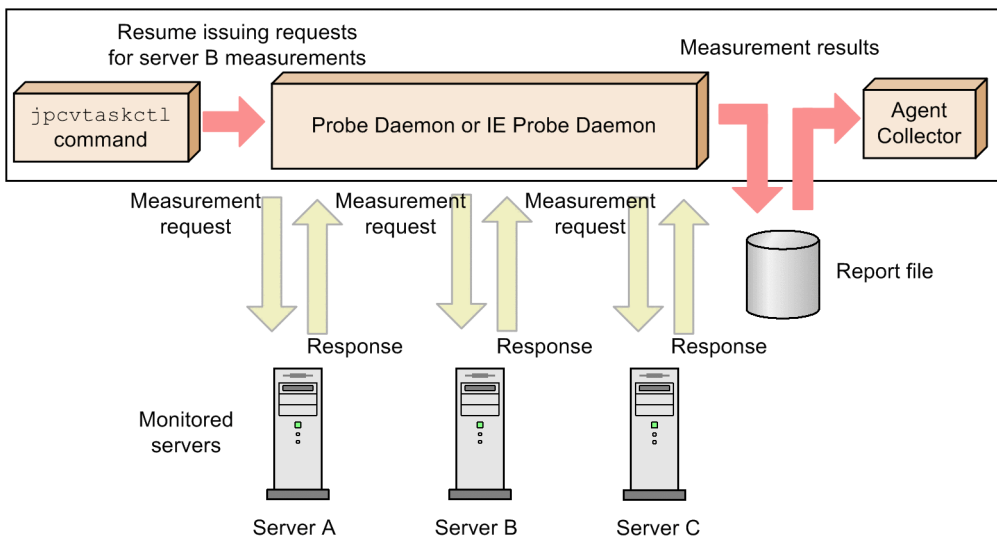
- Monitored server is in maintenance (when monitored server B is in maintenance and out of service)

PFM - Agent for Service Response



- Monitored server starts working again (when monitored server B starts working again)

PFM - Agent for Service Response



In addition, you can pause or resume the measurement at a predefined time by defining execution of a command as a custom job for JP1/Automatic Job Management System 3. To do so, define the command as a job that is executed on the Windows host (custom PC job). For details about the custom job, see the *JP1/Automatic Job Management System 3 Linkage Guide*.

2.2 Selecting the type of measurement for Web server monitoring

If you want to monitor your Web server using PFM - Agent for Service Response, select the type of measurement from:

- Measurement of Internet services (HTTP or HTTPS)
- Measurement of Web transactions
- Measurement of IE scenarios

If you want to monitor only the operating status of a monitored server or monitor a single Web page (for example, to monitor the top page only), you can use the type of measurement of Internet services (HTTP or HTTPS). This measurement is available with simple definition information compared with the measurement of Web transactions or of IE scenarios.

If you want to monitor transition and response performance of several Web pages, use the measurement of either Web transactions or IE scenarios. The table below shows the difference between measurement of Web transactions and measurement of IE scenarios.

Table 2–6: Difference between measurement of Web transactions and measurement of IE scenarios

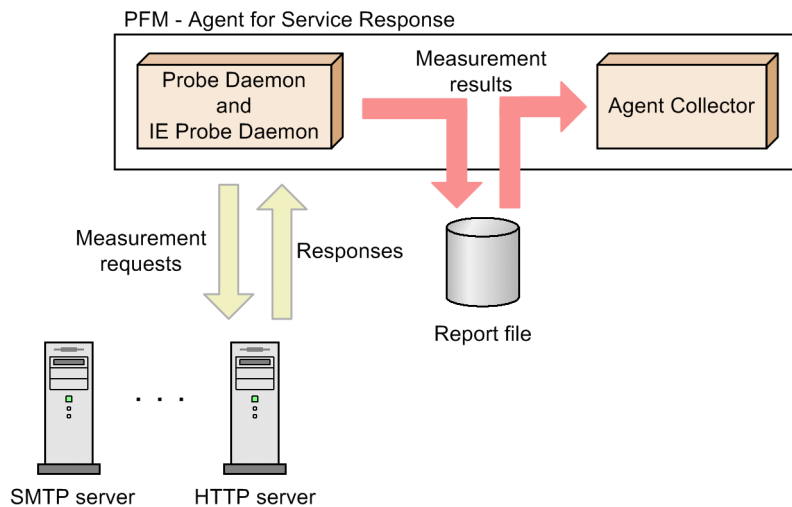
Item	Web transactions	IE scenarios
Measurable response performance	If you use the Web transactions, you can measure the amount of the time it takes to communicate with the Internet services (HTTP(S), DNS, or the like) as the response performance.	If you use IE scenarios, you can measure the elapsed time between the time you perform operations in Internet Explorer and the time these operations are completed as the response performance. You can monitor the approximate response performance to the ones users feel when operating in Internet Explorer.
Password management	The passwords are not managed in the Web transaction files but in the password file.	The passwords are managed in the IE scenario files.
Scope definitions	The scope of the Web transactions is a series of skips (a skip is a unit of the HTTP request and its HTTP response).	The scope of the IE scenarios is a series of operations in Internet Explorer.
Response determination	You can define a condition or a combination of two or more conditions as a response determination condition.	You can define a condition or a combination of two conditions as a response determination condition.
Acquisition of embedded resources	You must define in the transaction files whether or not the embedded resources are acquired.	Internet Explorer acquires the embedded resource automatically.
Support for dynamic session management	You must analyse the dynamically changing information and define necessary information to process dynamic session.	Internet Explorer processes automatically.
Specification of the character set	You must define the character set in the Web transaction files.	Internet Explorer processes automatically.

The measurement of IE scenarios depends heavily on the specifications of Microsoft Internet Explorer. Therefore, some Web pages cannot be measured depending on these specifications. Hitachi recommends that you use the trial version of PFM - Agent for Service Response and check to see if the software can measure monitored Web pages successfully before using the product version. For details about Web pages that cannot be measured in the measurement of IE scenarios, see [5.2.3 Notes on IE scenarios](#) and [5.2.4 Notes on the navigation](#).

2.3 Overview of collecting and managing performance data

The following figure shows the flow of performance data collection by PFM - Agent for Service Response.

Figure 2–12: Flow of performance data collection by PFM - Agent for Service Response



In PFM - Agent for Service Response, the Probe Daemon and the IE Probe Daemon measures a target's response times. The measurement results are output to a report file. Agent Collector collects the most recent data from the report file and manages it in the format of records.

The procedures for collecting and managing performance data depend on the record type used to store the performance data. The records for PFM - Agent for Service Response are classified into the following three types:

- PI record type
- PD record type
- PL record type

For details about how to collect and manage performance data, see the following chapters:

- Performance data collection procedure
For details about how to collect performance data, see the chapter that describes the functions of Performance Management in the *JP1/Performance Management Planning and Configuration Guide*.
For details about the values of the collected performance data, see [10. Records](#).
- Performance data management procedure
For details about the performance data management procedure, see the chapter that describes management of operation monitoring data in the *JP1/Performance Management User's Guide*.

You use PFM - Web Console to select the performance data to be used from the records collected and managed by PFM - Agent. For details about how to select performance data, see the chapter that describes management of operation monitoring data in the *JP1/Performance Management User's Guide*.

2.4 Example of performance monitoring operation

To maintain stable Internet service, it is important to monitor performance in order to have a good understanding of the status of an Internet service. This section explains how to use PFM - Agent for Service Response to monitor performance.

2.4.1 Purpose of performance monitoring

To maintain stable Internet services, it is important to monitor the performance of Internet services.

Major performance monitoring objectives using PFM - Agent for Service Response are to analyze performance data of Internet services and to determine the causes of bottlenecks.

PFM - Agent for Service Response helps the user become aware of the problem about the Internet services operations at an early stage by monitoring the performance data and sending users notifications for abnormalities.

Using PFM - Agent for Service Response as described above to correctly monitor performance is vital for stable system operation.

For details about how to monitor performance, see [2.4.3 Definition examples \(Measurement of Web transactions\)](#), and [2.4.4 Definition examples \(Measurement of IE scenarios\)](#). Actual settings need to be considered based on the system operation form.

2.4.2 Determining baselines

Determining baselines involves using the results of performance management to calculate the line at which no Internet service operation problems are anticipated.

Performance Management products use baseline values as thresholds for monitoring system operation. The determination of baselines is therefore an important task for successfully monitoring performance.

Note the following recommendations when you determine baselines:

- Measure system performance at peak load (for example, when a high-load test is run for the operating environment).
- Thresholds depend greatly on the system configuration. Therefore, performance should be measured again to re-determine the baselines if system resources and the operating environment have been changed.

2.4.3 Definition examples (Measurement of Web transactions)

This section explains the definition when you measure Web transactions on the sites with the dynamic session management. PFM - Web Console is taken for example as the sites with the dynamic session management.

To measure the sites with the dynamic session management as a Web transaction, you must specify the variable character strings each time you measure those sites.

When you use PFM - Web Console to measure Web transactions, you must consider the fact that these sites manage the sessions using the dynamically changing session IDs given to its users whenever they log in. The location of the session IDs (that is, in URLs, message bodies, or so) varies depending on the sites.

Thus, to measure Web transaction properly, the session IDs in the URL or message body must be replaced with the newly given session IDs whenever PFM - Agent for Service Response measure Web transactions.

Suppose that you record the following series of procedures in PFM - Web Console as a Web transaction:

1. Logging on to PFM - Web Console
2. Operations by using the PFM - Web Console (Displaying reports)
3. Logging off from PFM - Web Console

The following describes the overview of the procedures to measure this Web transaction correctly.

1. Record Web transactions
Use the Web Recorder to record step information of a Web transaction.
2. Define measurement conditions
Add necessary settings to measure the recorded Web transaction.
3. Test measurement conditions
Check whether the added definition is correct. At the same time, acquire the information to specify the setting for the dynamic session management.
4. Set conditions for dynamic session management
Set the conditions to replace the variable string with the substitute string.
5. Web transaction operation check
Check whether the Web transaction is measured correctly.

The following subsections describe the details of the procedures:

The information listed below is used in the following procedures. The values are displayed in italics.

Table 2–7: Necessary items to measure Web transaction

Item	Value
Web transaction file name	<i>sample01.xml</i>
Web transaction name	<i>sample01</i>
Prefix of step ID	<i>SAMPLE_STEP</i>
Task ID	<i>103#</i>

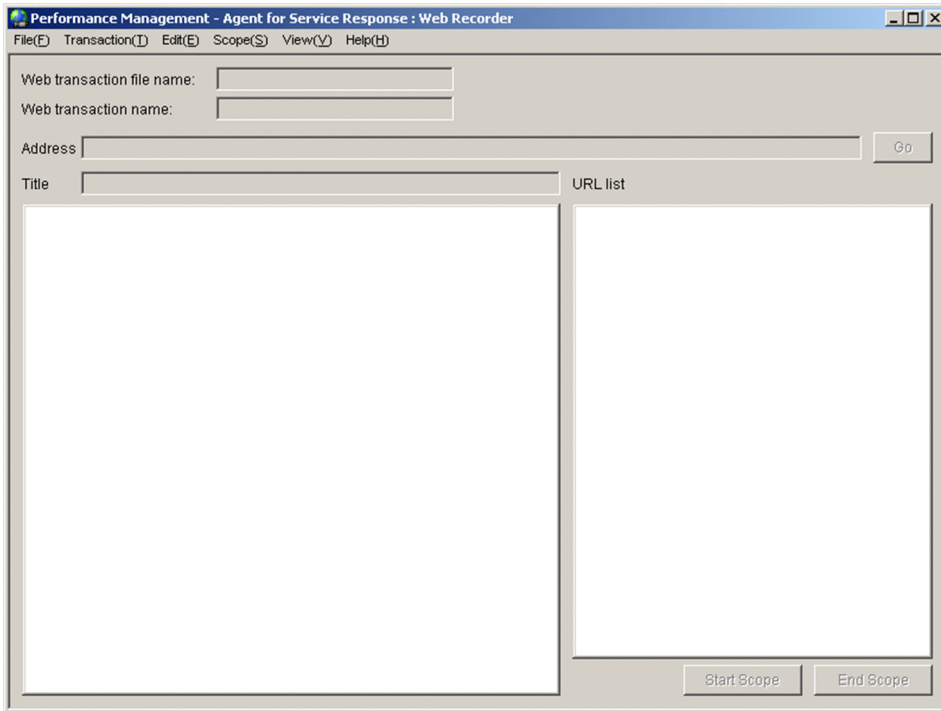
#

Each Task ID in the same Web transaction file must be unique.

(1) Recording Web transactions

The following shows the procedures to record the Web transactions.

1. From Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, and then **Web Recorder**.
The **Web Recorder (main)** window appears.



For details about the Web Recorder (main) window, see [7.2.1 Web Recorder \(main\) window](#).

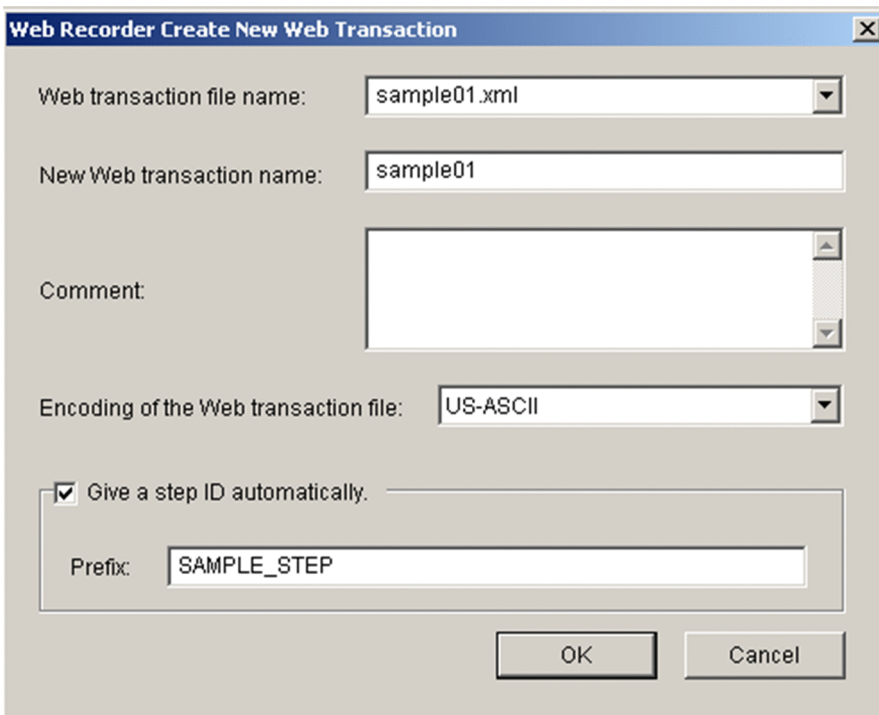
- From the **Transaction** menu, choose **New**.

The Web Recorder **Create New Web Transaction** window appears.

- Specify necessary items to create new Web transaction.

Specify *sample01.xml* in **Web transaction file name** and specify *sample01* in **New Web transaction name**.

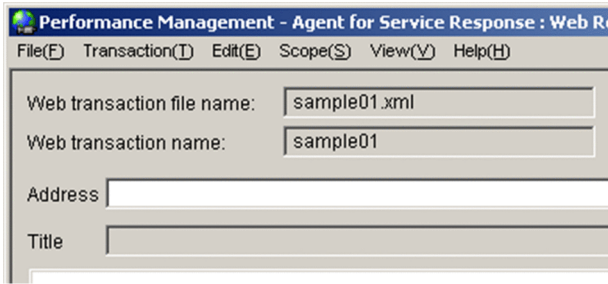
Check **Give a step ID automatically** check box, and then, enter a prefix in **Prefix**. The step IDs are necessary for outputting the acquired HTML and HTTP header in a file collected from pages that are to be accessed by the Web transaction.



For details about the **Create New Web Transaction** window, see [7.2.2 Create New Web Transaction window](#).

4. Click the **OK** button.

A new Web transaction is created, the specified values are display in **Web transaction file name** and **Web transaction name of the Web Recorder (main)** window.



5. In the **Web Recorder (main)** window, from the **Transaction** menu, choose **Set Transaction**.

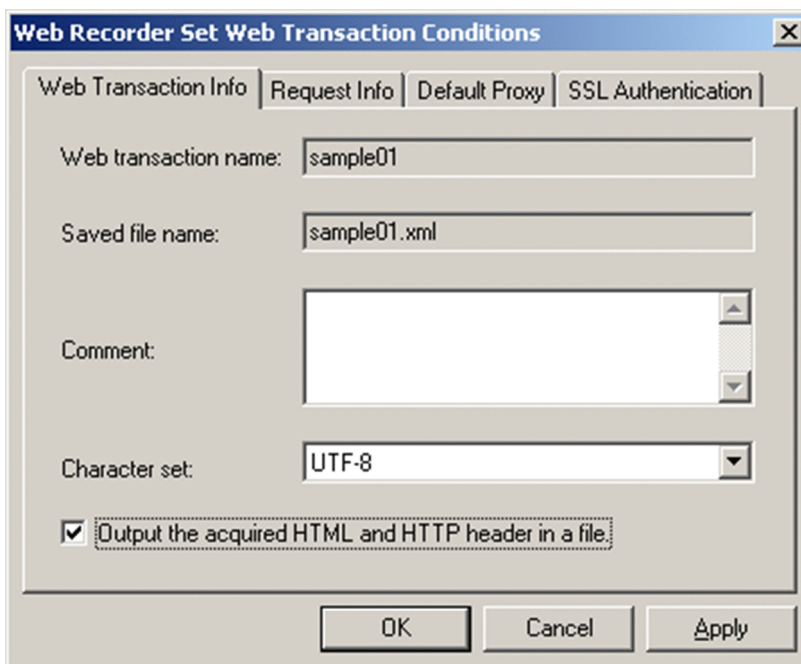
The **Set Web Transaction Conditions** window appears.

6. Set the configuration to output the acquired HTML and HTTP header in a file in **Web Transaction Info** page.

- Select the **Output the acquired HTML and HTTP header in a file** check box.

After selecting this check box, you can acquire the necessary information to replace the variable string (that is, the session ID when recording) with the substitute string (that is, the newly given session ID when logging in again). You can also check whether PFM - Agent for Service Response monitor transactions correctly.

- Select **UTF-8** in **Character set**.



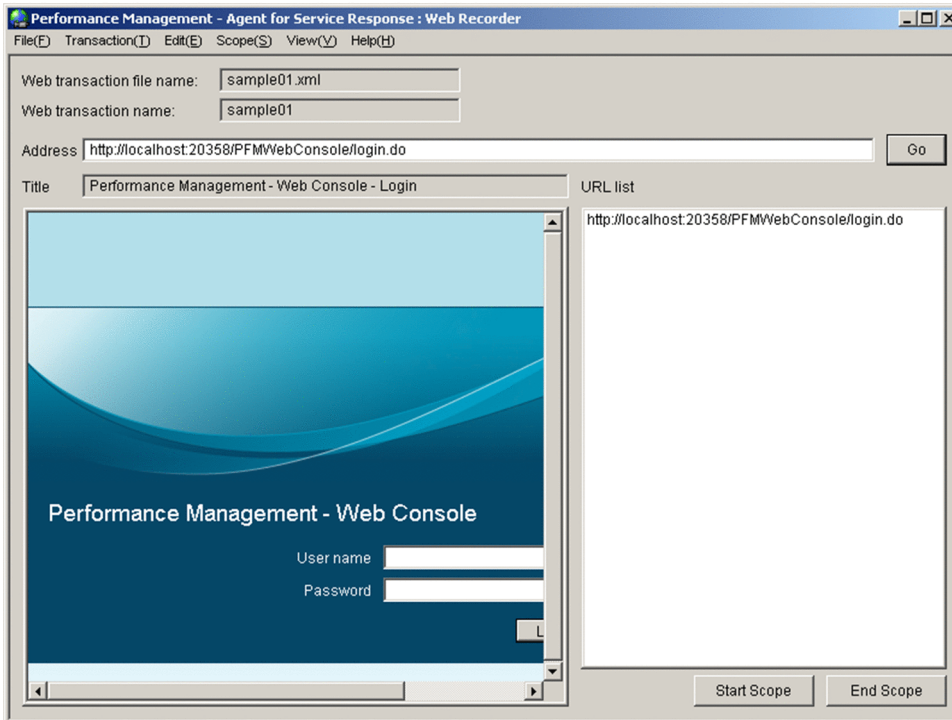
For details about **Set Web Transaction Conditions** window, see [7.2.6 Set Web Transaction Conditions window](#).

7. Click the **OK** button.

The **Set Web Transaction Conditions** window is closed.

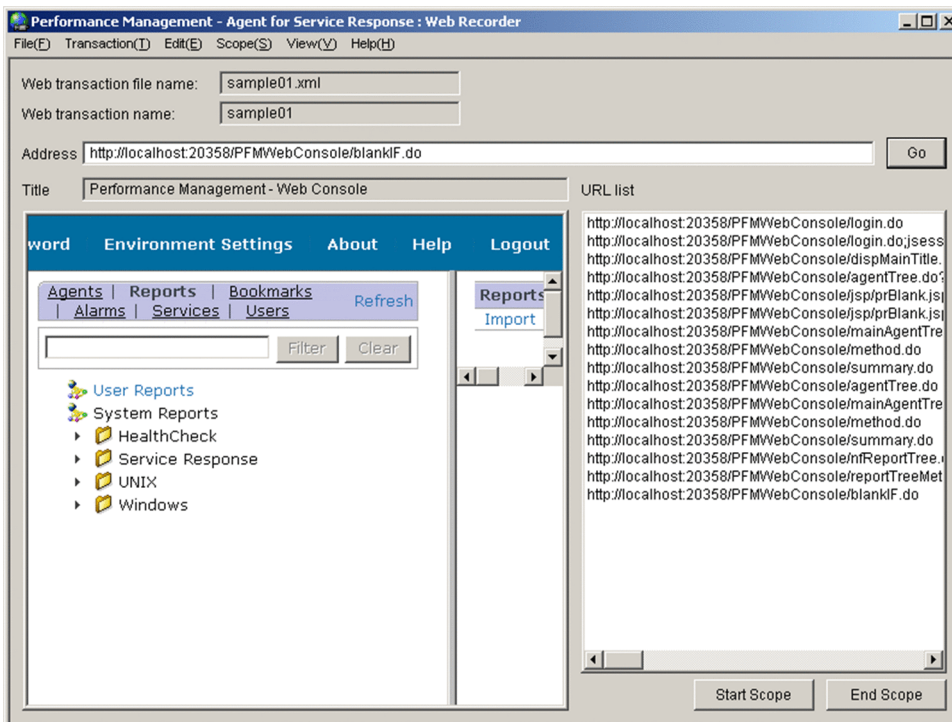
8. In the **Web Recorder (main)** window, in **Address**, enter the URL of the login window of PFM - Web Console and then click the **Go** button.

The **Login** window of PFM - Web Console appears in the **IE window**.



9. Enter a **User name** and **Password** in the **Login** window and click the **Login** button. Log on to PFM - Web Console. The main window appears in the **IE window**.

10. In the navigation frame of the **main** window, select the **Reports** tab.



11. In the menu bar frame of the **main** window, click the **Logout** menu to log off from PFM - Web Console. The **Login** window of PFM - Web Console appears in the **IE window**.

12. From the **Transaction** menu, choose **Save**. The Web transaction file is saved.

(2) Defining measurement conditions

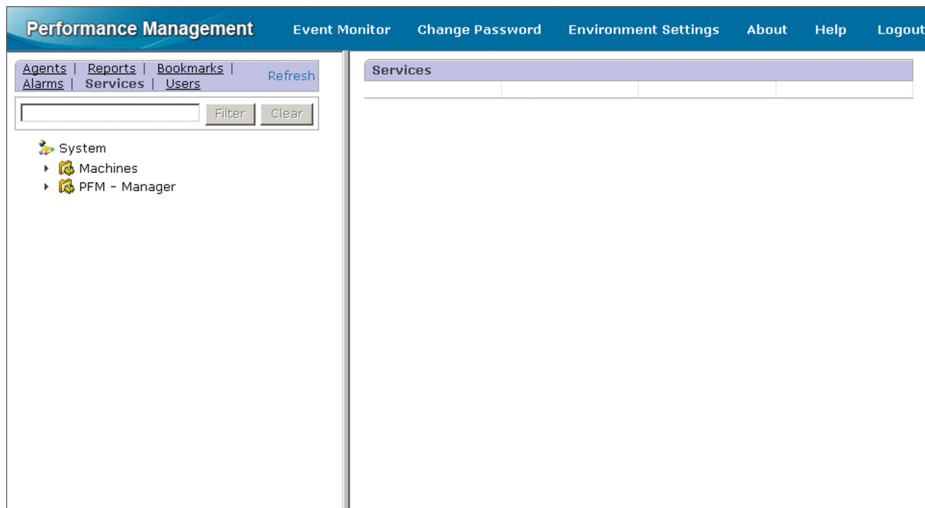
The following shows the procedures to define measurement conditions for Web transactions by using PFM - Web Console.

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

The **main** window of PFM - Web Console appears.

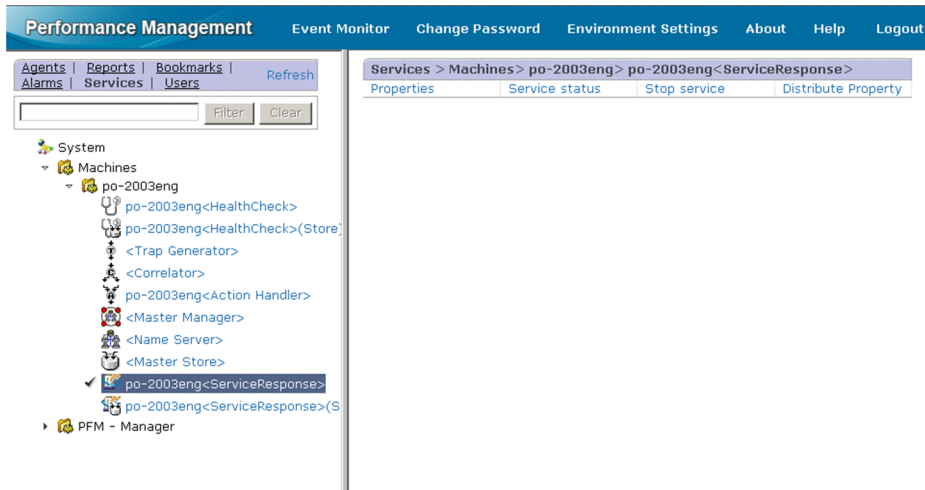
2. In the navigation frame of the **main** window, choose the **Services** tab.

The **Services** window appears.

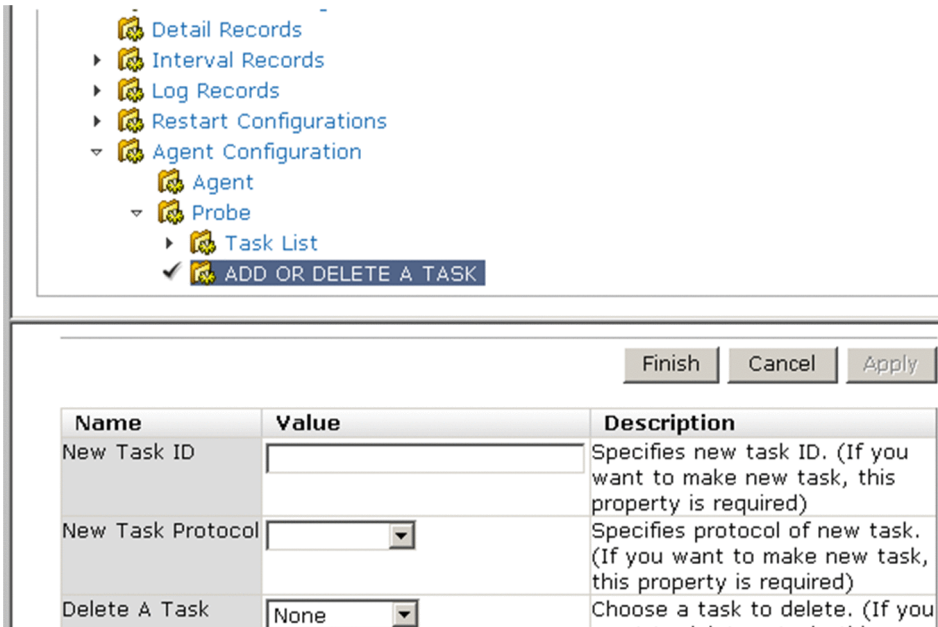


3. In the navigation frame of the **Services** window, expand the contents of the monitoring agent host folder, and select the Agent Collector service.

The **Properties** page appears.

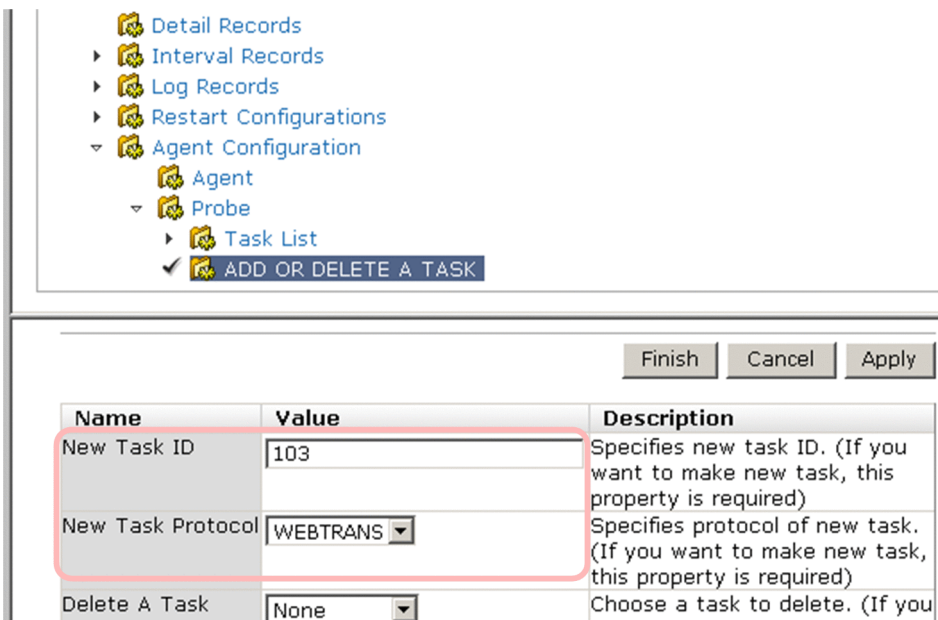


4. Expand the hierarchy under the **Probe** folder, and select the **ADD OR DELETE A TASK**.



5. Set properties appear at the bottom of the information frame.

Set *103* to the New Task ID, *WEBTRANS* to the New Task Protocol.



6. Click the *OK* button at the bottom of the information frame.

The created folder **WEBTRANS_103** appears under **Task List**.

Log Records
Restart Configurations
Agent Configuration
Agent
Probe
Task List
WEBTRANS_103
IESCENA_1
ADD OR DELETE A TASK

Finish Cancel

Name	Value	Description
First Registration Date	Wed Apr 03 15:21:17 GMT-08:00 2013	Displays the first date time the service was recognized by PFM - Manager.
Last Registration Date	Thu Apr 04 12:51:05 GMT-08:00 2013	Displays the most recent date and time the serv

7. Select the **WEBTRANS_103** tree

8. Set properties appear at the bottom of the information frame.

Set *80* to the Interval, *sample01.xml* to the Filename, and *sample01* to the Transaction.

Log Records
Restart Configurations
Agent Configuration
Agent
Probe
Task List
WEBTRANS_103
IESCENA_1
ADD OR DELETE A TASK

Interval	80	(optional item) Specifies the measurement interval. Values from 60 to 86400 can be specified.
Timeout	30	Specifies the maximum amount of time within which a single measurement must be completed by second. Values from 1 to 3600 can be specified.
Filename	sample01.xml	Specifies the name of Web transaction file.
Transaction	sample01	Specifies the name of Web transaction.

9. Click the **OK** button.

The specified settings are applied in the measurement condition registration file.

Reference note:

You can specify these conditions by editing the measurement condition registration file directly. In this case, add the following contents in the measurement condition registration file:

```
<TASK>
  <GEN_PARAM>
    <TASKID>103</TASKID>
```



```

<INTERVAL>80</INTERVAL>
<TIMEOUT>30</TIMEOUT>
</GEN_PARAM>
<SERV_PARAM>
<WEBTRANS>
  <TRANSACTION_FILE>sample01.xml</TRANSACTION_FILE>
  <TRANSACTION_NAME>sample01</TRANSACTION_NAME>
</WEBTRANS>
</SERV_PARAM>
</TASK>

```

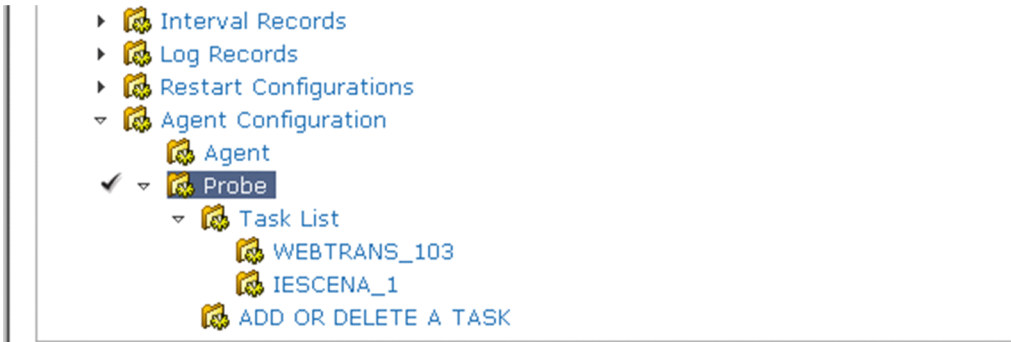
(3) Testing measurement conditions

The following shows the procedures to test the measurement conditions. Following these procedures, you also acquire the necessary information to specify the setting for the dynamic session management.

1. Select the **WEBTRANS_103** tree under **Task List**, check the value of **Status** is Valid.

Name	Value	Description
Task ID	103	ID of this task is displayed.
Status	Valid	Status of this task is displayed.
Task Label		Specifies user friendly name for this task. Must be shorter than 64 bytes width. (optional item)
Interval	80	Specifies the measurement interval. Values from 60 to 86400 can be specified.
Timeout	30	Specifies the maximum amount

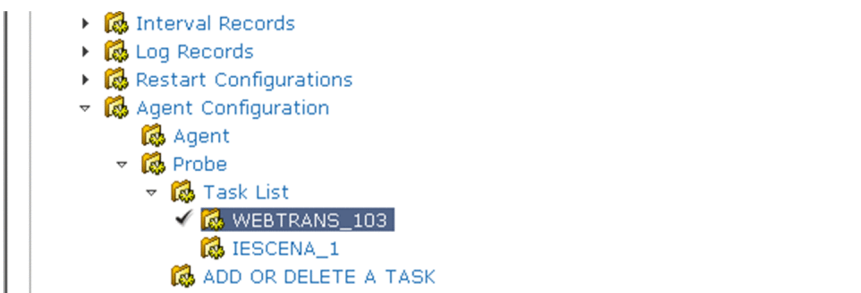
2. Select **Probe** folder under **Services** tree, select **Yes** in **Reload** and click the **OK** button.



Finish Cancel Apply

Name	Value	Description
Use Probe	Yes	Specifies whether to use Probe Daemon.
Reload	Yes	Selects if it reloads the measurement condition registration file.
Probe Status	Inactive	The status of Probe Daemon is displayed.
IE Probe Status	Active	The status of IE Probe Daemon is displayed.
Initial	0	The number of unreflected tasks is displayed. For those tasks, property

3. Select the **WEBTRANS_103** tree under **Task List**, check the value of **Status** is Applied.



Name	Value	Description
Task ID	103	ID of this task is displayed.
Status	Applied	Status of this task is displayed.
Task Label		Specifies user friendly name for this task. Must be shorter than 64 bytes width. (optional item)
Interval	80	Specifies the measurement interval. Values from 60 to 86400 can be specified.
Timeout	30	Specifies the maximum amount

4. Check whether the HTML file with *SAMPLE_STEP* as prefix in its file name (such as *SAMPLE_STEP00001.html*) is saved in the following folder by using the Explorer or so:

installation-folder\agtv\probe\probedata\webtrans

5. Open *SAMPLE_STEP00002.html*, check the substitute string in <frame> tag.

Look at the underlined string on the example below:

```
<frameset border="0" frameborder="no" framespacing="0" rows="32,*"
onUnload="baseLogout () ">
```

```

<frame name="PrTitle" noresize scrolling="no" frameborder="no"
src="/PFMWebConsole/dispMainTitle.do?
prSessionId=A_00E71812A672E7E3AA00385404F53228_1197249957218&launchMode="
/>

<frameset cols="350,*" border="8" frameborder="yes" framespacing="4"
bordercolor="silver">

```

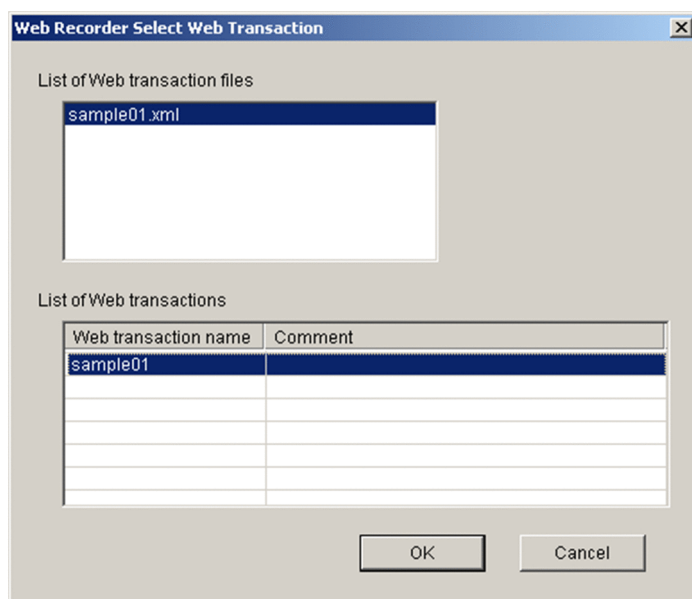
Hint:

In this example, since the first page where the session ID is found is *SAMPLE_STEP00002.html*, check firstly *SAMPLE_STEP00002.html*.

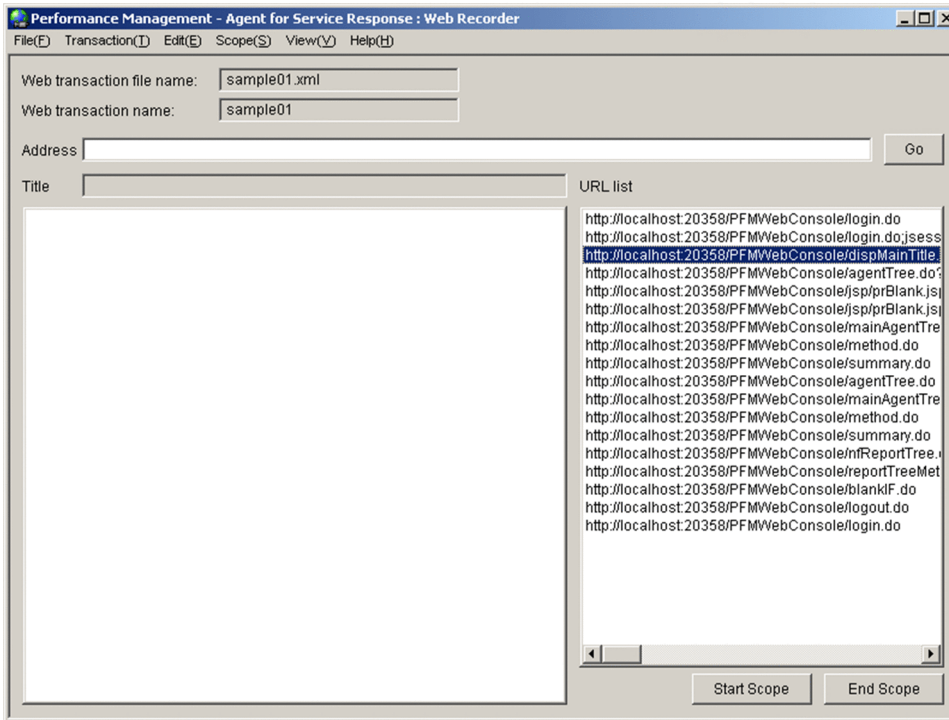
(4) Setting conditions for dynamic session management

The following shows the procedures to replace the variable string with the substitute string:

1. From Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, and then **Web Recorder**.
The **Web Recorder (main)** window appears.
2. From the **Transaction** menu, choose **Open**.
The **Select Web Transaction** window appears.

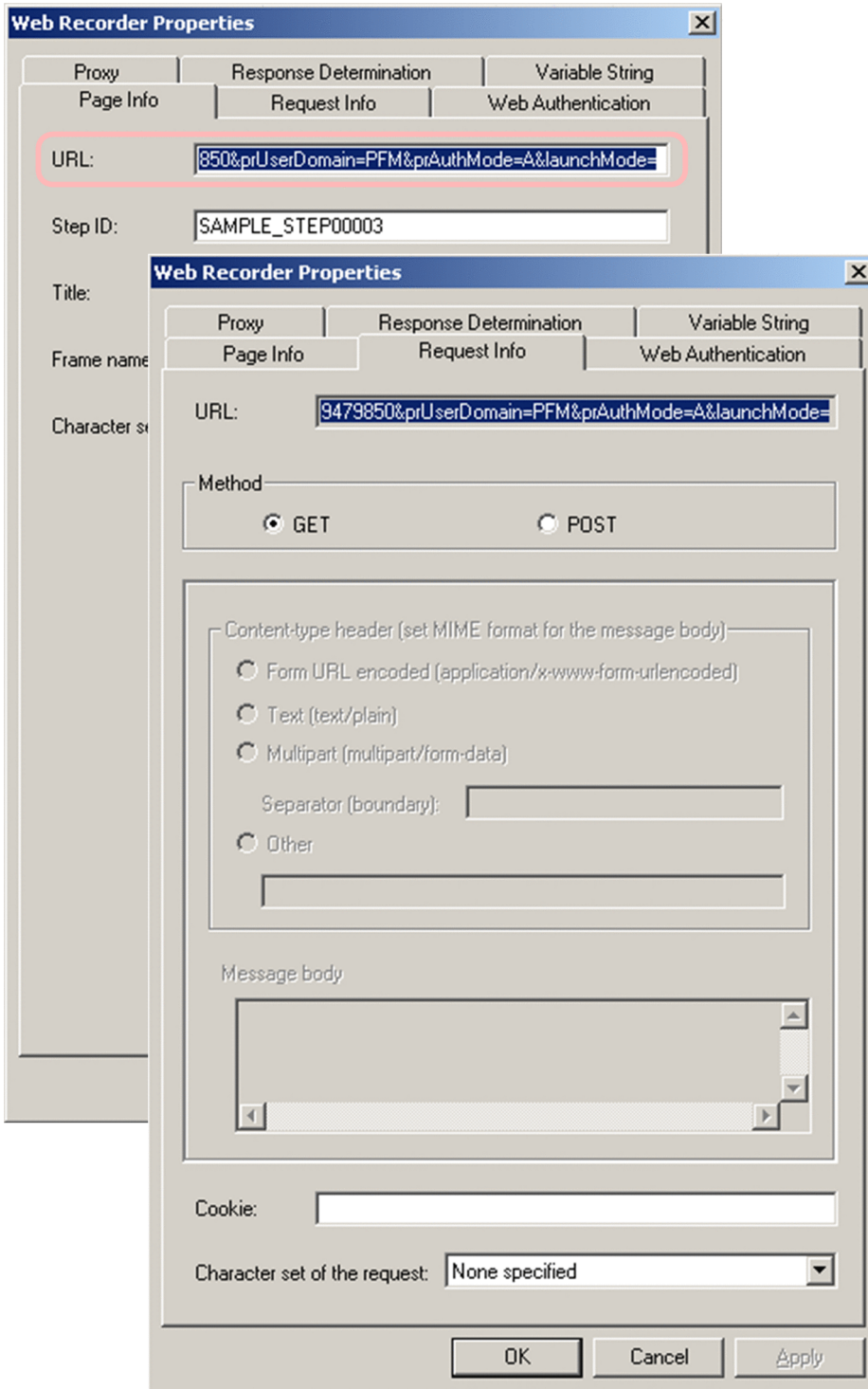


3. From **List of Web transaction files**, select *sample01.xml* and from **List of Web transactions**, select *sample01*, then click the **OK** button.
The specified measurement conditions are read, the **Select Web Transaction** window is closed.
4. In the **Web Recorder (main)** window, from **URL list** select the URL, and from the **Edit** menu choose **Property**.
The **Properties** window appears.



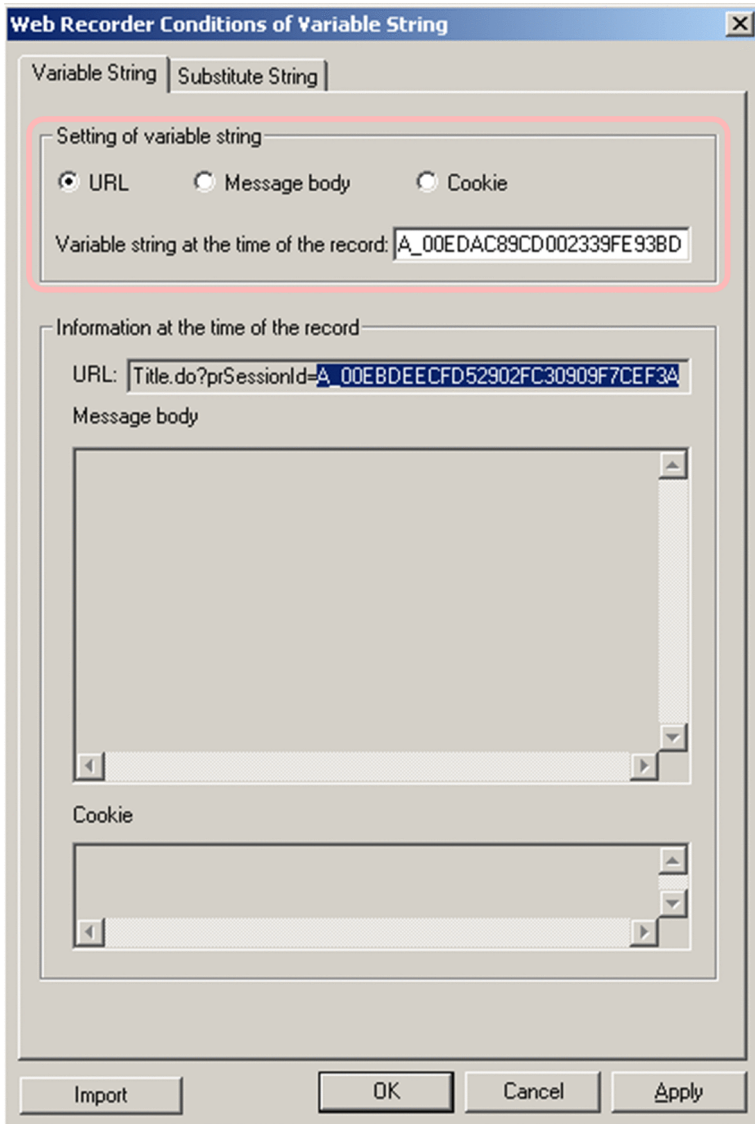
5. Check whether the **URL** in the **Page Info** page or **Message body** in the **Request Info** page contains the variable string.

If the same string (that is, variable string) as which you checked the substitute string in (3) *Testing measurement conditions* exists in either the URL or the Message body, follow the procedures below. If the string does not exist in both pages, skip the remaining procedures.



For details about the **Properties** window, see [7.2.7 Properties window](#).

6. Click the **Variable String** page.
The Variable String page appears.
7. Click the **Add** button.
The **Conditions of Variable String** window appears.
8. Select the location of the variable string checked at the procedure 5 in the **Setting of variable string** of the Variable String page.

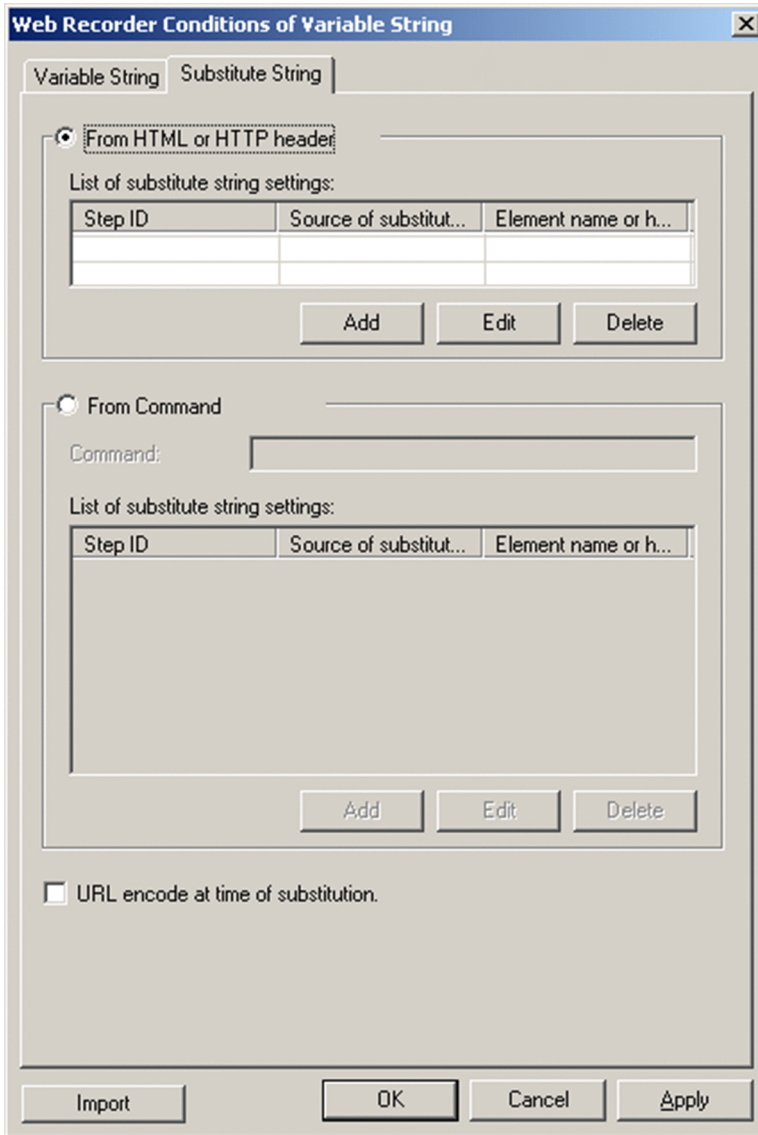


Select either the **URL** or **Message body** button.

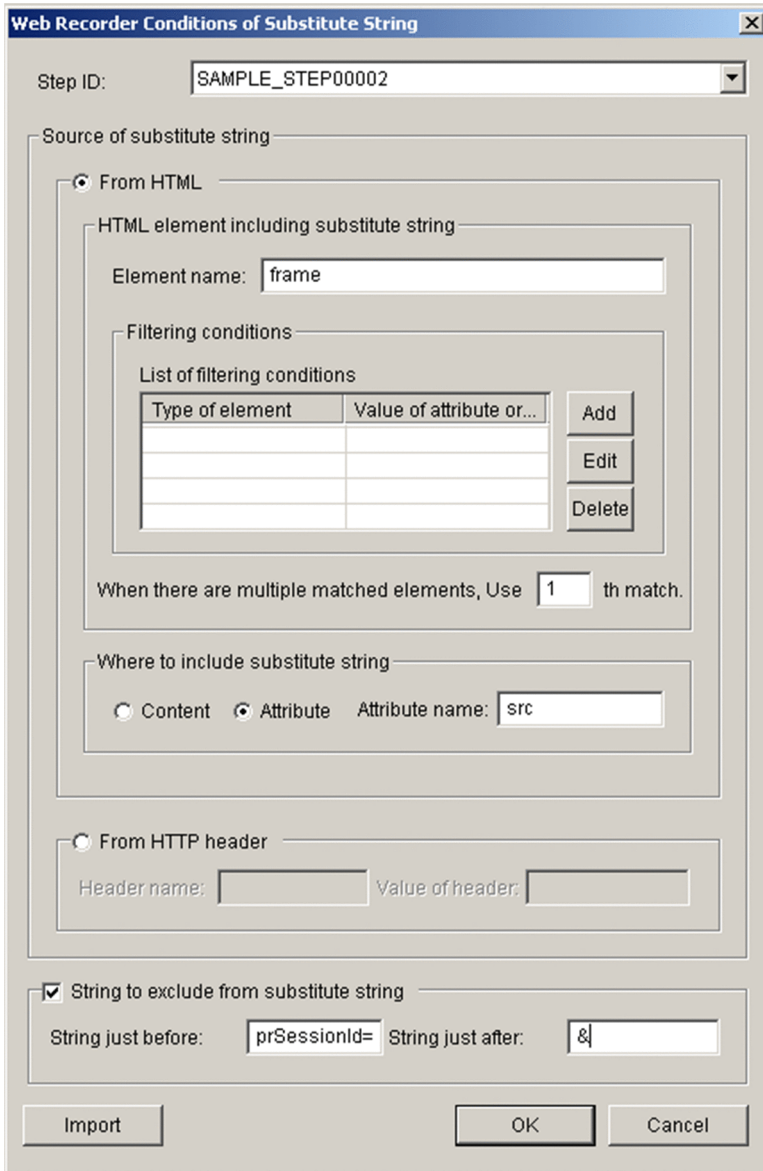
For details about the Conditions of Variable String window, see [7.2.8 Conditions of Variable String window](#).

9. Enter the variable string you checked at the procedure 5 in the **Variable string at the time of the record**.
The variable string when recording is displayed in the **Information at the time of the record**.

10. Click the **Substitute String** page.
The **Substitute String** page appears.



11. Click the **From HTML or HTTP header** button, click the **Add** button.
The **Conditions of Substitute String** window appears.



12. Specify the substitute string in the **Conditions of Substitute String** window.
Specify the values show following table list:

Item to be specified	Value
Step ID	Select <i>SAMPLE_STEP00002</i> .
Source of substitute string	Click the From HTML button.
Element name	Enter <code>frame</code> ^{#1} in the text box.
Where to include substitute string	Click the Attribute button, and enter <code>src</code> ^{#1} in the Attribute name text box.
String to exclude from substitute string	Select the String to exclude from substitute string check box, and enter <code>prSessionId=</code> in the String just before text box, enter <code>&</code> in the String just after text box. ^{#2}

#1

The variable string you checked in (3) *Testing measurement conditions* exists in the `src` attribute of the `<frame>` tag.

#2

These strings surround the variable string when you checked the string in (3) *Testing measurement conditions*.

For details about the Conditions of Substitute String window, see [7.2.10 Conditions of Substitute String window](#).

13. Click the **OK** button in the **Conditions of Substitute String** window.

The Conditions of Substitute String window is closed.

14. Click the **OK** button in the **Conditions of Variable String** window.

The Conditions of Variable String window is closed.

15. Click the **OK** button in the **Properties** window.

The Properties window is closed.

16. Repeat the procedure 4 to 15 for each step containing the variable string in a Web transaction file.

The settings of the variable strings and the substitute strings can be imported by clicking the **Import** button in the Conditions of Variable String window and the Conditions of Substitute String window.

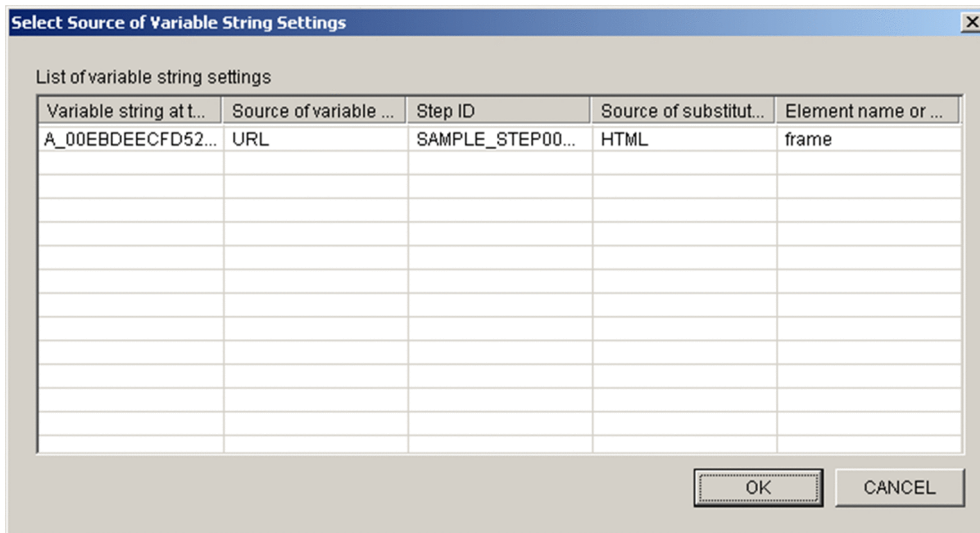
Example:

1. Select the next URL (step ID: SAMPLE_STEP00004) after the URL selected in step 4. Then, from the **Edit** menu choose **Property**.

2. Click the **Add** button on the **Variable String** page. The Conditions of Variable String window appears.

3. In the Conditions of Variable String window, click the **Import** button.

The Conditions of Substitute String window appears.



4. In the Select Source of Variable String Settings window, select **Variable string at the time of the record**, and then click the **OK** button.

The selected variable string appears in the **Variable string at the time of the record** field in the Conditions of Substitute String window.

For details, see the following sections:

When you import the setting of variable strings:

- [7.2.8 Conditions of Variable String window](#)
- [7.2.9 Select Source of Variable String Settings window](#)

When you import the setting of substitute strings:

- [7.2.10 Conditions of Substitute String window](#)
- [7.2.11 Select Source of Substitute String Settings window](#)

17. In the **Web Recorder (main)** window, from the **Transaction** menu, choose **Save**.

The settings are saved in the Web transaction file.

For details about the definitions for supporting dynamic session management, see [4.4.6 Defining settings for the dynamic session management](#).

(5) Web transaction operation check

The following shows the procedures to check the Web transaction measuring:

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**, right-click the *PFM - Agent for Service Response* service in the Services dialog box, and from the pulldown menu choose *Start* (or *Restart*).
2. Open each HTML file under the *installation-folder\agtv\probe\probedata\webtrans* folder by using a text editor, check whether the messages that show the session disconnects or the invalid operations are not output on each HTML file.

The following shows the example of displaying messages:

```
<tr class="v50pr-err-contents">
  <td>Message</td>
  <td class="v50pr-space-normal">
The window displayed for already logout session is operated.
  <br/>
Close the window, re-open the window.
  <td>
</tr>
```

2.4.4 Definition examples (Measurement of IE scenarios)

This section explains the definitions when you measure IE scenarios on the sites with the dynamic session management. PFM - Web Console is taken for example as the sites with the dynamic session management.

To use the IE Recorder, you can create the IE scenario without considering the dynamically changing *session IDs*.

Suppose that you record the following series of procedures in PFM - Web Console as an IE scenario:

1. Logging on to PFM - Web Console
2. Operations by using the PFM - Web Console (Displaying reports)
3. Logging off from PFM - Web Console

The following describes the overview of the procedures to measure this IE scenario correctly:

1. Record IE scenarios
Use the IE Recorder to record IE scenarios.
2. Test IE scenarios
Check whether the recorded IE scenarios are replayed correctly.
3. Register measurement conditions
Register the recorded IE scenarios in the measurement condition registration file.
4. IE scenario operation check

Check whether the IE scenarios are measured correctly.

You can operate the procedures 1 to 3 listed above on the IE Recorder.

The following subsections describe the details of the procedures:

Reference note:

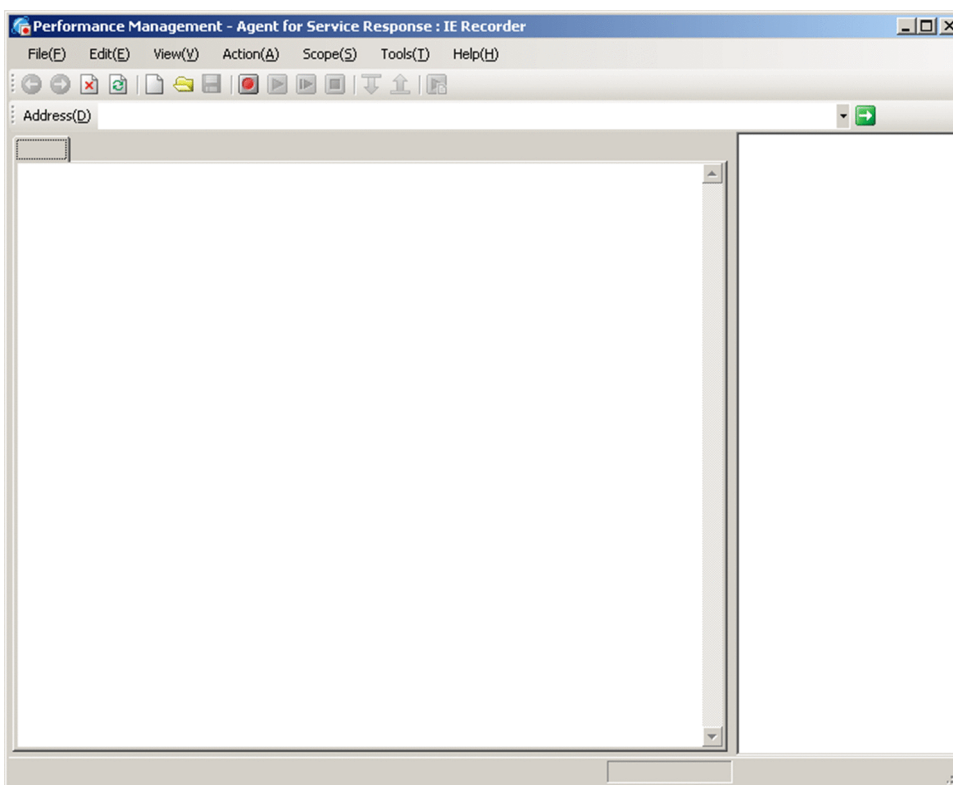
You can operate the IE Recorder using the buttons on the toolbar as well as the commands in the menu bar. For details about the toolbar buttons of the **IE Recorder (main)** window, see [7.3.1 IE Recorder \(main\) window](#).

(1) Recording IE scenarios

The following shows the procedures to record IE scenarios.

1. From Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, and then **IE Recorder**.

The **IE Recorder (main)** window appears.



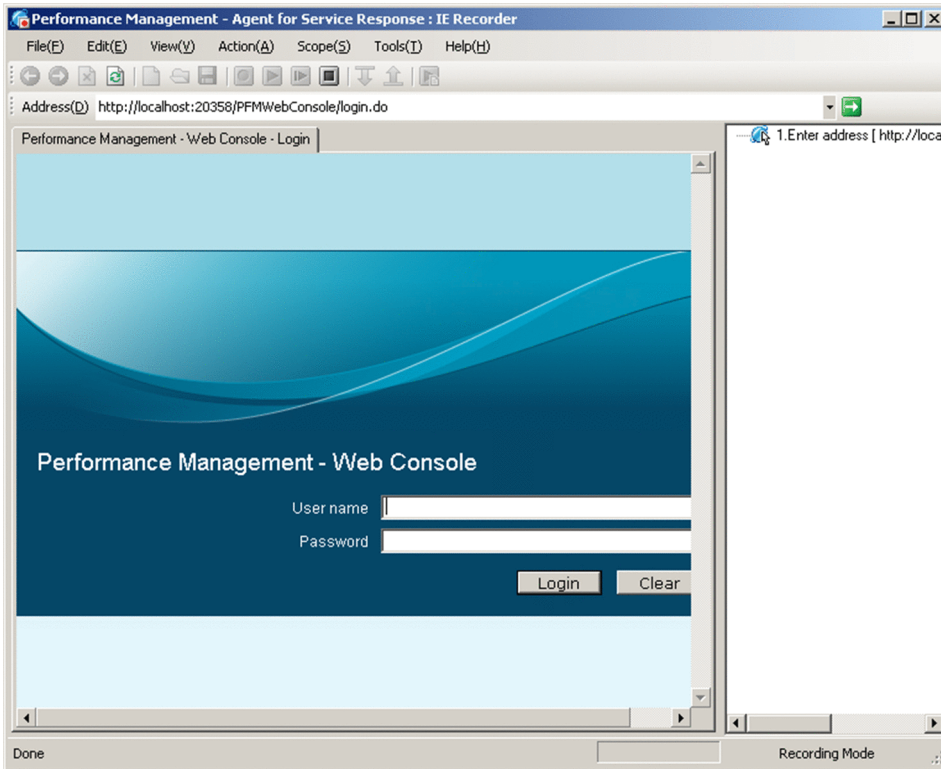
2. From the **Action** menu, choose **Record**.

The IE scenario is started to record.

3. In **Address**, enter the URL of the Login windows of PFM - Web Console.

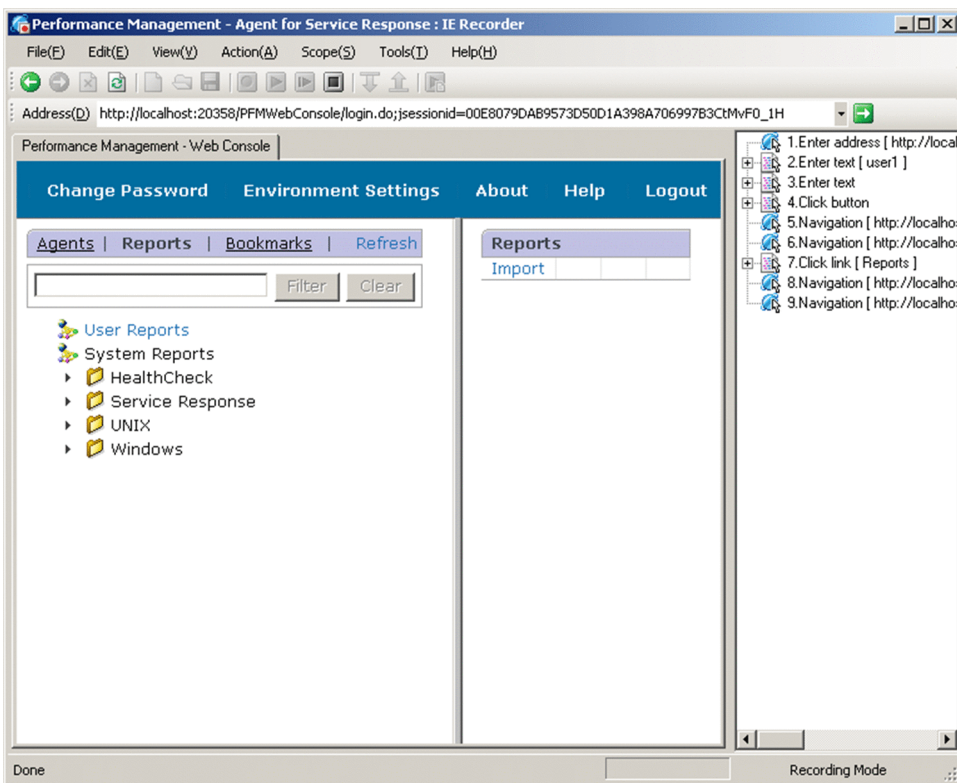
4. From the **View** menu, choose **Go To**.

The **Login** window of PFM - Web Console appears in the **IE window**.



5. Enter a *User name* and *Password* in the **Login** window and click the **Login** button. Log on to PFM - Web Console. The main window appears in the **IE window**.

6. In the navigation frame of the **main** window, select the **Reports** tab.



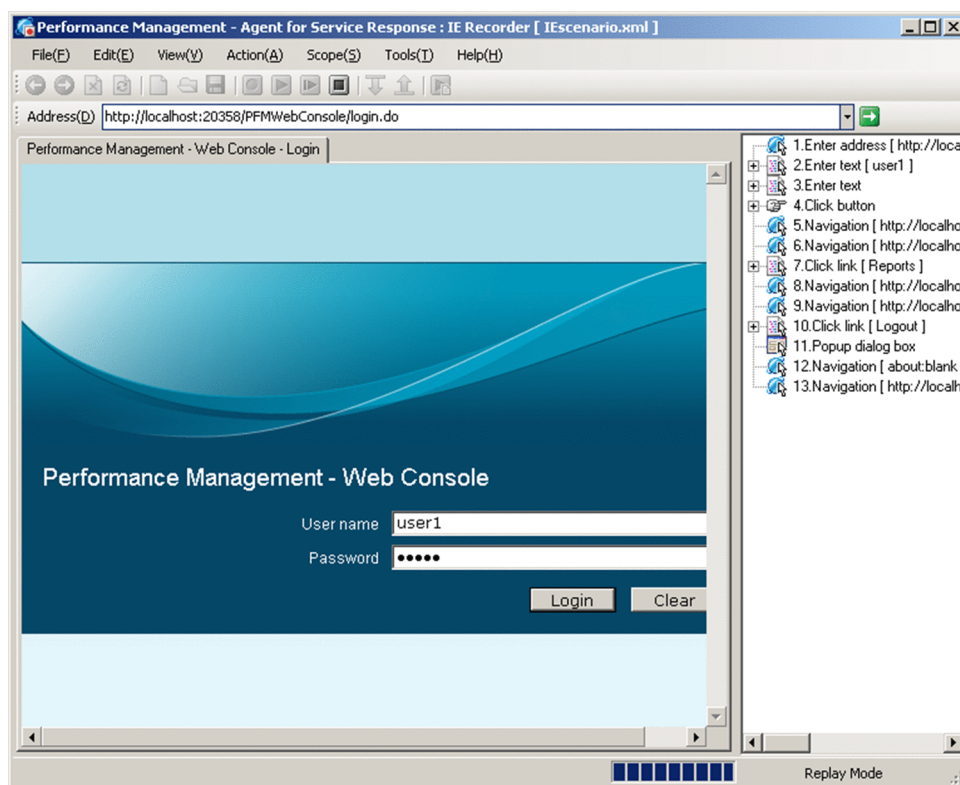
7. In the menu bar frame of the main window, click the **Logout** menu to log off from PFM - Web Console. The **Login** window of PFM - Web Console appears in the **IE window**.

8. From the **Action** menu, choose **Stop**.
The IE scenario is stopped to record.
9. From the **File** menu, choose **Save As**.
The Save As dialog appears.
10. Specify `iescena` folder as the **Save In drop-down** box and `IE-Scenario` as the **File Name**, and then click the **Save** button.
The IE scenario is saved in the IE scenario file.

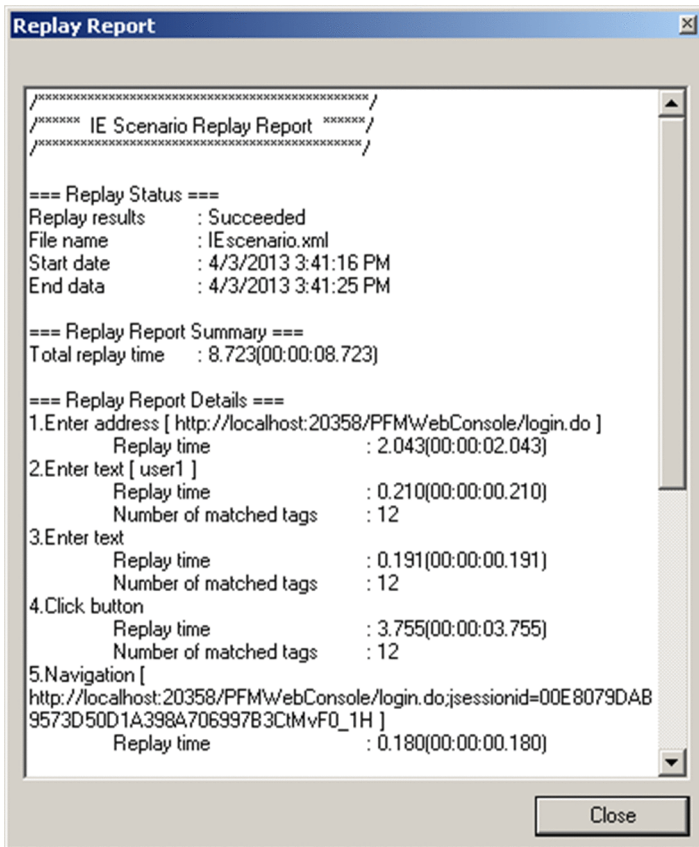
(2) Testing IE scenarios

The following shows the procedures to replay the recorded IE scenarios.

1. In the **IE Recorder (main)** window, from the **Action** menu, choose **Measurement Test**.
The recorded operations are replayed in the IE window.



The result of replaying is displayed in the **Replay Report** window.



For details about the Replay Report window, see [7.3.8 Replay Report window](#).

Reference note:

If the replaying the IE scenario fails, you can identify the cause of the failure by choosing **Replay** or **Replay by Step** from the **Action** menu in the **IE Recorder (main)** window.

(3) Registration measurement conditions

The following shows the procedures to register simply the measurement conditions of the IE scenario in the measurement condition registration file.

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**, right-click the *PFM - Agent for Service Response* service in the Services dialog box, and from the pulldown menu choose **Stop**.

If you use Windows services to start the IE probe service, the IE probe service also stops. In this case, skip procedure 2.#

For details about the configuration for starting the IE probe service using the Windows services, see [5.1.5 Starting and stopping the IE probe service using the Windows services](#).

2. If you start the IE probe from Windows **Start** menu, right-click the **IE Probe** icon on the System Tray, and from the popup menu choose **Exit**.

The IE Probe Daemon service is stopped.

3. In the **IE Recorder (main)** window, from the **Tools** menu, choose **Simplified Registration**.

The message `KAVK38120-I The measurement condition has been registered successfully.` is displayed.

For details about the simplified registration, see [4.5.3 Defining measurement conditions](#).

(4) IE scenario operation check

The following shows the procedures to check the IE scenario measuring:

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**, right-click the *PFM - Agent for Service Response* service in the Services dialog box, and from the pulldown menu choose **Start**.

If you use the Windows services to start the IE probe service, the IE probe service also starts. In this case, skip the procedure 2.#

For details about the setting of starting the IE probe service using the Windows services, see [5.1.5 Starting and stopping the IE probe service using the Windows services](#).

2. From Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, and then **IE Probe**.

The IE Probe Daemon starts.

3. Check that the *output-number_sequence-number_frame-number.html* file is stored in the *installation-folder\agtv\probe\probedata\iescena\ieprobed_measurement-condition-ID\measurement-start-time-for-IE-scenario* folder.

Check whether the following error message is not output in the file.

The following shows the example of displaying messages for failure to measure:

```
(PFM7532)
  </td>
</tr>
<tr class="v50pr-err-contents">

  <td>Message</td>

  <td class="v50pr-space-normal">
The window displayed for already logout session is operated. <br/>
Close the window, and re-open the window.
  </td>
</tr>
</table>
</td>
<td class="v50-dialog-right-contents"></td>
</tr>
```

3

Installation and Setup

This chapter describes the procedures for installing and setting up PFM - Agent for Service Response.

For details about how to install and set up an entire Performance Management system, see the chapter on installation and setup for Windows in the *JP1/Performance Management Planning and Configuration Guide*.

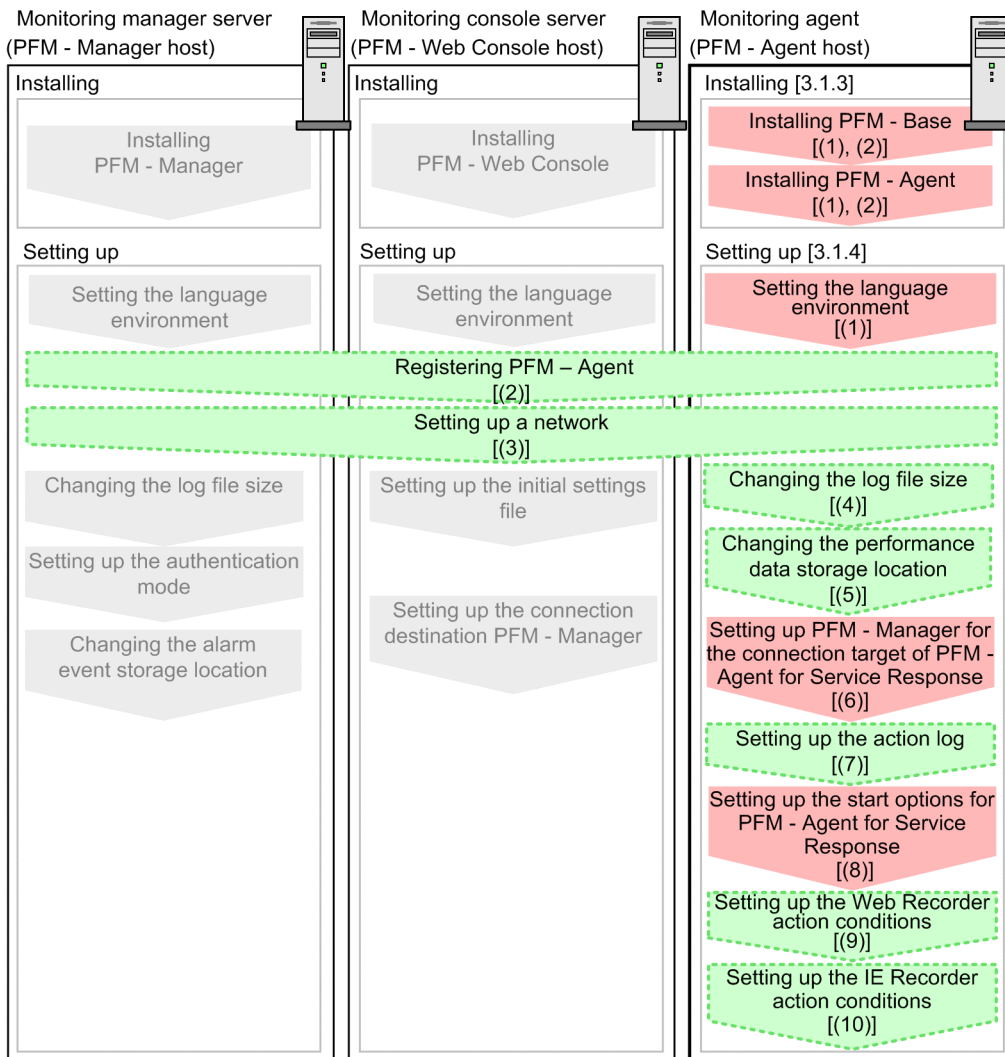
3.1 Installation and setup

This section explains the procedures for installing and setting up PFM - Agent for Service Response.


3.1.1 Installation and setup flow

This subsection describes the procedures for installing and setting up PFM - Agent for Service Response.


Figure 3–1: Installation and setup procedures



Legend:

 : Required setup item

 : Optional setup item

 : Item for which a procedure is described in the *JP1/Performance Management Planning and Configuration* or *JP1/ Performance Management User's Guide*

[] : See the indicated section

For details about how to install and set up PFM - Manager and PFM - Web Console, see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*.

Note that you, for setup commands that require user input, you can select whether to execute such commands interactively or non-interactively.

If you execute a setup command interactively, you need to enter values in accordance with the command directives.

If you execute a setup command non-interactively, user input during command execution is not required because such input can be provided instead by values in option specifications or in definition files. Also, batch processing or remote execution can automate setup operations to reduce administrator workload and operating costs.

For details about commands, see the manual *JPI/Performance Management Reference*.

3.1.2 Before installation and setup

This section describes the items to be checked before installing and setting up PFM - Agent for Service Response.

(1) Requisite OS

PFM - Agent for Service Response can run on the following operating system (OS):

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2016

(2) Network environment setup

This subsection describes the network environment needed for Performance Management operation.

(a) Setting up IP addresses

You must set up the environment for a PFM - Agent for Service Response host in such a manner that IP addresses can be determined from the host names.

PFM - Agent for Service Response cannot start in an environment in which IP addresses cannot be resolved.

Actual host names or alias names can be used for a monitoring host name (the name used as the host name of a Performance Management system).

- When using an actual host name as a monitoring host name
Execute the `hostname` command on a Windows system or `uname -n` command on a UNIX system to check the host name, and set up the environment so that it can resolve IP addresses. Note that on a UNIX system, the host name obtained by the `hostname` command can also be used.
- When using an alias name as a monitoring host name

Set up the environment so that it can resolve the IP addresses for the set alias name.

For details about the configuration of a monitoring host name, see the chapter on installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

Use one of the following methods to set the host name and IP address:

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

Notes:

- Although Performance Management can operate in a DNS environment, do not specify host names in FQDN format. When you specify a monitoring host name, remove the domain name portions.
- If you use Performance Management in multiple LAN environments, use the `jpchosts` file to set IP addresses. For details, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*. Note that the IP addresses set in the `jpchosts` file are not used for resolving the IP addresses of monitored hosts.
- Performance Management cannot be run on a host on which DHCP is used to assign dynamic IP addresses. Set fixed IP addresses on all hosts on which Performance Management is installed.

Because Performance Management supports network configurations for IPv4 environments and IPv6 environments, you can use Performance Management in a network configuration that contains both IPv4 and IPv6 environments. PFM - Agent for Service Response can communicate with PFM - Manager by using IPv6. Note, however, that this applies only when Windows or Linux runs on a host with PFM - Manager installed.

For details about the scope of communication in IPv4 and IPv6 environments, see *K. About Communication in IPv4 Environments and IPv6 Environments*.

To use IPv6 for communication, IPv6 must be enabled on both the PFM - Manager host and the PFM - Agent host by using the `jpccconf ipv6 enable` command.

In addition, before installing PFM - Agent for Service Response, you need to enable the use of IPv6 on the PFM - Agent for Service Response host. You have to execute the `jpccconf ipv6 enable` command to enable this setting. If this setting is already enabled, however, you do not need to execute the command. If you want to check whether the use of IPv6 is enabled, execute the `jpccconf ipv6 display` command.

For details about the `jpccconf ipv6 enable` command and the `jpccconf ipv6 display` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*. For details about the conditions or occasions for executing the `jpccconf ipv6 enable` command, see the chapter that describes network configuration examples in an environment that includes IPv6 in the *JPI/Performance Management Planning and Configuration Guide*.

(b) Setting up port numbers

The port numbers listed in the table below are assigned by default to the Performance Management program services. An available port number is assigned automatically to any other service or program each time such a service is started. You must use fixed port numbers when Performance Management is used in a firewall environment. For details about how to fix port numbers, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

Table 3–1: Default port numbers for Performance Management program services

Service description	Service name	Parameter	Port number	Remarks
Service configuration information management function	Name Server	<code>jp1pcnsvr</code>	22285	Port number used by PFM - Manager's Name Server service. This port number is set at all hosts of Performance Management.
Service status management function	Status Server	<code>jp1pcstatsvr</code>	22350	Port number used by the Status Server service of PFM - Manager and PFM - Base. This port number is set at the host where PFM - Manager and PFM - Base are installed.

Service description	Service name	Parameter	Port number	Remarks
JP1/SLM linkage facility	JP1/ITSLM	--	20905	The port number set by JP1/SLM.

Legend:

--: None

You should set up your network in such a manner that communication can be established with the port numbers used by these PFM - Agent for Service Response programs.

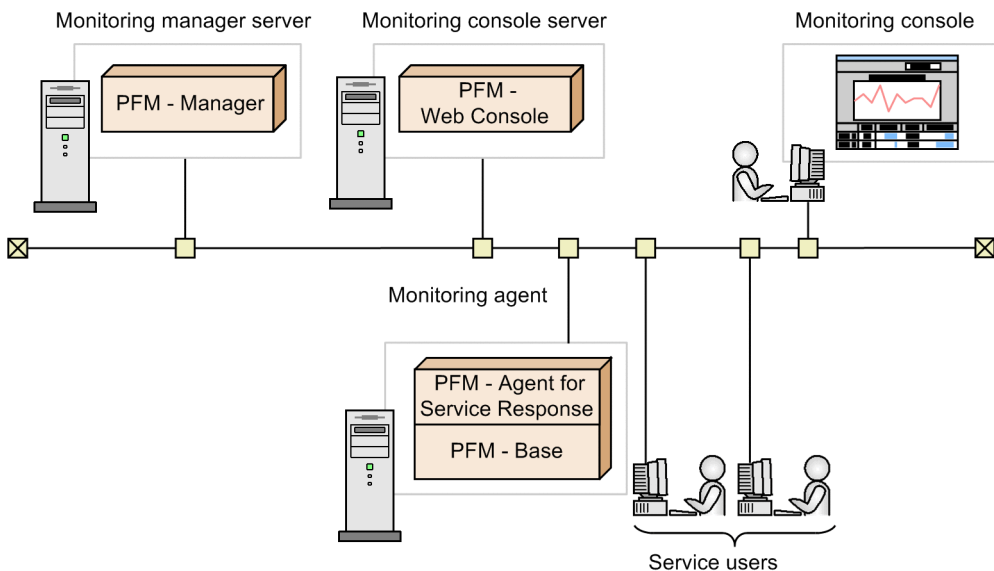
(3) OS user permission necessary for installation

Make sure that you are using an account that has Administrator permissions when you install PFM - Agent for Service Response.


(4) Required programs

This subsection describes the programs that are required to install PFM - Agent for Service Response. The following figure shows the configuration of the programs.

Figure 3–2: Program configuration



Legend:

 : Program provided by Performance Management

PFM - Agent and PFM - Base must be installed on the monitoring agent. PFM - Base is a prerequisite program for PFM - Agent. You need only one PFM - Base even when multiple PFM - Agents are installed on the same host.

Note that if you install PFM - Manager and PFM - Agent on the same host, PFM - Base is not required.

To use PFM - Agent for Service Response to measure and monitor Internet services, you need PFM - Manager and PFM - Web Console.

The response information measured by PFM - Agent for Service Response consists of the response times when a target service is accessed from the machine where PFM - Agent for Service Response is installed. If you install PFM - Agent for Service Response at a location close to the service user's terminal, you can obtain data that is closer to the actual response times experienced by the service user.

The following programs are prerequisite for the IE Recorder and IE Probe Daemon. These programs must be installed on the same host:

- .NET Framework 3.5 (For Windows Server 2012 or later)
- Internet Explorer

(5) Installing and setting up in a cluster system

The required network environment and program configuration are different for a cluster system than for a normal non-cluster system. In a cluster system, installation and setup are required at both the executing and standby nodes. For details, see *6. Operation in a Cluster System*.

(6) Preparation for collecting data in the event of an error

If a problem occurs, memory dumps, user mode process dumps, and other data might be required. To obtain these dumps when a problem has occurred, use one of the following methods to set up output of these dumps in advance.

You can use the following registry setting to obtain user mode process dumps of data that you can investigate for troubleshooting when an application program terminates:

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

Specify the following registry key values:

- DumpFolder: REG_EXPAND_SZ *dump-output-folder-name*
Permission to write to the output destination folder is needed.
- DumpCount: REG_DWORD *Number-of-dumps-to-be-saved*
- DumpType: REG_DWORD 2

Important

- When you set the registry to output user mode process dumps, user mode process dumps are output for not only JP1 programs, but also for other application programs. Make sure you keep this in mind when you specify that user mode process dumps are to be output.
- When user mode process dumps are output, available disk space can be adversely affected. Make sure that you specify a dump output folder that has enough disk space for the dumps.

(7) Notes

This subsection provides notes about installing and setting up Performance Management.

(a) Precautions regarding the registry

PFM - Agent for Service Response can only be run on environments set up using the standard method provided by the OS. Despite the information provided by Microsoft technical support, if the OS environment is customized such as by using a registry editor to directly edit registry information, performance data might no longer be collected properly.

(b) Precautions regarding environment variables

Because Performance Management uses `JPC_HOSTNAME` as an environment variable, do not set it as a user-specific environment variable, as this will prevent Performance Management from operating properly.

(c) Notes on installing and setting up multiple Performance Management programs on the same host

Performance Management enables you to install PFM - Manager, PFM - Web Console, and PFM - Agent on the same host. This subsection provides notes about such an installation.

- If you install PFM - Manager and PFM - Agent on the same host, there is no need to install PFM - Base. In this case, PFM - Agent requires PFM - Manager; therefore, install PFM - Manager first, and then install PFM - Agent.
- PFM - Base and PFM - Manager cannot be installed on the same host. To install PFM - Manager on a host where PFM - Base and PFM - Agent are already installed, uninstall all Performance Management programs (other than PFM - Web Console), and then install PFM - Manager and PFM - Agent in that order. Similarly, to install PFM - Base on a host where PFM - Manager and PFM - Agent are already installed, uninstall all Performance Management programs (other than PFM - Web Console), and then install PFM - Base and PFM - Agent in that order.
- If you install PFM - Agent for Service Response on a host where PFM - Manager is already installed, the PFM - Manager on the local host becomes the connection-target PFM - Manager. In such a case, you can no longer change the connection-target PFM - Manager to a PFM - Manager on a remote host. Therefore, if you want to connect to a PFM - Manager on a remote host, make sure that PFM - Manager has not already been installed on the target host.
- If PFM - Agent for Service Response already exists on the host where PFM - Manager is being installed, the local host is reset as the connection-target PFM - Manager for that PFM - Agent for Service Response. The resulting settings are output to the common message log file; check the results.
- If PFM - Web Console already exists on a host where PFM - Agent for Service Response is to be installed, close all Web browser windows before starting installation.
- When you perform a new installation of a Performance Management program, the status management facility will be enabled by default. To change the setting of the status management facility, see the chapter on error detection for Performance Management in the *JPI/Performance Management User's Guide*.

Hint

To improve system performance and reliability, we recommend running PFM - Manager, PFM - Web Console, and PFM - Agent on separate hosts.

(d) Notes on version upgrade

For details about notes on upgrading the versions of Performance Management programs, see the section describing the notes on version upgrading in the chapter that explains installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

Observe the following precautions when upgrading the version of PFM - Agent for Service Response:

- You cannot upgrade PFM - Agent for Service Response when the IE Recorder or IE Probe Daemon is running. Before upgrade installation, stop the IE Recorder and IE Probe Daemon.

(e) Other notes

- If you are installing PFM - Agent for Service Response in an environment in which no Performance Management program has been installed, make sure that there are no files or folders in the installation-target folder.
- If you attempt to install PFM - Agent for Service Response while Performance Management programs and services are running, or while other programs that reference Performance Management files (such as Windows Event Viewer)

are running, a message prompting for a system restart may be displayed. If this occurs, restart the system according to the message and then complete the installation.

- If you attempt to install PFM - Agent for Service Response while Performance Management programs and services are running, or while other programs that reference Performance Management files (such as Windows Event Viewer) are running, file expansion may fail if there is not enough disk space, or if you do not have folder permission. In such a case, terminate all such programs and then re-install PFM - Agent for Service Response. If there is not enough disk space or if you do not have directory permission, resolve the problem and then re-install PFM - Agent for Service Response.
- When installing the Performance Management program, check whether any of the following security-related programs are installed. If they are installed, perform the measures explained.
 - Security monitoring programs
Stop or change the settings for security monitoring programs so that installation of the Performance Management program is not prevented.
 - Virus detection programs
We recommend that any virus detection programs be stopped before the Performance Management program is installed.
If a virus detection program is running during installation of the Performance Management program, the installation speed might suffer, and installation might not be executed, might not be performed correctly.
 - Process monitoring programs
Stop or change the settings for any process monitoring programs, so that monitoring is not performed for Performance Management services or processes, and Common Component services or processes.
If a process monitoring program starts or stops these services or processes during installation of the Performance Management program, installation might fail.
- You cannot upgrade PFM - Agent for Service Response when the IE Recorder or IE Probe Daemon is running. Before upgrade installation, stop the IE Recorder and IE Probe Daemon.

3.1.3 Installation procedure

This subsection describes the program installation sequence for PFM - Agent for Service Response and how to install the program from the supplied medium.

(1) Program installation sequence

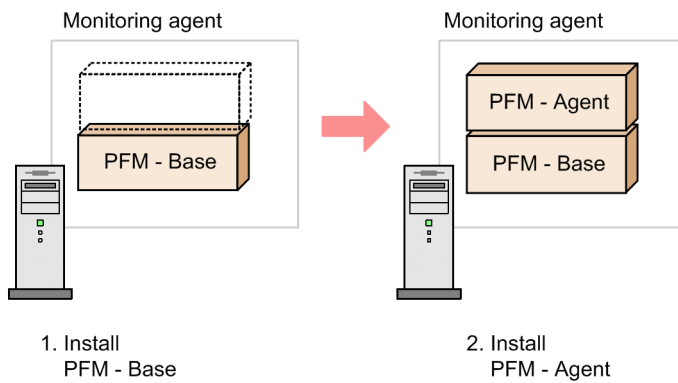
You must install PFM - Base before you install PFM - Agent for Service Response. A PFM - Agent cannot be installed on a host on which PFM - Base has not been installed.

To install PFM - Agent and PFM - Manager on the same host, install PFM - Manager first and then PFM - Agent.

When the Store database version is updated from 1.0 to 2.0, the setup procedure differs depending on the version of PFM - Manager or PFM - Base that is already installed. For details about how to set up version 2.0 of the Store database, see [3.4.2 Updating the Store version to 2.0](#).

Multiple PFM - Agents installed on the same host can be installed in any order.

Figure 3–3: Program installation procedure



(2) Program installation procedure

You can install Performance Management programs on a Windows host either by using the supplied medium or by using JP1/SD to perform a remote installation. For details about the method that uses JP1/SD, see the *Job Management Partner I/Software Distribution Administrator's Guide Volume 1 (for Windows systems)*.

! Important

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

To install from the supplied medium:

1. Log on to the host on which you intend to install the programs as an administrator.
2. If any Performance Management services are running on the local host, stop all of them.
The services you are going to stop are the Performance Management services running on both the physical and logical hosts. For details about how to stop services, see the chapter that explains startup and termination of Performance Management in the *JP1/Performance Management User's Guide*.
In addition, if IE Recorder, IE Probe Daemon, and their services are running, stop all of them.
3. Insert the supplied medium into the machine and execute the installer.
Proceed with installation by following the instructions of the installer that starts.
The following items, which have been set upon the installation of PFM - Manager or PFM - Base, are displayed for your information:
 - User information
 - Installation folder
 - Program folder
4. Click the **Install** button to start the installation process.

3.1.4 PFM - Agent for Service Response setup procedure

This subsection describes the setup that is required before you can use PFM - Agent for Service Response.

Optional indicates a setup item whose requirement depends on the environment being used, or an optional setup item when you wish to change a default setting.

(1) Setting the language environment

Windows has several locations for setting the language environment. The setting must be the same for all of them.

For details about how to set the language environment, see the section describing how to set the language environment in the *JPI/Performance Management Planning and Configuration Guide*.

(2) Registering PFM - Agent for Service Response Optional

To use PFM - Manager and PFM - Web Console for centralized management of PFM - Agents, PFM - Agent for Service Response must be registered into PFM - Manager and PFM - Web Console. You must register PFM - Agent for Service Response in the following cases:

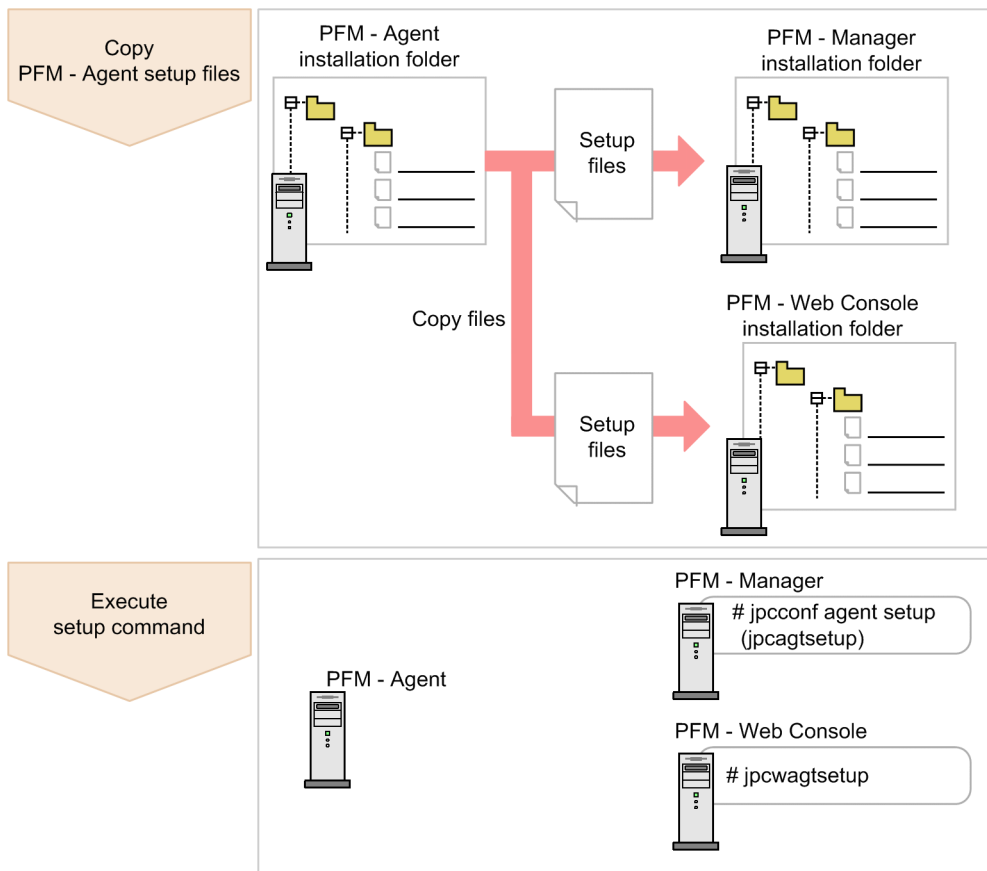
- When a new PFM - Agent for Service Response is installed in the Performance Management system
- When the data model version for the registered PFM - Agent for Service Response is being updated

When the version of PFM - Manager is 09-00 and later, you do not need to perform the procedure explained here, because PFM - Agent is automatically registered.

Note, however, that PFM - Agent or PFM - RM that is *released later* than PFM - Manager might require manual registration. For details about whether manual registration is necessary, see the *Release Notes* for PFM - Manager.

The following figure shows the procedure for registering PFM - Agent for Service Response.

Figure 3–4: Procedure for registering PFM - Agent for Service Response



Note:

- If you are adding the same version of PFM - Agent for Service Response to a Performance Management system in which information about PFM - Agent for Service Response has already been registered, there is no need to register the PFM - Agent.
- If you install a different version of PFM - Agent for Service Response on a separate host, set up the old version first and then the new version.
- If you have installed PFM - Agent on the same host as PFM - Manager, the `jpcconf agent setup` command executes automatically and the message `KAVE05908-I New agent setup ended successfully` is output to the common message log. Check the results, and if the command did not execute correctly, re-execute it. For details about executing commands, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

(a) Copying the PFM - Agent for Service Responsesetup files

Copy the setup files from the host where PFM - Agent for Service Response was installed to the host where PFM - Manager and PFM - Web Console were installed.

To copy the setup files:

1. Stop PFM - Web Console if it is running.
2. Copy the PFM - Agent for Service Response setup files in the binary mode.
The table below shows the source and target locations of the files to be copied.

Table 3–2: Setup files to be copied

Source			PFM - Agent for Service Response setup file
PFM program name	OS	Copy destination folder	
PFM - Manager	Windows	<i>PFM-Manager-installation-folder</i> \setup	<i>installation-folder</i> \setup\jpcagtvw.EXE
	UNIX	/opt/jp1pc/setup/	<i>installation-folder</i> \setup\jpcagtvu.Z
PFM - Web Console	Windows	<i>PFM-Web-Console-installation-folder</i> \setup	<i>installation-folder</i> \setup\jpcagtvw.EXE
	UNIX	/opt/jp1pcwebcon/setup/	<i>installation-folder</i> \setup\jpcagtvu.Z

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

To use PFM - Manager to set up PFM - Agent for Service Response, execute the following command:

```
jpcconf agent setup -key SR
```

Although the above example shows interactive execution, you can also execute the `jpcconf agent setup` command non-interactively. For details about the `jpcconf agent setup` command, see the chapter that explains the commands in the manual *JPI/Performance Management Reference*.

Note:

An error may occur if the `jpcconf agent setup (jpcagtsetup)` command is executed on a local host where Performance Management programs and services have not stopped completely. If an error occurs, make sure that all Performance Management programs and services have stopped completely, and then re-execute the `jpcconf agent setup` command.

After completing this step, you may delete the PFM - Agent for Service Response setup files from the PFM - Manager host.

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

To use PFM - Web Console to set up PFM - Agent for Service Response, execute the following command:

```
jpcwagtsetup
```

After completing this step, you may delete the PFM - Agent setup files from the PFM - Web Console host.

(3) Setting up a network Optional

You must specify network settings only when you change the network configuration where Performance Management is used.

The following two network items can be set:

- IP addresses

Set this information to use Performance Management in a network that is connected to multiple LANs. To set multiple IP addresses, define the host names and IP addresses in the `jpchosts` file. Make sure that there is consistency in the `jpchosts` file specifications throughout the entire Performance Management system.

For details, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

- Port numbers

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

For details about setting port numbers, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

(4) Changing the log file size Optional

Performance Management's operating status is output to a log file unique to Performance Management. This log is called the *common message log*; it consists of two files with a default size of 2,048 kilobytes each. This setting is required only when you wish to change this file size.

For details, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

(5) Changing the performance data storage destination Optional

These settings are required only when you wish to change the storage location, backup folder, export folder, or import folder for the database that stores the performance data managed by PFM - Agent for Service Response.

The default storage locations for the performance data are as follows:

- Storage location: `installation-folder\agtv\store\`
- Backup location: `installation-folder\agtv\store\backup\`
- Partial backup destination folder: `installation-folder\agtv\store\partial\`
- Export location: `installation-folder\agtv\store\dump\`

- Import destination folder: `installation-folder\agtv\store\import\`

For details, see [3.4.1 Changing the performance data storage destination](#).

(6) Setting up PFM - Manager for the connection target of PFM - Agent for Service Response

On the host where PFM - Agent for Service Response is installed, you must specify the PFM - Manager that is to manage that PFM - Agent for Service Response. This PFM - Manager is called the *connection-target PFM - Manager*, and you use the `jpccconf mgrhost define` command to set it.

Notes:

- There can be only one PFM - Manager as the connection destination for a PFM - Agent for Service Response, even when multiple PFM - Agents are installed on the same host. A different PFM - Manager cannot be specified for each PFM - Agent.
- If PFM - Agent for Service Response and PFM - Manager are installed on the same host, the PFM - Manager that is on the local host is automatically the connection-target PFM - Manager. You cannot change the connection-target PFM - Manager to some other PFM - Manager.

To specify the connection-target PFM - Manager:

1. Stop all Performance Management programs and services.

Before you start the setup procedure, you must terminate all Performance Management programs and services that are running on the local host. For details about stopping services, see the chapter that describes starting and stopping Performance Management in the *JPI/Performance Management User's Guide*.

If a Performance Management program or service remains active during execution of the `jpccconf mgrhost define` command, a message is displayed that asks you to terminate the program.

2. Execute the `jpccconf mgrhost define` command with the host name of the connection-target PFM - Manager specified.

For example, if the connection-target PFM - Manager is on host `host01`, specify the command as follows:

```
jpccconf mgrhost define -host host01
```

Although the above example shows interactive execution, you can also execute the `jpccconf mgrhost define` command non-interactively. For details about the `jpccconf mgrhost define` command, see the chapter that explains the commands in the manual *JPI/Performance Management Reference*.

(7) Setting up the action log Optional

You can log information in the action log when, for example, PFM services start and stop, and the status of the connection to PFM - Manager changes. The action log stores history information that is output in conjunction with the alarms for thresholds related to system load and other conditions.

For details about how to set up the action log, see [I. Outputting Action Log Data](#).

(8) Setting up the start options for PFM - Agent for Service Response

At the host where PFM - Agent for Service Response is installed, you must set start options, such as the maximum number of measurement conditions for a probe and the maximum size of a report file.

You set the start options for PFM - Agent for Service Response by editing the Probe action condition definition file. For details about the Probe action condition definition file, see [8.2 Probe action condition definition file \(esp.conf\)](#).

(9) Setting up the Web Recorder action conditions

To use Web Recorder to define Web transactions, you must set action conditions for the Web Recorder at the host where PFM - Agent for Service Response is installed.

You define Web Recorder action conditions by editing the Web Recorder action condition definition file. For details about the Web Recorder action condition definition file, see [8.4 Web Recorder action condition definition file \(wr.conf\)](#).

(10) Setting up the IE Recorder action conditions

To use IE Recorder to define IE scenarios, you must set action conditions for the IE Recorder on the host where PFM - Agent for Service Response is installed.

You define IE Recorder action conditions by editing the IE Recorder action condition definition file. For details about the IE Recorder action condition definition file, see [8.8 IE Recorder action condition definition file \(jpcvierec.conf\)](#).

3.2 Uninstallation and unsetup

This section explains the procedures for uninstalling and unsetting up PFM - Agent for Service Response.

3.2.1 Before uninstallation

This section provides notes about uninstalling and unsetting up PFM - Agent for Service Response.

(1) Note on the OS user permission required for uninstallation

When you uninstall PFM - Agent for Service Response, make sure that you use an account that has Administrator permissions.

(2) Note on the network

Uninstalling a Performance Management program does not delete port numbers defined in the `services` file.

(3) Notes on programs

- If you uninstall PFM - Agent for Service Response while Performance Management programs and services or other programs that reference Performance Management files (such as Windows Event Viewer) are running, some files and folders may remain in the system. In such a case, manually delete all files and folders under the installation folder.
- If you attempt to uninstall PFM - Agent for Service Response while Performance Management programs and services or other programs that reference Performance Management files (such as Windows Event Viewer) are running, a message prompting for a system restart may be displayed. If this occurs, restart the system to complete the uninstallation procedure.
- If PFM - Base and PFM - Agent are both installed on the host, PFM - Base cannot be uninstalled unless you first uninstall PFM - Agent. First, uninstall PFM - Agent, and then uninstall PFM - Base. Similarly, if PFM - Manager and PFM - Agent are both installed on the same host, PFM - Manager cannot be uninstalled unless you first uninstall PFM - Agent; uninstall PFM - Agent, and then uninstall PFM - Manager.

(4) Notes on services

If you uninstall only PFM - Agent, the information on the services that can be displayed using the `jpctool service list` command is not deleted. In this case, delete the service information by using the `jpctool service delete` command on the host on which the PFM - Manager is installed. To apply the deletion of the service information to the PFM - Web Console host, you need to execute the `jpctool service sync` command to synchronize the agent information on the PFM - Manager host and PFM - Web Console host.

For details about how to delete service information, see the section on service deletion in the chapter explaining installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

(5) Other notes

- If you uninstall a Performance Management program from a host on which PFM - Web Console has been installed, close all Web browser windows before starting the uninstallation procedure.
- You cannot uninstall PFM - Agent for Service Response when the IE Recorder or IE Probe Daemon is running. Before uninstallation, stop IE Recorder or IE Probe Daemon.

3.2.2 Unsetup procedures

(1) Canceling the connection-target PFM - Manager

To cancel the connection-target PFM Manager, you need to first delete the service information of the PFM - Agent for Service Response that is connected to the PFM - Manager in question.

For details about how to delete service information, see the section describing how to delete service information in the chapter that explains installation and setup (in Windows) in the *JPI/Performance Management Planning and Configuration Guide*.

To change the connection target to another PFM - Manager, see *3.1.4(6) Setting up PFM - Manager for the connection target of PFM - Agent for Service Response*.

3.2.3 Uninstallation procedure

To uninstall PFM - Agent for Service Response:

1. At the host where PFM - Agent for Service Response is to be uninstalled, log on as a user with Administrator permissions.
2. Stop all Performance Management programs and services at the local host.
Display the service information to make sure that no service is running. For details about stopping services and displaying service information, see the chapter that describes startup and termination of Performance Management in the *JPI/Performance Management User's Guide*.
Stop all Performance Management programs and services that are running on the local host; this includes all services on both physical and logical hosts.
3. Select the Performance Management program to be uninstalled.
In Windows **Control Panel**, choose **Programs and Features**[#], and then select the Performance Management program you want to uninstall.
[#]: This name might differ depending on the Windows version.
4. Select **Remove** and then choose the **OK** button.
The selected program is uninstalled.

Precautions regarding uninstallation:

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

3.3 Changing the PFM - Agent for Service Response system configuration

You must change the system configuration for PFM - Agent for Service Response whenever a change occurs in the system, such as a change in the name of the host at which PFM - Agent for Service Response is installed. This subsection describes how to change the system configuration for PFM - Agent for Service Response.

When you change the system configuration for PFM - Agent for Service Response, you must also change the settings for PFM - Manager and PFM - Web Console. For details about how to change the system configuration for Performance Management, see the chapter that describes installation and setup in the *JP1/Performance Management Planning and Configuration Guide*. Note that when a physical host name or alias name is changed, some instances of PFM - Agent will require specific addition operations, but PFM - Agent for Service Response will not.

3.4 Changing the PFM - Agent for Service Response operation method

It may be necessary to change the operating method for PFM - Agent for Service Response for a reason such as a change in the method of handling the collected operation monitoring data. This section describes how to change the operating method for PFM - Agent for Service Response. For details about how to change the operating method for the overall Performance Management system, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

3.4.1 Changing the performance data storage destination

The performance data collected by PFM - Agent for Service Response is managed in the Store database of the Agent Store service of PFM - Agent for Service Response. The following explains how to change the storage location for performance data.

(1) Using the `jpccconf db define` command to change settings

The Store database uses the following folders to manage the collected performance data. These folders can be changed by using the `jpccconf db define` command. If you need the performance data collected before the Store database storage location is changed, execute the `jpccconf db define` command with the `-move` option specified. For details about the `jpccconf db define` command, see the manual *JPI/Performance Management Reference*.

- Save destination folder
- Backup destination folder
- Partial backup destination folder[#]
- Export destination folder
- Import destination folder[#]

#

This folder can be set only when the Store version is 2.0.

The following table describes the options of the `jpccconf db define` command, including the values that can be specified.

Table 3–3: Options of the command that changes the performance data storage location

Item	Option	Specifiable value (Store 1.0) [#]	Specifiable value (Store 2.0) [#]	Default
Save destination folder	sd	Folder name of 1-127 bytes	Folder name of 1-214 bytes	<i>installation-folder\agtv\store</i>
Backup destination folder	bd	Folder name of 1-127 bytes	Folder name of 1-211 bytes	<i>installation-folder\agtv\store\backup</i>
Partial backup destination folder	pbd	--	Folder name of 1-214 bytes	<i>installation-folder\agtv\store\partial</i>
Maximum backup	bs	1 to 9	1 to 9	5

Item	Option	Specifiable value (Store 1.0)#	Specifiable value (Store 2.0)#	Default
generation number	bs	1 to 9	1 to 9	5
Export destination folder	dd	Folder name of 1-127 bytes	Folder name of 1-127 bytes	<i>installation-folder\agtv\store\dump</i>
Import destination folder	id	--	Folder name of 1-222 bytes	<i>installation-folder\agtv\store\import</i>

Legend:

--: This item cannot be set.

#

The folder name must be an absolute path name or a relative path name from the default Store database folder (*installation-folder\agtv\store*).

(2) Editing the jpcsto.ini file to change settings (for Store version 1.0 only)

If the Store version is 1.0, you can directly edit the `jpcsto.ini` file to change the settings of the above items.

(a) Setting items in jpcsto.ini

The following table lists the label names for which information can be edited in the `jpcsto.ini` file, and other information such as the values that can be specified.

Table 3–4: Performance-data storage location settings (under [Data Section] in `jpcsto.ini`)

Item	Label name	Specifiable value (Store 1.0)#1	Default
Save destination folder	<code>Store Dir#2</code>	Folder name of 1-127 bytes	<i>installation-folder\agtv\store</i>
Backup destination folder	<code>Backup Dir#2</code>	Folder name of 1-127 bytes	<i>installation-folder\agtv\store\backup</i>
Maximum backup generation number	<code>Backup Save</code>	1 to 9	5
Export destination folder	<code>Dump Dir#2</code>	Folder name of 1-127 bytes	<i>installation-folder\agtv\store\dump</i>

#1

- The folder name must be an absolute path name or a relative path name from the default Store database folder (*installation-folder\agtv\store*).
- Characters that can be specified are alphanumeric characters, symbols, and spaces, excluding the characters listed below:

`;, /, *, ?, ', ", <, >, |`

- If the specified value is invalid, the Agent Store service cannot start.

#2

You cannot specify the same folders for Store Dir, Backup Dir, and Dump Dir.

(b) Before editing the jpcsto.ini file

- When changing the Store database folder, make sure that the folder after the change has already been created.
- When the Store database folder is changed, performance data collected before the change can no longer be used. If the performance data collected before the change is needed, carry the data over as follows:
 1. Use the `jpctool db backup` command to back up the performance data stored in the Store database.
 2. Change the Store database folder as shown in (c) *Editing the jpcsto.ini file*.
 3. Use the `jpctool db restore` command to restore the backed up data into the new folder.

(c) Editing the jpcsto.ini file

To edit the `jpcsto.ini` file:

1. Stop the PFM - Agent services.
If PFM - Agent programs and services are running at the local host, stop all of them.
2. Use a program such as a text editor to open the `jpcsto.ini` file.
3. Make necessary changes (for example, change performance data storage folders).
Correct the shaded information shown below, as necessary.

```

:
[Data Section]
Store Dir=.
Backup Dir=.\backup
Backup Save=5
Dump Dir=.\dump
:

```

Notes:

- Do not enter any space characters at the beginning of a line, or before or after an equal sign (=).
 - A period (.) in a label value indicates the default storage folder for the Agent Store service's Store database (*installation-folder\agtv\store*). To change the storage folder, specify a path relative to this folder, or specify the absolute path.
 - To change the Store database storage location, you must already have created the folder that you specify here.
 - The `jpcsto.ini` file contains not only the database storage folder, but also definition information. Make sure that you do not change any values other than in the `[Data Section]` section. If a value outside the `[Data Section]` section is changed, Performance Management may not function normally.
4. Save the `jpcsto.ini` file and then close it.
 5. Start the Performance Management programs and services.

Note:

When you use this procedure to change the Store database folder, the performance data files are not deleted from the previous folder. If these files are no longer necessary, delete only the following files:

- All files with the .DB extension
- All files with the .IDX extension

3.4.2 Updating the Store version to 2.0

The Store database comes in two versions, 1.0 and 2.0. The difference between the two versions is the saving format. For details about Store 2.0, see the *JP1/Performance Management Planning and Configuration Guide*.

Version 2.0 of the Store database is set up by default in the following case: PFM - Agent for Service Response 09-00 or a later version is installed as a new installation in an environment in which PFM - Base or PFM - Manager whose version is 08-11 or later is installed. In other cases, the Store version remains 1.0. If you want to use Store 2.0, you must use a setup command to update the version to 2.0.

If you have to restore Store 1.0 from Store 2.0, perform unsetup of Store 2.0.

The following table describes the installation conditions, whether Store 2.0 is available for the given conditions, and the procedure for enabling Store 2.0.

Table 3–5: Availability of Store 2.0 and the procedure for enabling it

Installation conditions		Whether Store 2.0 is available	Procedure for enabling Store 2.0
Version of installed PFM - Base or PFM - Manager	PFM - Agent installation type		
Earlier than 08-11	Overwrite installation	No	Update the version of PFM - Base or PFM - Manager to 08-11 or later, and then execute the setup command.
	New installation		
08-11 or later	Overwrite installation	Available after setup	Execute the setup command.
	New installation	Yes	None

(1) Setup of Store 2.0

The following shows the setup procedure required when the Store version is updated to 2.0.

1. Estimate the system resources and determine the retention period.

Check whether the system resources that Store 2.0 requires are suitable for the execution environment. The system resources to be considered are the following:

- Disk capacity
- Number of files
- Number of files opened by one process

These can be adjusted by the retention period settings. When you specify the retention period, take into account the resources available in the execution environment. For details about estimating the system resources, see the *Release Notes*.

2. Review the folder settings.

When the Store version is updated to 2.0, the Agent Store service might fail to start with the same folder settings that were available in Store 1.0. For this reason, you must review the settings of the folders used by the Agent Store service. You can use the `jpccconf db define` command to view and change the settings of these folders.

The maximum length of the names of the save destination folder, backup destination folder, and other folders used by the Store database in Store 2.0 differs from the maximum length in Store 1.0. In particular, be careful when the folder settings have been changed to use a relative path name in Store 1.0. If the settings have been changed, confirm that the length of the absolute path name for the relative path name is no more than 214 bytes, which is the maximum length for folder names in Store 2.0. If the absolute path name is longer than the maximum, change the settings of each folder used by the Agent Store service before proceeding to the next step.

3. Execute the setup command.

Execute the following command to update the Store version to 2.0:

```
jpccconf db vrset -ver 2.0 -key SR
```

For details about the `jpccconf db vrset` command, see the manual *JPI/Performance Management Reference*.

4. Set the retention period.

Specify the retention period that you determined in step 1. Start the Agent Store service, and then specify the retention period in PFM - Web Console.

(2) Unsetup of Store 2.0

Use the `jpccconf db vrset -ver 1.0` command to perform unsetup of Store 2.0. When unsetup is performed, the entire Store database is initialized and the Store version reverts to 1.0.

For details about the `jpccconf db vrset` command, see the manual *JPI/Performance Management Reference*.

(3) Precautions

The following explains precautions regarding migration.

(a) When migrating from Store version 1.0 to Store version 2.0

When the Store database is migrated from Store version 1.0 to Store version 2.0, retention period settings for records of the PI record type are carried over. For records of the PD record type, however, the default number of retention days is set for each record regardless of the previously set value (number of retained records), and data collected before the number of retention days is deleted.

For example, in Store version 1.0, when the number of retained records is set to 1,000 for PD records for which **Collection Interval** is set to 3,600 seconds, 24 PD records are retained in a day. As a result, data for 1,000 / 24 (roughly 42) days is retained. After this Store database has been migrated to Store version 2.0, if the default number of retention days is set to 10, data from 11 or more days before is deleted and can no longer be viewed.

Before migrating to Store version 2.0, check the settings for the number of retained records for records of the PD record type. If data is set to be retained for the default number of retention days or more for Store version 2.0, use the `jpctool db dump` command to output the data in the database. For details about the default number of retention days in Store version 2.0, see the *Release Notes*.

(b) When returning from Store version 2.0 to Store version 1.0

When unsetup is performed for Store version 2.0, data is initialized. Therefore, before changing to Store version 1.0, use the `jpctool db dump` command to output Store version 2.0 information.

3.4.3 Changing the integrated trace log function settings

PFM - Agent for Service Response uses the Hitachi Network Objectplaza Trace Library (HNTRLib2) to output measurement processing log information. In the event of a failure, this log file is useful for determining the cause.

The following table shows the default settings for output of log files using the Hitachi Network Objectplaza Trace Library (HNTRLib2).

Table 3–6: Default values for log files

Item	Default value
Size of log file	256 kilobytes
Number of log files	4
Log file output destination folder	<i>system-drive</i> \Program Files\Hitachi\HNTRLib2\spool

You use the `hntr2util` command to change default settings.

When you execute the `hntr2util` command, the Hitachi Network Objectplaza Trace Utility 2 dialog box appears, enabling you to change any of the items listed in Table 2-6.

For details about the `hntr2util` command, see *hntr2util (changes the integrated trace log settings)* in *11. Commands*.

3.4.4 Interpolating performance data

PFM - Agent for Service Response might not collect the performance data during a certain period of time, depending on the collection interval time of the Agent Collector and the measurement interval time of the Probe Daemon and the IE Probe Daemon.

This section describes how to turn on the data interpolation function using the last collected data. For details about the cases where the lack of collecting performance data occurs, see *5.2.2(2) Notes about Agent Collector's collection interval settings*.

The **Data Interpolation** property determines the behavior of the performance data interpolation. To edit the **Data Interpolation** property:

1. From the monitoring console Web browser, log in to PFM - Web Console.
The Main window appears.
2. In the navigation frame of the Main window, click the **Services** tab.
The **Services** page appears.
3. From the navigation frame, select the Agent Collector service.
The **Properties** page appears.
4. Select the **Agent** tree.
5. Set the value of the **Data Interpolation** property.
When interpolating data, specify **Yes**. When not interpolating data, specify **No**. The default value of the **Data Interpolation** is **No**.
6. Click the **OK** button.

Reference note:

Hitachi recommends that the collection intervals of the Agent collector and the measurement interval of the Probe Daemon and the IE Probe Daemon should be properly set in order to continue collecting the performance data.

3.5 Backup and restoration

This section describes back up and restoring PFM - Agent for Service Response.

As a protection in the event of a failure and resulting damage to the system, you should back up the settings for PFM - Agent for Service Response on a regular basis. You should also back up the settings when any change has been made to the system, such as when PFM - Agent for Service Response is set up.

For details about backup and restoration of the entire Performance Management system, see the chapter that describes backup and restoration in the *JPI/Performance Management User's Guide*.

3.5.1 Backup

When you back up the configuration files, you back up those files in any measure (such as copying the files). To copy files manually, make sure that all services of PFM - Agent for Service Response have stopped. To use a backup script, see the chapter that describes backup and restoration in the *JPI/Performance Management User's Guide*.

Note:

When you back up the configuration files, record the product version number of PFM - Agent for Service Response. For details about the product version number, see the *Release Notes*.

While you are backing up the files, do not change a file being backed up. If you make any changes, the files will not be backed up correctly.

The files to be backed up are changed when you perform one of the following operations:

- Change a file by using a utility such as a text editor.
- Register, delete or, change measurement conditions by using Web Console
- Register measurement conditions or edit a measurement condition registration file by using the IE Recorder
- Change an IE scenario file or Web transaction file by using the IE Recorder or Web Recorder
- Change a password file by using the `esppasswd` command

The following table lists the files to be backed up for PFM - Agent for Service Response information.

For details about other files, see the section presenting a list of files to be backed up for PFM - Agent for Service Response (in Windows) in the *JPI/Performance Management User's Guide*.

Table 3–7: Files to be backed up for PFM - Agent for Service Response (when any measure is used)

File name	Description
<code>installation-folder\agtv\agent*.ini</code>	Settings files for the Agent Collector service
<code>installation-folder\agtv\store*.ini</code>	Settings files for the Agent Store service
Files under <code>installation-folder\agtv\probe\conf</code>	Each settings file
Files under <code>installation-folder\agtv\probe\task\esp</code>	Measurement condition registration files
<code>installation-folder\agtv\probe\task\esp*.dat</code>	Relay files for internal processing of the measurement pause

File name	Description
Files under <i>installation-folder</i> \agtv\probe\passwd	Password files
Files under <i>installation-folder</i> \agtv\probe\webtrans	Web transaction files
Files under <i>installation-folder</i> \agtv\probe\iescena	IE scenario files
Files under <i>installation-folder</i> \agtv\probe\user	User-defined commands
Files under <i>installation-folder</i> \agtv\probe\cert	Certificates
<i>folder-on-shared-disk</i> \jp1pc\agtv\agent*.ini	Settings files for the Agent Collector service (only in a cluster configuration)
<i>folder-on-shared-disk</i> \jp1pc\agtv\store*.ini	Settings files for the Agent Store service (only in a cluster configuration)
Files under <i>folder-on-shared-disk</i> \jp1pc\agtv\probe\task\esp	Measurement condition registration files (only in a cluster configuration)

3.5.2 Restoration

When restoring settings information for PFM - Agent for Service Response, check the following prerequisites, and then copy the backed up files to their original locations. The backed up settings information files will overwrite the settings information files on the host.

Prerequisites:

- PFM - Agent for Service Response has been installed.
- All services of PFM - Agent for Service Response have stopped.

Note:

When settings information for PFM - Agent for Service Response is restored, the product version number of the backed up environment and restored environment must be identical. For details about product version numbers, see the *Release Notes*.

3.6 Settings for browsing manuals in a Web browser

The manual for Performance Management can be viewed in a Web browser by copying the manual from the manual supplied medium shipped with the program product, to the host on which PFM - Web Console is installed. When running PFM - Web Console on a cluster, copy the manuals on each physical host for the active node and standby node.

3.6.1 Setting required to view manuals

(1) When browsing the manual from the help section of PFM - Web Console

1. Follow the setup procedures for PFM - Web Console, and register PFM - Agent with PFM - Web Console (perform additional setup for PFM - Agent).
2. Create the directory into which the manual will be copied, on the host on which PFM - Web Console is installed.
 - For Windows: *Web-Console-installation-folder*\doc\language-code*PFM-Agent-help-id*
 - For UNIX: /opt/jp1pcwebcon/doc/language-code/*PFM-Agent-help-id*
For details about the PFM - Agent help ID specified for *PFM-Agent-help-id*, see the list of IDs given in the appendix of this manual.
3. Copy the following files and directories from the manual supplied medium to the directory created above.

For HTML manuals

For Windows: All HTML files and the FIGURE folder, in *applicable-drive*\MAN\3021*materials-number* (such as 03004A0D)

For UNIX: All HTML files and the GRAPHICS folder, in /*distribution-media-mount-point*/MAN/3021/*materials-number* (such as 03004A0D)

For PDF manuals

For Windows: PDF files in *applicable-drive*\MAN\3021*materials-number* (such as 03004A0D)

For UNIX: PDF files in /*distribution-media-mount-point*/MAN/3021/*materials-number* (such as 03004A0D)

When copying, make sure to copy the INDEX . HTM file for the HTML manual, or the PDF files for the PDF manual, is placed directly within the created directory.

4. Restart PFM - Web Console.

(2) When browsing the manual from the hard disk drive on the local machine

Perform installation using `setup.exe` on the supplied medium, or by directly copying the HTML files, `STYLE2.CSS` file, PDF files, and GIF files to the desired folder. For the HTML manual, use the following directory configuration:

```
html (HTML files, CSS file, and PDF files)
└─ GRAPHICS (GIF files)
```

3.6.2 Viewing manuals

To browse the manual:

1. From the menu bar frame of the Main window for PFM - Web Console, click the **Help** menu to display a help selection window.
2. Click the manual name, or **PDF** next to the manual name.
When the manual name is clicked, the HTML manual is displayed. When **PDF** is clicked, the PDF manual is displayed.

Precautions regarding character display in Web browsers:

In Windows, when the online manual is displayed from the **Start** menu, the HTML manual might be displayed in a Web browser window that is already open.

4

Definitions for Measuring Services

This chapter describes the definitions for using PFM - Agent for Service Response to measure the response performance of services.

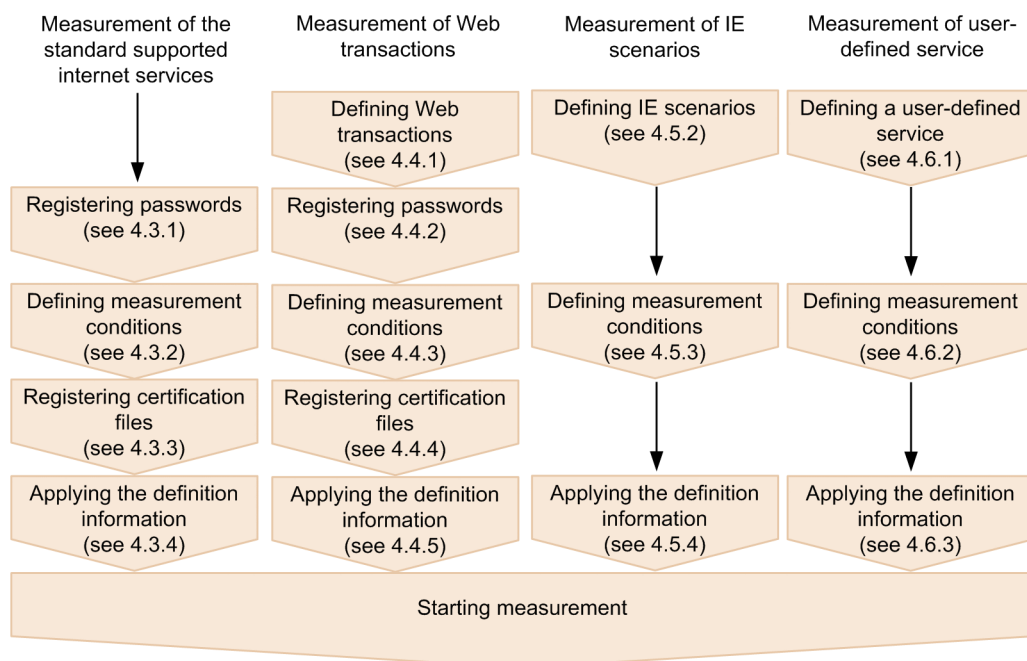
4.1 Definition procedure

There are four modes of measurement when PFM - Agent for Service Response is used:

- Measurement of the standard Internet services supported by PFM - Agent for Service Response
- Measurement of Web transactions
- Measurement of IE scenarios
- Measurement of user-defined services

The following figure shows the definition procedure for each mode. For details about each procedure, see the indicated sections.

Figure 4–1: Definition procedures for measuring Internet services



You can define the measurement conditions in PFM - Web Console. For details about defining the measurement conditions, see [4.7 Defining measurement conditions in PFM - Web Console](#).

4.2 Notes on service measurement definition

In PFM - Agent for Service Response, the Probe Daemon and the IE Probe Daemon measure an Internet service's response performance, and Agent Collector collects the results as performance data. Therefore, you must set the Probe Daemon's measurement interval and the IE Probe Daemon's measurement interval so that they are the same as or less than the Agent Collector's measurement interval. Also, the Probe Daemon's timeout value and the IE Probe Daemon's timeout value must be smaller than the Agent Collector's collection interval.

For details about the data collection schedule, see [5.2.2 Notes about the functions of PFM - Agent for Service Response](#).

4.3 Definitions for measuring Internet services

To measure the standard Internet services supported by PFM - Agent for Service Response, you must do the following:

- Register passwords
- Define measurement conditions
- Register certification files (Optional)
- Applying the definition information

4.3.1 Registering passwords

To measure the Internet services listed in the table below, you must register the passwords that are required to access the target Internet services.

Table 4–1: Internet services that require password registration

Service	Condition	Password to be registered
HTTP, HTTPS	Web page requiring authentication	Password for the Web page
HTTP, HTTPS	Use of a proxy that requires authentication	Password for the proxy
HTTPS	Client authentication is to be performed	Private key password
SMTP	POP3 (POP before SMTP) authentication is to be performed	Password for the POP3 server
POP3	Required	Password for the POP3 server
IMAP4	Required	Password for the IMAP4 server
FTP	Required	Password for the FTP server

You use the *password utility* (`esppasswd` command) to register passwords. Each registered password is converted to character string format and then stored in the password file (`esp.pdb`).

Password file storage location:

```
installation-folder\agtv\probe\passwd
```

For details about how to use the password utility, see *esppasswd (registers, changes, and deletes passwords)* in *11. Commands*.

4.3.2 Defining measurement conditions

You use PFM - Web Console to define measurement conditions for measuring an Internet service in the measurement condition registration file (`esptask.xml`) (or you can edit the file directly and define the conditions).

This subsection describes the Internet services that can be specified as measurement targets, the measurement items, and how to create a measurement condition registration file.

(1) Measurement target and measurement items

The following table lists the standard Internet services supported by PFM - Agent for Service Response and the measurement items for each service.

Table 4–2: List of measurement target services and measurement items

Measurement target service	Measurement items
HTTP	<ul style="list-style-type: none"> • Total response time • Setup time • HTTP time • DNS time • TCP connection time • Server processing time • Data transfer time • Total amount of data • Number of requests • Total size of resources • Throughput
HTTPS	Same as the HTTP measurement items
SMTP	<ul style="list-style-type: none"> • Total response time • Setup time • SMTP time • DNS time • TCP connection time • Preprocessing time • Data transfer time • Total amount of data • Throughput
POP3	<ul style="list-style-type: none"> • Total response time • Setup time • POP time • DNS time • TCP connection time • Preprocessing time • Data transfer time • Deletion time • Total amount of data • Total size of emails • Number of downloaded emails • Throughput
IMAP4	<ul style="list-style-type: none"> • Total response time • Setup time • IMAP time • DNS time • TCP connection time • Preprocessing time • Data transfer time • Deletion time • Total amount of data • Total size of emails • Number of downloaded emails

Measurement target service	Measurement items
IMAP4	<ul style="list-style-type: none"> • Throughput
DNS	<ul style="list-style-type: none"> • Total response time • Total amount of data
DHCP	<ul style="list-style-type: none"> • Total response time • Address presentation time • Address acquisition time • Total amount of data
FTP	<ul style="list-style-type: none"> • Total response time • Setup time • FTP time • DNS time • TCP connection time • Preprocessing time • Data transfer time • Size of transferred file • Total amount of data • Throughput
TCP	<ul style="list-style-type: none"> • Total response time • DNS time • TCP connection time

For details about the measurement items for each service, see [10. Records](#).

(2) Creating the measurement condition registration file (esptask.xml)

To specify measurement conditions for the target Internet services, you must create a measurement condition registration file (`esptask.xml`). You can define measurement condition registration file in PFM - Web Console. The measurement condition registration file contains settings common to all services, as well as settings specific to individual services.

The following table lists and describes the settings that are common to all services.

Table 4–3: List of measurement condition items (common to all services)

Item	Description
Measurement condition ID	Specifies an identifier for the measurement condition. Each measurement condition ID must be unique.
Measurement interval	Specifies a measurement interval.
Timeout	Specifies the timeout value for each measurement.
Service-specific conditions	Specifies definitions for the target service.

The items common to all services include settings such as the measurement interval and a timeout value for the target service. Measurement conditions are managed by the measurement condition IDs. You can register the same measurement condition for the same target service under different measurement condition IDs in order to treat them as separate measurement conditions. For details about the service-specific settings and the measurement condition registration file, see [8.3 Measurement condition registration file \(esptask.xml\)](#).

You save the created measurement condition registration file in the following folder:

Measurement condition registration file storage folder:

installation-folder\agtv\probe\task\esp

4.3.3 Registering certification files

To apply server authentication and client authentication during measurement of Web transactions, you must register a certification file in the same way as for measurement by using the HTTPS probe. For details, see [HTTPS \(PI_HTTPS\)](#) in *10. Records*.

4.3.4 Applying the definition information

To apply the definition information, use either of the following methods:

- Reloading the definition information by using PFM - Web Console
For details about how to reload the definition information from PFM - Web Console, see [4.7.4 Applying the Task information](#).
- Restarting PFM - Agent for Service Response and reloading the definition information
If you perform one of the following operations, you need to restart PFM - Agent for Service Response and reload the definition information:
 - Add, change, or delete the definitions by editing the Probe action condition definition file (`esp.conf`).
 - Add, change, or delete the measurement conditions by directly editing the measurement condition registration file (`esptask.xml`).
 - Change or delete passwords.
 - Change or delete the certification file.

Make sure that you stop PFM - Agent for Service Response before directly editing the measurement condition registration file (`esptask.xml`). If you directly edit the file while PFM - Agent for Service Response is running, and then perform operations from PFM - Web Console, the edited definition information might be lost.

For details about how to start and stop PFM - Agent for Service Response, see [5.1 Starting and stopping PFM - Agent for Service Response](#).

4.4 Definitions for measuring Web transactions

To measure Web transactions, you must perform the following:

- Define Web transactions
- Register passwords
- Define measurement conditions
- Register certification files (Optional)
- Apply the definition information
- Define the settings for the dynamic session management (Optional)

4.4.1 Defining Web transactions (creating Web transaction files)

You create a Web transaction file for each Web page frame that is accessed by a series of transitions. A Web transaction file contains information such as the URLs, the Web authentications, and the use of a proxy.

There are two ways to create a Web transaction file:

- By using Web Recorder
If there is a large amount of information to be defined for a Web transaction, it is easiest to use Web Recorder to create a Web transaction file.
- By editing the Web transaction file directly
If there is only a small amount of information to be defined for a Web transaction, you can directly edit the Web transaction file.
Web transaction files must be stored in the folder shown below. They can have any name, but the extension must be `.xml`. All files with the extension `xml` under this folder are handled as Web transaction files.

Web transaction file storage folder:

```
installation-folder\agtv\probe\webtrans
```

For details about the format of Web transaction files, see [8.5 Web transaction files](#).

This subsection describes how to use Web Recorder to create a Web transaction file.

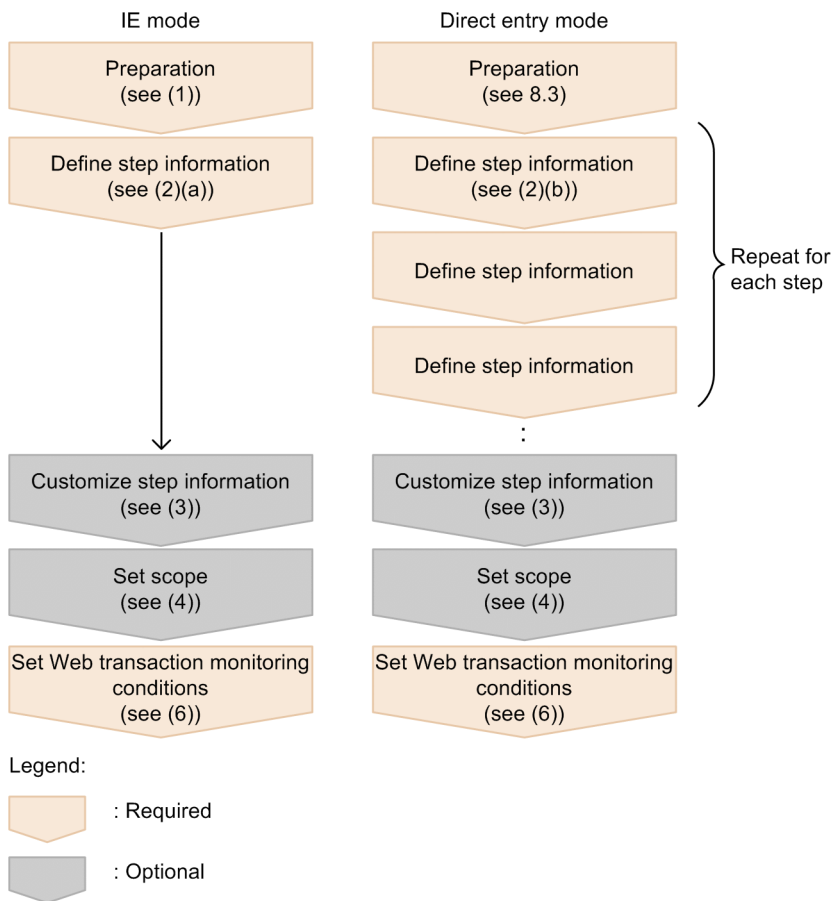
(1) Procedures for creating a Web transaction file

Web Recorder operates in the following two modes:

- IE mode
In this mode, an Internet Explorer window is called from Web Recorder, which defines the Web transaction by recording the browser operations (navigations) performed in that window. You can display the Internet Explorer window by entering only the first URL that you use to navigate to the site that is to be accessed.
- Direct entry mode
In this mode, you define the Web transaction by directly entering the series of URLs without navigating from the Internet Explorer window.

The following shows the procedure for defining a Web transaction in each mode. For details about each procedure, see the indicated section.

Figure 4–2: Procedures for defining a Web transaction



This subsection describes the procedure for defining a Web transaction when you use Web Recorder.

Preparations for defining a Web transaction

Before starting a definition of a Web transaction, you must select the series of processes that are to be defined as the Web transaction. If you use the IE mode, make a note of the first URL to be accessed. If you use the direct entry mode, make a note of all the URLs to be accessed.

(2) Defining step information

You define as step information the information about each page to be accessed as a stage of the Web transaction. Web Recorder provides two modes, the IE mode and the direct entry mode; the method for defining step information depends on the mode.

- IE mode
Step information is recorded automatically when you use browser operations to navigate in the IE window that is displayed in the Web Recorder (main) window.
- Direct entry mode
You must enter manually each item of step information for each page that is to be accessed.

The following table lists the step information items, the items that are recorded automatically in the IE mode, and the items that you must set when you use the direct entry mode.

Table 4–4: List of step information items and required items

Item	IE mode	Direct entry mode
URL	Recorded automatically	Must be set by user
Title	Recorded automatically	--
Frame name	Recorded automatically	--
Character set	--	--
Character set of request information	--	--
Method	Recorded automatically	Must be set by user
Content type	Recorded automatically	##_#6
Message body	Recorded automatically	##_#6
Cookie	--	--
Web authentication	Web authentication	--
	Web authentication user name	##_#1
	Use of ESP password utility	--
	Web authentication password	##_#2
Proxy	Proxy setting	--
	Proxy host name	##_#3
	Proxy port number	##_#3
	Proxy authentication	--
	Proxy authentication user name	##_#4
	Use of ESP password utility	--
	Proxy authentication password	##_#5
Response determination	--	--
Variable string	--	--

Legend:

--: Not recorded automatically or setting by user is optional

#1

If Web authentication is to be performed, direct entry is required.

#2

If Web authentication is to be performed but the password utility is not used, direct entry is required.

#3

If **Use this setting value** is selected in the proxy settings, direct entry is required.

#4

Proxy authentication requires direct entry.

#5

If proxy authentication is to be performed but the password utility is not used, direct entry is required.

#6

If the POST method is to be used, this item is required.

#7

If Web authentication is to be performed, this item is required.

#8

If Web authentication is to be performed but the password utility is not used, this item is required.

#9

If **Use this setting value** is selected in the proxy settings, this item is required.

#10

If proxy authentication is to be performed, this item is required.

#11

If proxy authentication is to be performed but the password utility is not used, this item is required.

The following describes the definition method in each mode.

(a) IE mode

To record step information in the IE mode:

1. Specify a value for `web_rec_browser_mode` in the Web Recorder action condition definition file (`wr.conf`). For details about the value of `web_rec_browser_mode`, see `web_rec_browser_mode` in the [Table 8-23 Definition in the Web Recorder section](#).

2. From Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, then **Web Recorder**.

The Web Recorder (main) window appears.

3. From the **Transaction** menu, choose **New**.

The Web Recorder **Create New Web Transaction** window appears.

4. Specify in **Web transaction file name** the name of the Web transaction file at the storage destination. Then specify in **New Web transaction name** a name for the Web transaction to be defined and click the **OK** button.

Note:

Each Web transaction name in the same Web transaction file must be unique. A name cannot include the vertical bar (`|`).

5. In the **Web Recorder (main)** window, in **Address**, enter the URL of the first page to be accessed, and then click the **Go** button.

The page corresponding to the URL entered in the **IE window** is displayed.

6. In the **IE window**, perform browser operations to navigate to the desired page.

The step information for each accessed URL is recorded automatically, and each URL that is accessed is added to **URL list**.

7. If necessary, customize step information and set scopes.

For details about customizing step information, see [\(3\) Customizing step information](#); for details about setting scopes, see [\(4\) Setting a scope](#).

8. If necessary, set measurement conditions.

For details about setting measurement conditions, see [\(6\) Setting a transaction](#).

9. From the **Transaction** menu, choose **Save**.

The Web transaction file is saved in the following folder:

`installation-folder\agtv\probe\webtrans`

Notes:

You should note the following points when you use the IE mode:

- Your navigation operations in the **IE window** depend on the Internet Explorer settings on the machine where PFM - Agent for Service Response is installed. This means that if an application that affects Internet Explorer operations is running at the same time the Web transaction is being defined, the Web Recorder also picks up and records those effects.
- On the page displayed in the **IE window**, a script that controls the window itself (for instance, to resize it) may not function normally. A script that opens a new window to display a page cannot be executed. In this case, the window is displayed in the same format as the **IE window**, and normal window components such as menus in Internet Explorer are not displayed. Even when a new window is opened from the **IE window**, you can continue recording the step information using that window.

(b) In direct entry mode

To define step information in the direct entry mode:

1. Specify a value for `web_rec_browser_mode` in the Web Recorder action condition definition file (`wr.conf`). For details about the value of `web_rec_browser_mode`, see `web_rec_browser_mode` in the *Table 8-23 Definition in the Web Recorder section*.
2. From the Windows **Start** menu, choose, in the following order, **All Programs, Performance Management, Agent Option for Service Response**, and then **Web Recorder**.
The **Web Recorder (main)** window appears.
3. From the **Transaction** menu, choose **New**.
The Web Recorder **Create New Web Transaction** window appears.
4. Specify in **Web transaction file name** the name of the Web transaction file at the storage destination. Then specify in **New Web transaction name** a name for the Web transaction to be defined and click the **OK** button.

Note:

Each Web transaction name in the same Web transaction file must be unique. A name cannot include the vertical bar (|).

5. In the **Web Recorder (main)** window, from the **Edit** menu, choose **Add Last**.
The **Properties** window appears.
6. In **URL**, enter the URL of the next page to be accessed, and set each item as required.
In the **Properties** window, set the measurement conditions for the step. For details about the settings, see *7.2.7 Properties window*.
7. Click the **OK** button.
The URL of the set step information is added at the end of **URL list**.
8. Repeat Nos. 4 through 6 for each step to set information about all the pages that are to be accessed by the Web transaction.
9. If necessary, customize step information and set scopes.
For details about customizing step information, see *(3) Customizing step information*; for details about setting scopes, see *(4) Setting a scope*.
10. If necessary, set measurement conditions.
For details about setting measurement conditions, see *(6) Setting a transaction*.

11. From the **Transaction** menu, choose **Save**.

The Web transaction file is saved in the following folder:

installation-folder\agtv\probe\webtrans

(3) Customizing step information

This subsection describes how to customize step information recorded in the IE mode or defined in the direct entry mode (customizing means inserting, adding, changing, or deleting a step).

(a) Inserting a step

To insert a new step:

1. In the **Web Recorder (main)** window, from **URL list**, select the line where the information for the new step information is to be inserted, and from the **Edit** menu, choose **Insert**.

The **Properties** window appears.

2. In **URL**, enter the URL of the page to be accessed, and set each item as required.

In the **Properties** window, set the measurement conditions for the step. For details about the settings, see [7.2.7 Properties window](#).

3. Click the **OK** button.

The URL of the new step is inserted in the specified location in **URL list**.

(b) Adding a step

To add a step (at the end of the list of steps):

1. In the **Web Recorder (main)** window, from the **Edit** menu, choose **Add Last**.

The **Properties** window appears.

2. In **URL**, enter the URL of the page to be accessed, and set each item as required.

In the **Properties** window, set measurement conditions for the step. For details about the settings, see [7.2.7 Properties window](#).

3. Click the **OK** button.

The URL of the new step is added at the end of **URL list**.

(c) Changing a step's information

To change the settings for a step (changing a step's information):

1. In the **Web Recorder (main)** window, from **URL list**, select the URL of the step that you wish to edit, and from the **Edit** menu, choose **Property**.

The **Properties** window appears.

2. Change the settings.

For details about the settings in the **Properties** window, see [7.2.7 Properties window](#).

3. Click the **OK** button.

If you have changed the URL, the URL displayed in **URL list** is now changed.

(d) Deleting a step

To delete a step:

1. In the **Web Recorder (main)** window, from **URL list**, select the URL of the step that you wish to delete, and from the **Edit** menu, choose **Delete**.

The URL of the step selected in **URL list** is deleted.

(4) Setting a scope

To monitor any desired sequence of page transitions, you set the applicable range of page transitions as the start and end of a scope. This subsection describes how to set the start and end of a scope, and how to delete a scope.

(a) Setting the start of a scope

To set the start of a scope:

1. In the **Web Recorder (main)** window, from **URL list**, select the URL that is to be the start of the scope.
2. Click the **Start Scope** button.
The **Select Scope** window appears. In this window, **Scope list** displays the names of scopes (1 through 8) for which no start point has been set yet.
3. From the **Scope list**, select the name of the scope for which the selected URL is to be set as the start point.
4. Click the **OK** button.
START scope-name is displayed in front of the URL selected from **URL list**.

(b) Setting the end of a scope

To set the end of a scope:

1. In the **Web Recorder (main)** window, from **URL list**, select the URL that is to be the end of the scope.
2. Click the **End Scope** button.
The **Select Scope** window appears. In this window, **Scope list** displays the names of scopes (1 through 8) for which no end point has been set yet.
3. From the **Scope list**, select the name of the scope for which the selected URL is to be set as the end point.
4. Click the **OK** button.
END scope-name is displayed in front of the URL selected from **URL list**.

(c) Deleting a scope

To delete a scope:

1. In the **Web Recorder (main)** window, from **URL list**, select the start (*START scope-name*) or end (*END scope-name*) of the scope that you want to delete.
2. From the **Scope** menu, choose **Delete Scope**.
A dialog box appears asking you to confirm your intention to make a deletion in the scope whose start point or end point was selected.

3. To delete the entire scope whose start point or end point was selected, choose the **Yes** button. To delete only the selected start or end point, choose the **No** button.

Clicking the **Yes** button deletes both the start point and end point of the selected scope. Clicking the **No** button deletes only the selected point (start point or end point) of the selected scope.

(5) Displaying and editing an existing Web transaction definition

To display and edit an existing Web transaction definition:

1. From the Windows **Start** menu, choose, in the following order, **All Programs**, **Performance Management**, **Agent Option for Service Response**, and then **Web Recorder**.

The **Web Recorder (main)** window appears.

2. From the **Transaction** menu, choose **Open**.

The **Select Web Transaction** window appears.

3. From **List of Web transaction files** and **List of Web transactions**, select the Web transaction file name and Web transaction name that you want to display or edit, then click the **OK** button.

In the **Web Recorder (main)** window, each item of existing step information is displayed. To edit displayed step information, see the applicable procedure in (3) *Customizing step information*.

4. To save the edited Web transaction definition, from the **Transaction** menu, choose **Save**. To save it as a different Web transaction definition or as a separate file, from the **Transaction** menu, choose **Save As**.

When you choose **Save As**, specify **Web transaction file name** and **New Web transaction name**.

The Web transaction file is saved in the following folder:

installation-folder\agtv\probe\webtrans

Note:

Each Web transaction name in the same Web transaction file must be unique. A name cannot include the vertical bar (|).

(6) Setting a transaction

To set measurement conditions for the entire Web transaction:

1. In the **Web Recorder (main)** window, from the **Transaction** menu, choose **Set Transaction**.

The **Set Web Transaction Conditions** window appears.

2. Set the necessary items.

The **Set Web Transaction Conditions** window has the following four tabs:

- **Transaction** tab
- **Request Info** tab
- **Default Proxy** tab
- **SSL Authentication** tab

For details about the **Set Web Transaction Conditions window**, see *7.2.6 Set Web Transaction Conditions window*.

3. Click the **OK** button.

Supplement:

The settings on the **Default Proxy** page become the default proxy settings for each step's information as it is specified on the **Proxy** page of the **Properties** window. If the proxy settings are omitted in the definition of step information for a step, the values specified on the **Default Proxy** page of the **Set Web Transaction Conditions** window are used. If the proxy settings have been set for a step, those settings take effect.

4.4.2 Registering passwords

You must register the passwords to be used so that Web pages can be accessed when a Web transaction requires authentication and a password for a proxy.

Table 4–5: Internet services that require password registration

Service	Condition	Password to be registered
Web transaction	Web page requiring authentication	Password for the Web page
	Use of proxy that requires authentication	Password for the proxy

You use the password utility (`esppasswd` command) to register passwords. Each registered password is converted to character string format and then stored in the password file (`esp.pdb`).

Password file storage location:

`installation-folder\agtv\probe\passwd`

For details about how to use the password utility, see *esppasswd (registers, changes, and deletes passwords)* in *11. Commands*.

4.4.3 Defining measurement conditions

You use PFM - Web Console to define the Web transaction filename, measurement interval, and timeout value for measurement in the measurement condition registration file (`esptask.xml`) (or you can directly edit the measurement condition registration file to define these settings).

The following describes the measurement items for Web transactions and the items to be defined in the measurement condition registration file.

(1) Measurement items

The following table lists the measurement items for a Web transaction.

Table 4–6: List of measurement items for a Web transaction

Measurement target service	Measurement item
Web transaction (Entire Web transaction or each scope)	<ul style="list-style-type: none">• Total response time• Setup time• HTTP time• DNS time• TCP connection time• Server processing time• Data transfer time

Measurement target service	Measurement item
Web transaction (Entire Web transaction or each scope)	<ul style="list-style-type: none"> • Total amount of data • Number of requests • Total size of resources • Throughput

For details about the measurement items, see [10. Records](#).

(2) Creating the measurement condition registration file (esptask.xml)

To define measurement conditions for a Web transaction, you must create a measurement condition registration file (`esptask.xml`). For management purposes, a measurement condition ID is assigned to the measurement conditions. The following table describes the items to be defined in the measurement condition registration file as the measurement conditions for a Web transaction.

Table 4–7: Items that can be specified for measurement of a Web transaction

Item	Description
Measurement condition ID	Specifies an identifier for the measurement conditions. Each measurement condition ID must be unique.
Measurement interval	Specifies a measurement interval.
Timeout	Specifies a timeout value for each measurement.
Service-specific conditions	Specifies a Web transaction file name and a Web transaction name.

For details about the measurement condition registration file, see [8.3 Measurement condition registration file \(esptask.xml\)](#).

4.4.4 Registering certification files

To apply server authentication and client authentication during measurement of Web transactions, you must register a certification file in the same way as for measurement by using the HTTPS probe. For details, see [HTTPS \(PI_HTTPS\)](#) in [10. Records](#).

4.4.5 Applying the definition information

To apply the definition information, use either of the following methods:

- Reloading the definition information by using PFM - Web Console
For details about how to reload the definition information from PFM - Web Console, see [4.7.4 Applying the Task information](#).
- Restarting PFM - Agent for Service Response and reloading the definition information
If you perform one of the following operations, you need to restart PFM - Agent for Service Response and reload the definition information:
 - Add, change, or delete the definitions by editing the Probe action condition definition file (`esp.conf`).
 - Add, change, or delete the measurement conditions by directly editing the measurement condition registration file (`esptask.xml`).

- Change or delete the Web transaction definitions.
- Change or delete passwords.
- Change or delete the certification file.

Make sure that you stop PFM - Agent for Service Response before directly editing the measurement condition registration file (`esptask.xml`). If you directly edit the file while PFM - Agent for Service Response is running, and then perform operations from PFM - Web Console, the edited definition information might be lost.

For details about how to start and stop PFM - Agent for Service Response, see [5.1 Starting and stopping PFM - Agent for Service Response](#).

4.4.6 Defining settings for the dynamic session management

PFM - Agent for Service Response provides the settings of the variable strings and the substitute strings to support the dynamic session management. If you use the variable strings and substitute strings, PFM - Agent for Service Response replaces the variable string part of the HTTP request with the substitute string and issues the replaced HTTP request while measuring. Note the following when you specify the HTTP Cookie as the variable string.

- If you specify the HTTP Cookie as the variable string and the response to the request replaced with the substitute string is a redirect, the request issued after the redirect is not replaced with the substitute string.
- If you specify the HTTP Cookie as the variable string, do not include linefeed characters in the substitute string. If the substitute string contains linefeed characters, the behavior is not guaranteed.

The following explains how to specify the variable strings and the substitute strings.

(1) Setting variable strings

You specify as the variable strings the character string to change dynamically in the URL, message body, or HTTP Cookie in the step.

If you use the Web Recorder to create a new Web transaction file and record the operations in the site with the dynamic session management, the used session ID when recording is defined in the Web transaction file.

Specify either of the following in the variable string.

- Replace the recorded session ID with the explicit character string such as `$VAR1$`, and specify `$VAR1$` as the variable string (recommended).
- Specify the recorded session ID as the variable string.

(2) Setting substitute strings

A substitute string is a character string to replace the variable string in the HTTP request with when issuing the HTTP request. The substitute string can be acquired by either of the following procedures.

- Acquire from the HTML file obtained by the step before applicable step.
- Acquire from the HTTP header obtained by the step before applicable step.
- Use results of executing the specified command to generate the substitute string.
The command to generate the substitute string is hereafter called the substitution-string generation command.

The definition of the substitute string is different according to the source of the substitute string.

(a) Acquiring substitute strings from HTML files

The following information are required to define substitute strings:

1. The step ID of the step from which PFM - Agent for Service Response acquires the HTML file containing the substitute strings.
2. The location of the substitute string (the element names, the attributes, or the contents).
3. The information to specify which part of the element, attribute, or the content specified in the above information 2 contains the substitute string (attributes or contents).

Note:

The following notes are on acquiring the substitute strings from HTML files:

- The range of the element is between its start tag and the next occurrence of the start tag of the same element (`<element name>`) or between its start tag and its end tag (`</element name>`) unless the specified element is an empty element (`<element name.../>`).
- If PFM - Agent for Service Response cannot find the HTML file containing the substitute string (i.e. you specified the step ID where PFM - Agent for Service Response does not acquire the HTML file), PFM - Agent for Service Response sends the HTTP request as it is, not changing the variable string part of the HTTP request.
- If PFM - Agent for Service Response cannot find the element containing the substitute string, PFM - Agent for Service Response replaces the variable string with the null string and sends the HTTP request.
- PFM - Agent for Service Response does not acquire the substitute string from the compressed HTML file.

(b) Acquiring the substitute strings from HTML headers

The following information are required to define substitute strings:

1. The Step ID of the step to acquire the HTTP headers containing the substitute strings.
2. Information to identify the HTTP headers containing the substitute strings (header name or part of values).

Note:

The following notes are on acquiring the substitute strings from the HTTP headers:

- If there are multiple HTTP headers matching the specified information to identify the HTTP header containing the substitute string, PFM - Agent for Service Response acquire the substitute string from the HTTP header to be received earlier.
- If PFM - Agent for Service Response does not find the HTTP header containing the substitute string, PFM - Agent for Service Response replaces the variable string with the null string and sends the HTTP request.

(c) Acquiring the substitute strings from commands

The following information are required to define substitute strings:

1. The name of the substitution-string generation command
2. The arguments given to the command

Important

The following notes are on acquiring the substitute strings from commands:

- In put to the commands

You can specify arguments as an interface to give the values to the command. If the arguments are fixed, you can specify the command name to include the argument when you specify the above information 1. If the arguments change dynamically, you can acquire the arguments of the command from the content of the HTML or the HTTP header obtained before this step.

The arguments specified as the above information 2 must be surrounded by the double quotes (") and when PFM - Agent for Service Response execute it PFM - Agent for Service Response inserts the arguments after the command in the specified order.

Note that the PFM - Agent for Service Response does not provide to the commands an interface to the standard input.

- Output from the commands

The commands must output the character strings as the substitute strings in the standard output. The output character string must not be longer than 10,000 bytes, because in that case PFM - Agent for Service Response may not successfully terminate the command. The output character string that is removed linefeed characters (1 or greater) in the end is the substitute string.

- Return codes of the commands

If the return codes of the commands (exit status) are other than 0, the commands are judged to be a failure. In this case, PFM - Agent for Service Response replaces the variable string with null characters and issues the HTTP request. If the commands output the substitute strings to the standard output correctly, the return codes must be 0.

- The commands are executed whenever the substitute strings are required.
- The commands are executed by the account of the Extensible Service Probe service.
- If an error occurs when executing the commands, PFM - Agent for Service Response replaces the variable string with null characters and issues the HTTP request.

4.5 Definitions for measuring IE scenarios

To measure IE scenarios, you must perform the following:

- Define IE scenarios
- Define measurement conditions
- Apply the definition information

4.5.1 Performing pre-measurement check on target Web pages

PFM - Agent for Service Response does not support measurements of Web pages with script errors. You may be able to check to see if target Web pages contain script errors by changing the settings of Internet Explorer.

The following shows the procedure to use Internet Explorer on the PFM - Agent for Service Response host to perform pre-measurement check on target Web pages:

1. In Internet Explorer, temporarily change the **Internet Options** settings as follows:

Advanced tab

- Select **Display a notification about every script error**.
- Clear **Disable script debugging (Internet Explorer)**.

Note:

You may see different setting options depending on the version of your Internet Explorer.

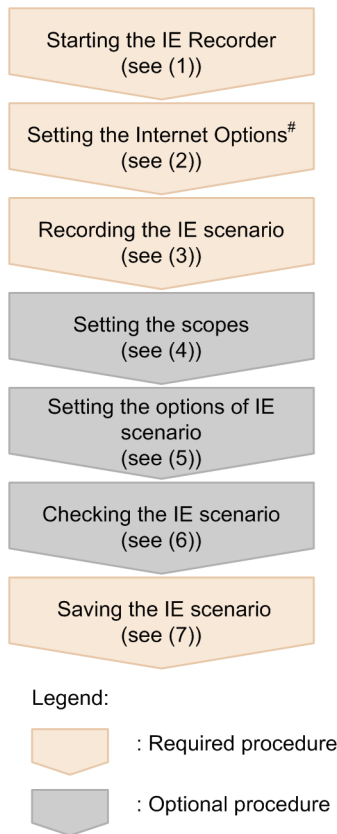
2. Use Internet Explorer to access the target Web page and check that no script error occurs.
If a script error occurs, the software cannot measure the target Web page.
3. Change the settings on the **Advanced** tab of **Internet Options** back to the state they were in step 1, and then click the **OK** button.

4.5.2 Defining IE scenarios (creating IE scenario files)

In PFM - Agent for Service Response, you can define an IE scenario and save the definitions as an IE scenario file by using the IE Recorder. For details about IE Recorder, see [7.3 IE Recorder windows](#).

The following shows the procedure for defining an IE scenario. For details about each procedure, see the indicated sections.

Figure 4–3: Definition procedures for measuring IE scenarios



Procedure that is required when you create a new IE Scenario

The following shows how to use the IE Recorder to create an IE scenario file.

Reference note:

In the IE Recorder, you can use the icons on toolbar, as well as the command buttons on menu bar. For details about the icons on the toolbar in the IE Recorder (main) window, see [7.3.1 IE Recorder \(main\) window](#).

(1) Starting the IE Recorder

The following shows the procedure for starting the IE Recorder.

1. Logging on by the account for the measurement to the host where you create IE scenario files.
2. Specify a value for `ie_rec_browser_mode` in the IE Recorder action condition definition file (`jpcvierec.conf`).
For details about the value of `ie_rec_browser_mode`, see `ie_rec_browser_mode` in the [Table 8-31 Definition in the IE Recorder section](#).
3. From Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, then **IE Recorder**.
The IE Recorder (main) window appears.

(2) Setting the Internet Options

If you create new IE scenarios, you set the Internet Options to record an IE scenario and define the environment for measurement.

The following shows the procedure for setting the Internet Options.

1. In the IE Recorder (main) window, from the **Tools**, choose the **Internet Options**.
The **Internet Options** window appears.
2. In the **Internet Options** window, define the environment for recording and measuring IE scenarios.
3. Click the **OK** button.

(3) Recording the IE scenario

In the IE window section of the IE Recorder (main) window, you record the browser operations performed as an IE scenario.

The following shows the procedure for recording the IE scenarios.

1. In the IE Recorder (main) window, from the **File**, choose the **New**. A new IE scenario file is created.
2. From the **Action**, choose the **Record**.
It is started to record the IE scenario.
3. Enter the **URL** of the monitoring target Web page in the **Address bar**, and press the **Enter** key.
The Web page is displayed in the IE window section.
4. In the IE window section, conduct operations in the displayed Web page.
The browser operations performed are recorded as an IE scenario. The recorded information is displayed in the **Operation list**. You can record not only a single operation but also a series of tasks consisting of multiple operations as an IE scenario.
5. From the **Action**, choose the **Stop**.
It is stopped to record the IE scenario.

(4) Setting the scopes

You can define a series of operations in an IE scenario as a scope and measure the performance information within that scope. In this case, set the start and end scopes in IE scenarios.

The following shows the procedure for setting and deleting start scopes and end scopes.

(a) Setting start scopes

The following shows the procedure for setting start scopes:

1. In the Operation list in the IE Recorder (main) window, choose the operation that you want to set as a start scope.
2. From the **Scope**, choose the **Set Start Scope**.
The **Start Scope Settings** window appears.
3. Select the scope ID that you want to set as a start scope in the **Start Scope Settings** window.
4. Click the **OK** button.
The start scope operation in the **Operation list** is displayed in the following way: `START [scope-name]`.

(b) Setting end scopes

The following shows the procedure for setting end of a scope.

1. In the Operation list in the IE Recorder (main) window, choose the operation that you want to set as an end scope.
2. From the **Scope**, choose the **Set End Scope**.
The **End Scope Settings** window appears.
3. Select the scope ID that you want to set as an end scope in the **End Scope Settings** window.
4. Click the **OK** button.
The end scope operation in the **Operation list** is displayed in the following way: END [scope-name].

(c) Deleting the Scopes

The following shows the procedure for deleting the start and end scopes.

1. In the Operation list in the IE Recorder (main) window, select the start scope (SCOPE scope ID (scope name)) or the end scope (SCOPE scope ID (scope name)) that you want to delete.
2. From the **Scope**, choose the **Delete Scope**.
The setting of the start and end scopes is deleted.

(5) Setting the IE scenario options

To customize the options of the recorded IE scenario, you can replay and measure IE scenarios to suit your needs.

(a) Identifying the Tags

After you record the IE scenario, the positions and attributes of the operation target tags in the HTML file may be changed due to the layout change of the target site. In that case, PFM - Agent for Service Response provides the way for you to customize how to identify the operation target tags, without changing the IE scenarios.

The following shows the procedure for specifying how to identify the operation target tags.

1. In the IE Recorder (main) window, from the **Edit**, choose the **Operation Settings**.
The **Operation Settings** window appears.
2. In the Operation Target page in the **Operation Settings** window, customize how to identify the tags for recording Web pages, click the **OK** button.

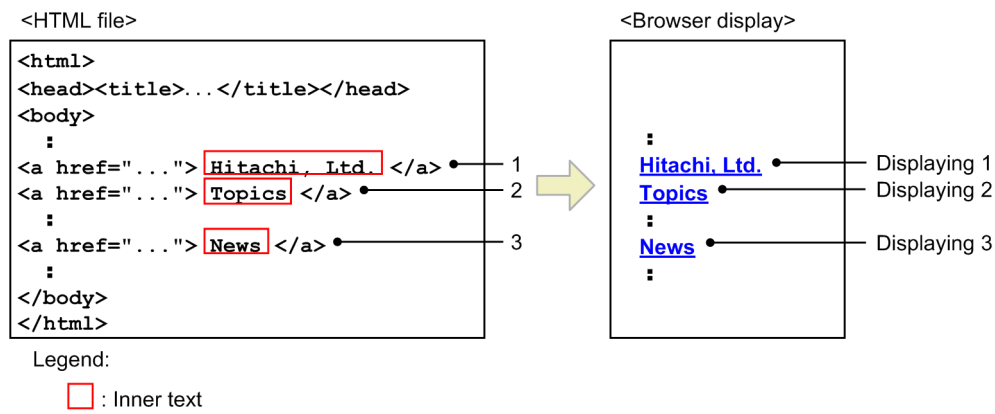
The following shows how to identify the operation target tags:

Inner text:

Identifies the operation target tags targets by the inner text that is surrounded by the start and end tags. If you select the *Inner text*, the tag that has the specified inner text is selected and operated when replaying the IE scenario.

The following example shows the inner texts in the HTML file and how it is displayed:

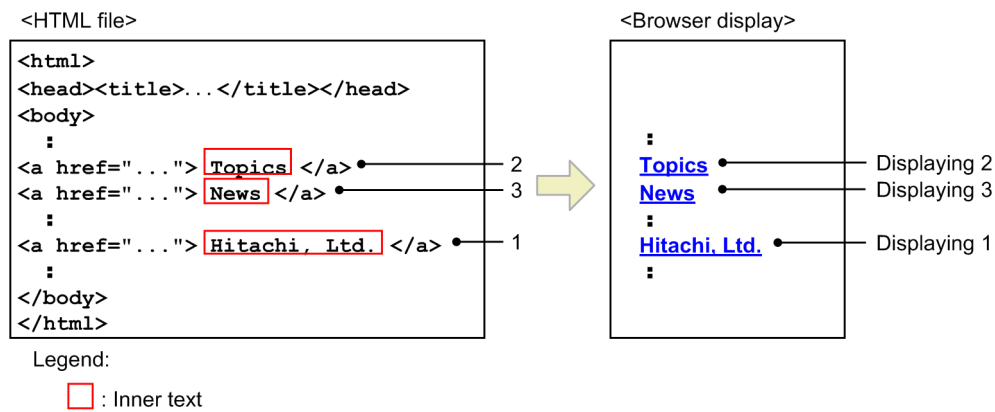
Figure 4–4: Example of the Inner texts in the HTML File and How it is Displayed



In the HTML file of the Figure 4-4, if you specify the inner text `Hitachi, Ltd.` of the `a` tag as the filter condition, the tag with the inner text `Hitachi, Ltd.` is selected and operated when replaying the IE scenario.

The following example shows the inner texts in the HTML file and how it is displayed, after you modify the HTML file:

Figure 4–5: Example of the Inner texts in the HTML file and How it is Displayed (the HTML File Modified)



In this case, even when you change the position of the tag with the inner text `Hitachi, Ltd.` as in the Figure 4-5, PFM - Agent for Service Response search the tag with the specified inner text `Hitachi, Ltd.` and replays the operation without re-recording the IE scenario, if you select *Inner text*.

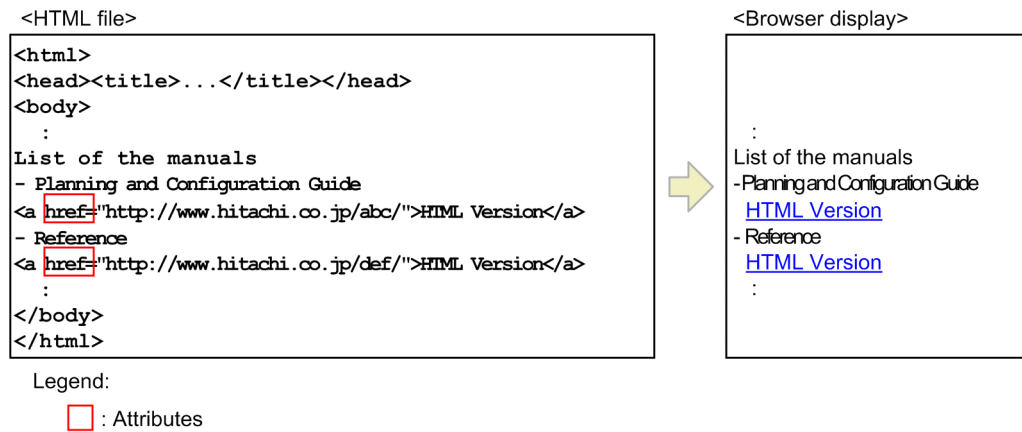
Attributes:

Identifies the operation target tags by the attribute value of the tag.

If you specify the attribute, the tag with the specified attribute value is selected and operated when replaying the IE scenario. If there are multiple tags with the specified attribute value, the tag that appears first in the HTML file is selected and operated.

The following example shows the attributes in the HTML file and how it is displayed.

Figure 4–6: Example of the Attributes in the HTML File and How it is Displayed



In the Figure 4-6, if you specify the inner text `HTML version` of the `a` tag as the filter condition, PFM - Agent for Service Response cannot replay the IE scenario correctly, because there are multiple `a` tags with the inner text `HTML version`. If you specify the attribute `href` of the `a` tag as the filter condition, the tag with the attribute `href` and appears first in the recorded IE scenario is selected and operated when replaying the IE scenario.

Tag position:

Identifies the operating target tags by the position of tag with the same inner text or attribute value in the HTML file.

If you specify the tag position, the tag in the specified position is selected and operated when replaying the IE scenario.

If there are multiple tags with the same inner texts or attribute values in the HTML file, the recorded IE scenario may be replayed incorrectly. In that case, if you specify the tag position, the IE scenarios will be replayed correctly.

When there are multiple tags with the same inner texts and attribute values in the HTML file, you combine inner texts, attributes, and tag positions to identify the operation target tag. When you combine these conditions, the tag that matches all the conditions is selected and operated when replaying the IE scenario.

When you specify the tag position, you specify *n*th match among the tags that meet the specified conditions searched from the top in the HTML file.

For details about setting items, see [7.3.2\(2\) Operation Target page](#).

(b) Response Determination

When you replay or measure IE scenarios, you can check whether HTTP responses are correct. For each operation, you specify the response determination condition for the HTTP responses. The all response pages for each operation are checked. You specify the character strings in the HTML file as the response determination conditions.

If the HTML file that meets the specified conditions is displayed, PFM - Agent for Service Response judges the response to be correct and continues on replaying or measuring. If the HTML file that does not meet the specified conditions is displayed, PFM - Agent for Service Response stops replaying or measuring.

The following shows the procedure for setting the response determination conditions.

1. In the Operation list in the IE Recorder (main) window, choose the operation that you set as a start scope.
2. From the **Edit**, choose the **Operation Settings**.
 The **Operation Settings** window appears.

3. In the Response Determination page in the Operation Settings window, customize the response conditions for recording the Web page, click the **OK** button.

For details about setting items, see [7.3.2\(3\) Response Determination page](#).

(6) Checking the IE scenario

To replay the recorded IE scenario, you can check whether the scenario is measured correctly. PFM - Agent for Service Response provides the following functions to check IE scenarios:

- Replaying IE scenarios
- Replaying by step IE scenarios
- Setting breakpoints
- Testing measurements

The following explains each function:

(a) Replaying IE scenarios

You can replay IE scenarios to the breakpoint or the end of the recorded operations.

In the IE Recorder (main) window, from the **Action**, choose the **Replay**, and then start replaying the IE scenario.

In the IE Recorder (main) window, from the **Action**, choose the **Stop**, and then stop replaying the IE scenario.

If the recorded IE scenario is not replayed correctly, take the actions listed below:

- In the IE Recorder (main) window, from the **Edit**, choose the **Operation Settings**, in the Operation Target page of the Operation Settings window, change the settings.
- Check whether the operations that cannot be recorded in the IE scenario, and if they exist record the IE scenario again to exclude these operations.

For details about the operations that cannot be recorded, see [5.2.3\(3\) Notes on recording and replaying the IE scenarios](#).

(b) Replaying by step IE scenarios

You can replay the IE scenario step by step to test IE scenario measurement.

In the IE Recorder (main) window, from the **Action**, choose the **Replay by Step**, and then IE scenario is replayed step by step.

(c) Setting breakpoints

When replaying the IE scenario, you can suspend the replay at the point set as a breakpoint to check the operations or set scopes.

The following shows the procedure for setting the breakpoints.

1. In the Operation list in the IE Recorder (main) window, choose the operation that you suspend.
2. From the **Action**, choose the **Set Breakpoint**.

The following shows the procedure for canceling the breakpoints.

1. In the Operation list in the IE Recorder (main) window, choose the operation that you set as a breakpoint.

2. From the **Action**, choose the **Delete Breakpoint**.

(d) Testing measurements

The IE scenario is replayed to the end of the recorded operations. After its replaying terminates, the result of replaying IE scenario in the Replay Report window is displayed. For details about the Replay Report window, see [7.3.8 Replay Report window](#).

In the IE Recorder (main) window, from the **Action**, choose the **Test Measurement**, and the IE scenario measurement test starts.

If the recorded IE scenario is not replayed correctly, you take appropriate actions based on the displayed information of the **Replay results** in the Replay Report window.

(7) Saving the IE scenario

The following shows the procedure for saving the recorded or edited IE scenario.

1. In the IE Recorder (main) window, from the **File**, choose the **Save As**.

The **Save As** window appears.

2. Specify a file name to the **File name**, and click the **Save** button.

The information of the IE scenario is saved into the IE scenario file.

Note:

If you save the IE scenario file in the folder other than `jplpc\agtv\probe\iescena`, you must copy `iescena.dtd` to the destination folder.

4.5.3 Defining measurement conditions

If you measure the IE scenarios, you must register to PFM - Agent for Service Response the measurement conditions, such as the IE scenario filenames, measurement interval, timeout values. When you use PFM - Agent for Service Response to experience performance monitoring (such as the time when you use PFM - Agent Service Response for the first time), use the simplified registration of the IE Recorder to register the measurement conditions. Note that when you use the simplified registration of the IE Recorder you must stop PFM - Agent for Service Response in advance.

If you want to customize the parameters such as the measurement intervals and timeout values or you do not want to stop PFM - Agent for Service Response, use PFM - Web Console to register the measurement conditions to the measurement condition registration file (`esptask.xml`).

This subsection describes the measurement items of the IE scenarios and the simplified registration of the measurement conditions.

(1) Measurement items

The following table lists the shows the measurement items of the IE scenario:

Table 4–8: Measurement items of IE scenario

Measurement target service	Measurement items
IE scenario (Entire IE scenario/Each scope)	Total replay time

For details about the measurement items, see [10. Records](#).

(2) Simplified registration into the measurement condition registration file (`esptask.xml`)

You can simply register measurement conditions of the opened IE scenario file into the measurement condition registration file (`esptask.xml`).

Note:

Before simply registering measurement conditions, you must stop PFM - Agent for Service Response.

The following shows the procedure for simplified registration of the IE scenario measurement conditions into the measurement condition registration file.

1. In the IE Recorder (main) window, from the **Tools**, choose the **Simplified Registration**.

The measurement conditions of the IE scenario are registered into the measurement condition registration file.

2. From the **Tools**, choose the **Edit esptask.xml**.

You can check and edit the information that is registered in the measurement condition registration file. If you edit the measurement condition registration file in the **IE Recorder (main)** window, you must stop *PFM - Agent for Service Response*. Thus, Hitachi recommends that you edit the registration file in PFM - Web Console, instead of the IE Recorder.

For details about editing the measurement condition registration file in PFM - Web Console, see [4.7.3 Setting the Task information](#).

For details about the measurement condition registration file, see [8.3 Measurement condition registration file \(`esptask.xml`\)](#).

4.5.4 Applying the definition information

To apply the definition information, use either of the following methods:

- Reloading the definition information by using PFM - Web Console

For details about how to reload the definition information from PFM - Web Console, see [4.7.4 Applying the Task information](#).

- Restarting PFM - Agent for Service Response and reloading the definition information

If you perform one of the following operations, you need to restart PFM - Agent for Service Response and reload the definition information:

- Add, change, or delete the definitions by editing the Probe action condition definition file (`esp.conf`).
- Add, change, or delete the measurement conditions by directly editing the measurement condition registration file (`esptask.xml`).
- Change or delete the IE scenario definitions.

Make sure that you stop PFM - Agent for Service Response before directly editing the measurement condition registration file (`esptask.xml`). If you directly edit the file while PFM - Agent for Service Response is running, and then perform operations from PFM - Web Console, the edited definition information might be lost.

For details about how to start and stop PFM - Agent for Service Response, see [5.1 Starting and stopping PFM - Agent for Service Response](#).

4.6 Definitions for measuring user-defined services

To measure user-defined services, you perform the following:

- Define the user-defined services
(create user-defined commands and then register them)
- Define measurement conditions

This section describes the definition of user-defined services and the registration of measurement conditions.

4.6.1 Defining a user-defined service

You must create a program for measuring the target service's performance, such as its response times, and then register the program as a user-defined command.

(1) Creating a user-defined command

A user-defined command is created as a program that executes from the command line. Each user-defined command measures only one item. To measure multiple items, you must create a user-defined command for each item. Note that you must execute the user-defined commands with Administrator permissions because they are called from PFM - Agent for Service Response.

(a) Input

PFM - Agent for Service Response does not provide an interface for passing input values. For a service-specific measurement condition, you must provide the information that is necessary for measurement by an appropriate method, such as by specifying arguments in the user-defined command or reading files.

(b) Output

If a measurement result is to be the standard output of a user-defined command, the user-defined command must output the value shown below to the standard output. PFM - Agent for Service Response treats a value in the standard output as the response performance information. If the measurement result is to be the time required for the execution of the user-defined command (from start to termination), do not output anything to the user-defined command's standard output.

Table 4–9: Output of a user-defined command

Value	Description
Response performance information	Outputs the value of a given measurement item (double-precision real number), such as total response time or throughput, expressed as a character string.

Supplement:

The measurement information obtained by a user-defined command is output to a report file. When a user-defined command's execution time is output, the value is in seconds with a precision of up to milliseconds. If the value output by a user-defined command is outside the permitted range or is in an invalid format, the system treats it as an error and stops the measurement.

(c) Return value

A user-defined command's return value indicates the measurement result. You must create your user-defined commands in such a manner that they return one of the values listed in the table below.

Table 4–10: Return values of user-defined commands

Return value	Description
0	Normal termination The measurement terminated normally and the response performance information was acquired.
Other than 0	Abnormal termination The measurement failed and any value obtained as the response performance information is invalid.

You should store your created user-defined commands in the following user-defined command storage folder provided by PFM - Agent for Service Response:

`installation-folder\agtv\probe\user`

To call a command that has been stored in a folder other than the user-defined command storage folder, you must create a batch file for calling the command, and then store the batch file in the user-defined command storage folder.

Note:

A user-defined command is executed after the timeout value specified in the measurement condition is reached. This prevents startup of measurement (issuance of a measurement request) for other Internet services from being delayed if the current user-defined command's internal processing takes a long time. Therefore, create your user-defined command in such a way that its processing will be completed within the timeout value specified as a measurement condition.

(2) Registering user-defined commands

Register your created user-defined commands in the command registration file (`espcommand.xml`). In the command registration file, you can define a user-selected service ID which will be used to identify the target service and service-specific measurement conditions. For details about the command registration file, see [8.6 Command registration file \(`espcommand.xml`\)](#).

4.6.2 Defining measurement conditions

As for the measurement conditions other than the ones you defined in the command registration file (`espcommand.xml`), you use PFM - Web Console to define them in the measurement condition registration file (`esptask.xml`) (or you can edit the file directly and define the conditions).

The following table describes the items that can be defined as measurement conditions for a user-defined service in the measurement condition registration file.

Table 4–11: Items that can be specified as measurement conditions

Item	Description
Measurement condition ID	Specifies an identifier for the measurement conditions. Each measurement condition ID must be unique.
Measurement interval	Specifies a measurement interval.
Timeout	Specifies a timeout value for each measurement.
Service-specific conditions	Specifies the user-defined service ID.

For details about the measurement condition registration file, see [8.3 Measurement condition registration file \(`esptask.xml`\)](#).

4.6.3 Applying the definition information

To apply the definition information, use either of the following methods:

- Reloading the definition information by using PFM - Web Console

For details about how to reload the definition information from PFM - Web Console, see [4.7.4 Applying the Task information](#).

- Restarting PFM - Agent for Service Response and reloading the definition information

If you perform one of the following operations, you need to restart PFM - Agent for Service Response and reload the definition information:

- Add, change, or delete the definitions by editing the Probe action condition definition file (`esp.conf`).
- Add, change, or delete the measurement conditions by directly editing the measurement condition registration file (`esptask.xml`).
- Change or delete the definitions of a user-defined service.

Make sure that you stop PFM - Agent for Service Response before directly editing the measurement condition registration file (`esptask.xml`). If you directly edit the file while PFM - Agent for Service Response is running, and then perform operations from PFM - Web Console, the edited definition information might be lost.

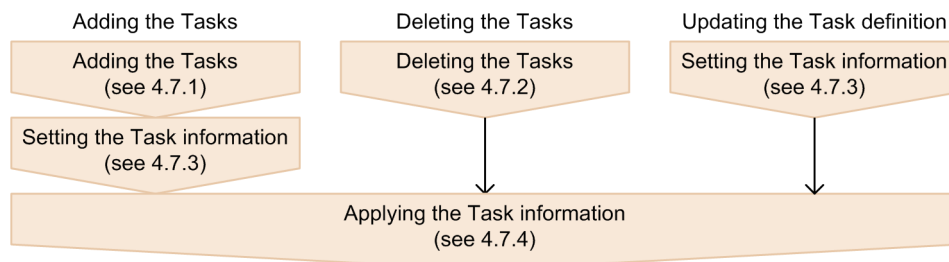
For details about how to start and stop PFM - Agent for Service Response, see [5.1 Starting and stopping PFM - Agent for Service Response](#).

4.7 Defining measurement conditions in PFM - Web Console

PFM - Agent for Service Response defines the Probe Daemon's task definitions and the IE Probe Daemon's task definitions in the measurement condition registration file (`esptask.xml`) in XML format. You can use PFM - Web Console to define these definitions in the measurement condition registration file.

This subsection describes how to use PFM - Web Console to add, delete, and edit the Probe Daemon's task definitions and the IE Probe Daemon's task definitions.

The following shows the procedure for adding, deleting, and editing the Probe Daemon's task definitions and the IE Probe Daemon's task definitions. For details about each procedure, see the indicated section.



You can distribute the defined tasks to the multiple Agent servers. For details about distributing, see [4.7.5 Distributing the Task information](#).

The task definition is loaded from the measurement condition registration file when the Probe Daemon and the IE Probe Daemon starts. If the definition is invalid, the Probe Daemon and the IE Probe Daemon stops and the measurements does not start. This case happens, for example, when PFM - Agent for Service Response does not find the Web transaction file defined in the task definition of the Web transaction. When you use PFM - Web Console to define the Web transaction task, PFM - Web Console checks whether the entered values are valid or not, but does not check whether the defined task is actually measurable. If the Probe Daemon and the IE Probe Daemon fails to start and stopped, check whether the measurement conditions are valid.

Note:

If you define the measurement condition registration file (`esptask.xml`) by editing the file directly and by using PFM - Web Console, note on the following. For details about editing the measurement condition registration file directly, see [8.3 Measurement condition registration file \(esptask.xml\)](#).

- If the measurement condition registration file has the XML syntax errors or the invalid task ID is given to the task definitions in the file, you cannot use PFM - Web Console to define the measurement conditions. Stop Agent Collector and the IE probe[#], edit the measurement condition registration file (`esptask.xml`), and start Agent Collector and the IE probe[#].

[#]

If you use the Windows services to start the IE probe service, it is not necessary to start the IE probe.

- The maximum number of the tasks displayed in PFM - Web Console is 500. If 501 or more tasks are defined in the measurement condition registration file, the first 500 tasks are displayed and the others are not displayed in PFM - Web Console, and the message `KAVF16023-W` is output in the common message log.

If 501 or more tasks are defined and you delete a task in PFM - Web Console, 501th task is displayed in PFM - Web Console.

- If the number of the tasks is more than 500 after adding the tasks, you cannot add a task in PFM - Web Console. If more than 500 tasks are displayed and you add a task in PFM - Web Console, the message `KAVF16023-W` is output in the common message log and you cannot add a task. In this case, the task is not registered in the measurement condition registration file, and is not created.

- If you define a task in PFM - Web Console, the formatted comments and indents of the task is output to the measurement condition registration file.

Reference note:

PFM - Web Console sorts the tasks by the service type ID in ascending order and displays them. If the tasks have same service type ID, PFM - Web Console sorts the tasks by the measurement condition ID in ascending order. For details about the service type ID, see *Common fields of 10. Records*.

4.7.1 Adding the Tasks

The following shows the procedure for adding the Probe Daemon's task definitions and the IE Probe Daemon's task definitions by using PFM - Web Console.

1. From the monitoring console browser, log on to PFM - Web Console.
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, expand the contents of the monitoring agent host folder, and select the Agent Collector service.
The **Properties** page appears.
4. Expand the hierarchy under the **Probe** folder, and select the **ADD OR DELETE A TASK**.
5. Set properties appear at the bottom of the information frame.
Specify the values of the properties listed in the following table to a new task. None is set by default.

Property name	Specifiable value
New Task ID	Specifies the task ID of a newly created task within the range from 1 to 65,535. The Task IDs must be unique. If you create a new task, you must specify this item.
New Task Protocol	Specifies the protocol of a newly created task from the drop-down list. Select HTTP, HTTPS, SMTP, POP3, IMAP4, DNS, DHCP, FTP, TCP, WEBTRANS, IESCENA, or USERSERV services. If you create a new task, you must specify this item.

Reference note:

Use the `Delete A Task` property when you delete a task (you can add a task and delete an existing task at the same time). Since the `Reserved` property is reserved for the system, you cannot use it.

6. In the bottom of the information frame, click the **OK** button.
When succeeding in adding the task, the folder `protocol name_task ID` is created appears under **Task List** tree. Immediately after a new task is added, the properties of the task are not defined. Specify the properties to the task. For details about how to specify the properties, see *4.7.3 Setting the Task information*.
You must apply information of the added task to the Probe Daemon and the IE Probe Daemon. For details about how to apply information, see *4.7.4 Applying the Task information*.

4.7.2 Deleting the Tasks

The following shows the procedure for deleting the Probe Daemon's task definitions and the IE Probe Daemon's task definitions by using PFM - Web Console.

1. From the monitoring console browser, log on to PFM - Web Console.
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, expand the contents of the monitoring agent host folder, and select the Agent Collector service.
The **Properties** page appears.
4. Expand the hierarchy under the **Probe** folder, and select the **ADD OR DELETE A TASK**.
5. Set properties appear at the bottom of the information frame.
Specify the values of the properties listed in the following table. None is set by default.

Property name	Specifiable value
Delete A Task	Specifies the task from the drop-down list. When you delete a task, you must specify the task.

Reference note:

Use the `New Task ID` and the `New Task Protocol` property to add a new task (you can delete an existing task and add a task at the same time). Since the `Reserved` property is reserved for the system, you cannot use it.

6. In the bottom of the information frame, click the **OK** button.
When succeeding in deleting the task, the task status becomes "Deleted". The deleted task remains in the **Task List** tree until its deletion is applied to the Probe Daemon and the IE Probe Daemon. The deleted task folder in the **Task List** tree disappears when its deletion is applied. You cannot add the task specifying the same task ID of the deleted task until its deletion is applied to the Probe Daemon and the IE Probe Daemon. For details about how to apply information to the Probe Daemon and the IE Probe Daemon, see [4.7.4 Applying the Task information](#).

4.7.3 Setting the Task information

You can use PFM - Web Console to change or check task definitions of the Probe Daemon and the IE Probe Daemon. When you change definitions, note the following:

- Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.
- When you specify property values, you do not need to take XML format into consideration.
When you use the characters `&`, `<`, `>`, `"`, and `'` in the XML syntax, you need to convert each character into the format `&entity name;`. If you enter property values in PFM - Web Console, you do not need to convert these characters. For example, when you want to specify `A&B` as the label name, enter `A&B` as it is as the **Task Label** property.
- When you apply the changes in the properties to the terminal nodes of the XML document structure in the measurement condition registration file, comments in the tags will be deleted.

The following shows the procedure for changing the definitions:

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

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, expand the contents of the monitoring agent host folder, and select the Agent Collector service.

The **Properties** page appears.

4. Expand the hierarchy under the **Probe** folder, and select the task tree that you want to change and check the task information under **Task List**.

Each task is displayed as the folder. The node name is *protocol-name_task-ID*. For example, if the task ID of the Web transaction is 100 and the label name is WEBTRANS, then the node name is WEBTRANS_100 (the label name is not used as node name).

The displayed tasks are sorted by the service type in the ascending order in the **Task List**, and the tasks of the same protocol are sorted by the task ID in ascending order. If you select the task from the **Task List**, the properties of the selected task are displayed. You can edit the values of the properties in this window. Yet, you cannot edit the read-only properties.

For details about the properties, see [E.2 Agent Collector service properties](#).

5. After editing the task properties, click the **OK** button.

The specified data is checked:

When the result is valid:

The **Status** property of the task becomes `Valid`. The settings are applied to the measurement condition registration file.

If the element displayed in PFM - Web Console contains the linefeed characters (other than `<MESSAGE_BODY >` tag of the HTTP, HTTPS service), the linefeed characters are deleted.

When the result is invalid:

The **Status** property of the task becomes `Invalid`. The message is output to the common message log.

If the byte number of the specified string property exceeds the maximum bytes, the first maximum bytes of the specified character strings are displayed (if you use the characters of the double-byte character set and the data in the maximum byte location of the specified character string is the first byte of a character, that character is not displayed). If you enter other than numeric data in the integer properties, 0 is displayed.

You must apply information of the changed task to the Probe Daemon and the IE Probe Daemon. For details about how to apply information, see [4.7.4 Applying the Task information](#).

4.7.4 Applying the Task information

The following shows the procedure for applying the task definitions to the Probe Daemon and the IE Probe Daemon by using PFM - Web Console.

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

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.

- In the navigation frame of the **Services** window, expand the contents of the monitoring agent host folder, and select the Agent Collector service.
The **Properties** page appears.
- Select **Probe** folder under **Services** tree.
- Select **Yes** in the **Reload** property and click the **OK** button.

The Probe Daemon and the IE Probe Daemon are restarted, and the changed measurement conditions are applied.

Note:

If you did not click the **OK** button after changing the properties of the measurement conditions (the procedure 5 in [4.7.3 Setting the Task information](#)), the changed measurement conditions are not applied to the Probe Daemon and the IE Probe Daemon.

- Check the status of the Probe Daemon and the IE Probe Daemon.

You can check the status of the Probe Daemon and the IE Probe Daemon by using PFM - Web Console.

Status of the Probe Daemon:

You can check the status of the Probe Daemon in the **Probe Status** property. If it displays **Unknown**, reload the properties.

Value of the Probe Status	Status of the service
Active	The Probe Daemon is running, or stopping.
Inactive	The Probe Daemon is stopped, or starting.
Unknown	Failure to acquire the status of the Probe Daemon.
Reloading	The Probe Daemon is reloading the settings.

Status of the IE Probe Daemon:

You can check the status of the IE Probe Daemon in the **IE Probe Status** property. If it displays **Unknown**, reload the properties.

Value of IE Probe Status	Status of the service
Active	The IE Probe Daemon is running, or stopping.
Inactive	The IE Probe Daemon is stopped, or starting.
Unknown	Failure to acquire the status of the IE Probe Daemon.
Reloading	The IE Probe Daemon is reloading the settings.

- Check the value of **Status** for each task is **Applied**.

The **Status** property represents the status of editing tasks and applying them. The following table lists the status name, their descriptions, and how to handle them.

Table 4–12: Value and description of the property and how to handle

Status name	Description	How to handle
Applied	The changed settings are applied to the Probe Daemon and the IE Probe Daemon.	Unnecessary.
Deleted	The deletion of the settings is not yet applied to the Probe Daemon and the IE Probe Daemon. If you change the properties of the tasks of this status, the changes are	1. Select Yes in Reload property and click the OK button. The task disappears from the Task List , and then you can add a task of the same task ID as the deleted one.

Status name	Description	How to handle
Deleted	invalid and not applied. You cannot add the task of the same ID until the status becomes <code>Applied</code> .	<ol style="list-style-type: none"> 1. Select <code>Yes</code> in Reload property and click the OK button. The task disappears from the Task List, and then you can add a task of the same task ID as the deleted one.
Initial	A new task is created, but you do not specify the values and not click the OK button yet.	<ol style="list-style-type: none"> 1. Enter the valid values to all the required properties, and click the OK button. The Status becomes <code>Valid</code>. 2. Select <code>Yes</code> in Reload and click the OK button. After the settings are applied to the Probe Daemon and the IE Probe Daemon, the Status becomes <code>Applied</code>.
Invalid #	One or more specified values of the properties are invalid.	<ol style="list-style-type: none"> 1. Enter the valid value to the properties with the invalid values, make sure that you specify the valid values to all the required properties, and click the OK button. The Status becomes <code>Valid</code>. 2. Select <code>Yes</code> in the Reload property and click the OK button. If the settings are applied to the Probe Daemon and the IE Probe Daemon, the Status becomes <code>Applied</code>.
Valid	All required properties are specified correctly, but the settings are not yet applied to the Probe Daemon and the IE Probe Daemon.	<ol style="list-style-type: none"> 1. Select <code>Yes</code> in Reload and click the OK button. After the settings are applied to the Probe Daemon and the IE Probe Daemon, the Status becomes <code>Applied</code>.

#

When the **Status** is `Invalid`, the status name is followed by the invalid properties delimited by comma (,) and surrounded by the square brackets. For example, the **URL** and **Depth** properties are invalid, the status is displayed as follows: `Invalid[URL, Depth]`.
You can check the properties with the invalid values by the messages output to the common message log.

4.7.5 Distributing the Task information

You can distribute the defined tasks to the multiple PFM - Agent for Service Response servers. If you add or delete a node of the task or specify property values, you can distribute the properties from that agent server to the destination agent servers so that the property settings with the tree structures of the source server and the destination servers become the same.

You can distribute the properties under the **Agent** folder and the properties under the **Task List** folder under the **Probe** folder. For details about the properties, see [E.2 Agent Collector service properties](#).

Since the other setting items (such as the passwords and the Web transaction file) are not distributed, you must define these settings on each PFM - Agent for Service Response server.

You can distribute the defined tasks when the version of PFM - Manager and PFM - Web Console is 08-11 or later.

For details about distributing the properties, see the chapter that describes operation monitoring, in the *JPI/Performance Management User's Guide*.

5

Starting and Stopping

This chapter describes how to start and stop PFM - Agent for Service Response. It also provides information you should make note of before you begin using PFM - Agent for Service Response.

5.1 Starting and stopping PFM - Agent for Service Response

This section describes the services provided by PFM - Agent for Service Response, and how to start and stop services. When you change the settings for measurement conditions, or when you perform recovery processing, you must start and stop the PFM - Agent for Service Response services manually. This section explains how to start and stop the services specific to PFM - Agent for Service Response.

5.1.1 List of the PFM - Agent for Service Response services

The following table lists the services of PFM - Agent for Service Response.

Table 5–1: List of services

Service name	Use
PFM - Agent for Service Response	Collects performance data.
PFM - Agent Store for Service Response	Manages performance data.
Extensible Service Probe	Measures a communication protocol's response performance.
Extensible Service IE Probe	Manages the program that measures a response performance of the operations in the Internet Explorer.
Hitachi Network Object plaza Trace Monitor 2	Enables you to use the Hitachi Network Object plaza Trace Library (HNTRLib2).

The start method and account for each service are set as follows:

- PFM - Agent for Service Response
Start method: *Manual*
Account: *System*
- PFM - Agent Store for Service Response
Start method: *Automatic*
Account: *System*
- Extensible Service Probe
Start method: *Manual*
Account: *System*
- Extensible Service IE Probe
Start method: *Manual*
Account: *System*[#]
- Hitachi Network Object plaza Trace Monitor 2
Start method: *Automatic*
Account: *System*

#

If you use the service, you must specify the account and the password for the measurement.

You use the following procedure to set a service of PFM - Agent for Service Response to start automatically at the time of system startup.

To set the services to start automatically:

1. From the Windows **Control Panel**, choose **Administrative Tools**, then **Services**.
2. Right-click the PFM - Agent for Service Response service and from the displayed pop-up menu, choose **Properties**.
3. In the Properties dialog box, choose **Startup type**, then **Automatic**.

5.1.2 Starting services

The following shows the procedure for starting the services of PFM - Agent for Service Response.

(1) Starting the services other than the IE Probe Daemon service

The following shows the procedure for starting the services other than the IE Probe Daemon service:

1. From the Windows Control Panel, choose Administrative Tools, then Services.
2. From the list of services, click the Start button for, in this order, the PFM - Agent Store for Service Response service, and the PFM - Agent for Service Response service.

(2) Starting the IE Probe Daemon service

The IE Probe Daemon service can be started in two ways: *as a Windows service* or *as an application*. You can use either of them to start the service.

- Start as a Windows service

From the Windows **Control Panel**, choose **Administrative Tools**, then **Services**. From the list of services, click the **Start** button for, in this order, the PFM - Agent Store for Service Response service, and the PFM - Agent for Service Response service.[#]

#

For details about the setting of using the Windows services to start and stop the IE probe service, see [5.1.5 Starting and stopping the IE probe service using the Windows services](#).

- Start as an application

From Windows Start menu, choose All Programs, Performance Management, Agent Option for Service Response, and then IE Probe.

5.1.3 Stopping services

The following shows the procedure for stopping the services of PFM - Agent for Service Response.

(1) Stopping the services other than the IE Probe Daemon service

The following shows the procedure for stopping the services other than the IE Probe Daemon service.

1. From the Windows **Control Panel**, choose **Administrative Tools**, then **Services**.
2. From the list of services, click the **Stop** button for, in this order, the PFM - Agent for Service Response service, and the PFM - Agent Store for Service Response service.

(2) Stopping the IE Probe Daemon service

The following shows the procedure for stopping the IE Probe Daemon service.

- Start as a Windows service

From the Windows **Control Panel**, choose **Administrative Tools**, then **Services**. From the list of services, click the **Stop** button for, in this order, the PFM - Agent for Service Response service, and the PFM - Agent Store for Service Response service.[#]

#

For details about the setting of using the Windows services to stop the IE probe service, see [5.1.5 Starting and stopping the IE probe service using the Windows services](#).

- Start as an application

Right-click the **IE Probe** icon on the system tray, and from the popup menu choose **Exit**.

5.1.4 Using commands to start and stop services

For details about how to use commands to start and stop services, see the manual *JP1/Performance Management Reference*.

5.1.5 Starting and stopping the IE probe service using the Windows services

The following shows the settings necessary to start and stop the IE Probe Daemon service using the Windows services.

(1) Setting the Probe action condition definition file

If you use the Windows services to start and stop the IE Probe Daemon service, change the setting of the Probe action condition definition file.

1. Set `Y` to the value of the `ie_service_flag` in the [General] section of the Probe action condition definition file (`esp.conf`).

When you upgrade PFM - Agent for Service Response, the Probe action condition definition file does not have the entry of the `ie_service_flag` in the [General] section. Add the `ie_service_flag` entry and set the value in the file.

For details about the Probe action condition definition file, see [8.2 Probe action condition definition file \(esp.conf\)](#).

To apply the definitions specified in the Probe action condition definition file, you must restart PFM - Agent for Service Response.

(2) Setting the account for measurement

Create an account for measuring the performance of the Internet Explorer operations.

(3) Setting the environment for measuring the IE scenario

The following shows the procedure for setting the environment for measuring the IE scenario.

1. Use the account for measurement and log on to the Windows.
2. From the **Tools** menu in Internet Explorer, choose **Internet Options**, then the **Internet Options** window appears.
3. In the **Internet Options** window, set the environment of measuring the IE scenario.
4. Click the **OK** button in the **Internet Options** window.

(4) Recording the IE scenarios

The following shows the procedure for operating in the IE windows section of the IE Recorder (main) window and recording the operations as an IE scenario.

1. Use the account for measurement, and log on to the Windows.
2. In the IE Recorder (main) window, from the **File** menu, choose **New**.
A new IE scenario file is created.
3. From the **Action** menu, choose **Record**.
Start recording the IE scenario.
4. In **Address**, enter the URL that you start to record, click the **Enter** key.
The Web page is displayed in the IE window section.
5. Operate in the displayed Web page in the IE window section.
The information of the operations is recorded as an IE scenario. The recorded information is displayed in the Operation list. You can record not only an operation, but also a series of tasks consisting of multiple sets of operations in the Internet Explorer as an IE scenario.
6. From the **Action** menu, choose **Stop**.
Stop recording the IE scenario.

(5) Check whether the IE scenarios are replayed correctly

Conduct a measurement after you check whether the recorded IE scenarios are replayed correctly in the IE scenario created in (4) *Recording the IE scenarios*.

(6) Setting the log-on account for the service

You need Administrator permissions to set the log-on account for the service.

The following shows the procedure for setting the log-on account for the Extensible Service IE Probe service.

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**.
2. Select Extensible Service IE Probe service, from the **Action** menu, choose **Properties**, and then the Properties of Extensible Service IE Probe dialog box appears.
3. Click the **This account** button on the **Log On** tab, then the **Browse** button is activated.
4. Specify a user account[#] that executes the service in the **Account** text box. Click the **Browse** button, the user account can be specified in the **Select User** dialog box.

#

Specify the user account that executes the service is the account for checking and measuring the IE scenarios you use in (5) *Check whether the IE scenarios are replayed correctly*.

5. Enter the password in the **Password** and **Confirm password** text boxes, and then click the **OK** button.

(7) Starting the service

You need Administrator permissions to start the service.

The following shows the procedure for starting the IE Probe Daemon service.

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**.
2. From the list of services, click the **Start** button for, in this order, the PFM - Agent Store for Service Response service, and the PFM - Agent for Service Response service.
The Extensible Service IE Probe service is started.

(8) Stopping the service

You need Administrator permissions to stop the service.

The following shows the procedure for stopping the IE Probe Daemon service.

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**.
2. From the list of services, click the **Stop** button for, in this order, the PFM - Agent for Service Response service, and the PFM - Agent Store for Service Response service.
The Extensible Service IE Probe service is stopped.

5.1.6 Notes about starting the IE probe

For the monitored Web page, specify the version of Internet Explorer where the IE probe is to be operated. The following shows the procedure to specify the version of Internet Explorer:

1. Before starting the IE probe, specify a value for `ie_probe_browser_mode` in the Probe action condition definition file (`esp.conf`).
Specify the same value as the value of `ie_rec_browser_mode` in the IE Recorder action condition definition file (`jpgcvierec.conf`) that is specified in [4.5.2\(1\) Starting the IE Recorder](#).
For details about the values of `ie_probe_browser_mode` in the Probe action condition definition file (`esp.conf`), see [Table 8-8 Definition in the IE Probe section](#).

5.2 Notes on operations

This section provides information you should make note of before you begin using PFM - Agent for Service Response.

5.2.1 Notes on system operation

(1) Changing the time at the host where PFM - Agent for Service Response is run

(a) Setting the time manually

To set the time manually:

1. Terminate the processes of PFM - Agent for Service Response.
If you are going to change the time backward to a point that has already passed, make note of the current system time.
2. Change the system time.
If you have changed the time backward, wait until the new system time reaches the time that was noted in step 1.
3. Start the processes that were terminated in step 1.

Note:

When you change the time manually at the host where PFM - Agent for Service Response is running, terminate PFM - Agent for Service Response before you make the time change.

(b) Using NTP to adjust the time

Typically, you will use NTP over a long period to make a series of small adjustments to the system time so that applications are not affected. This method of time adjustment can be used while PFM - Agent for Service Response is running.

(c) Using SNTP to adjust the time

SNTP is typically used to make a single adjustment to the system time so that it matches the actual time, in the same manner as when you set the time manually. This may result in a significant change to the system time, so you should make sure that this method is not used while PFM - Agent for Service Response is running. When you use SNTP, use the same procedure as when you set the time manually.

(d) Using any other method to adjust the time

If you are sure that the time adjustment method to be used will not affect the operation of normal applications, implement the method in the same manner as when NTP is used. If there is no such assurance, implement the method in the same manner as when SNTP is used.

(2) Starting automatically the IE probe

To start the IE probe from the **Start** menu of Windows, you must log on to the host by the account for measurement. When you cannot manually log on to the host after restarting the Windows (such as when you schedule the automatic reboot of the system), consider to place the IE Probe in the Startup folder and enable the automatic logon in Windows. If you use the Windows services to start IE Probe, you do not have to enable the automatic logon. For details about

setting to start the IE probe using the Windows service, see [5.1.5 Starting and stopping the IE probe service using the Windows services](#).

The following shows the procedure for starting the IE probe from the Startup folder in Windows.

Note:

If the host joins a domain, you cannot enable automatic logon in Windows by the following procedure. In that case, log on to the host manually and start the IE probe.

1. Create the account for measurement.
2. Enable automatic logon in Windows.
For setting automatic logon in Windows, see your Windows documentation.
3. Place the IE probe in the **Startup** folder of the account created by the procedure 1.

(3) Security management when using the IE probe

To start the IE probe from the Windows **Start** menu, you must log on to the host by the account for measurement. For the sake of security, consider the following operations:

- Control the physical or software access to the host so as to prevent the unauthorized use.
- Use the screensaver password protection to prevent the unauthorized use.

5.2.2 Notes about the functions of PFM - Agent for Service Response

(1) Considerations needed for performing successful measurement

This subsection discusses points to be taken into consideration when you determine the maximum number of measurement conditions for a probe and an IE probe that are defined in the Probe action condition settings file (`esp.conf`), and when you determine the measurement interval and timeout value that are defined in the measurement condition registration file (`esptask.xml`).

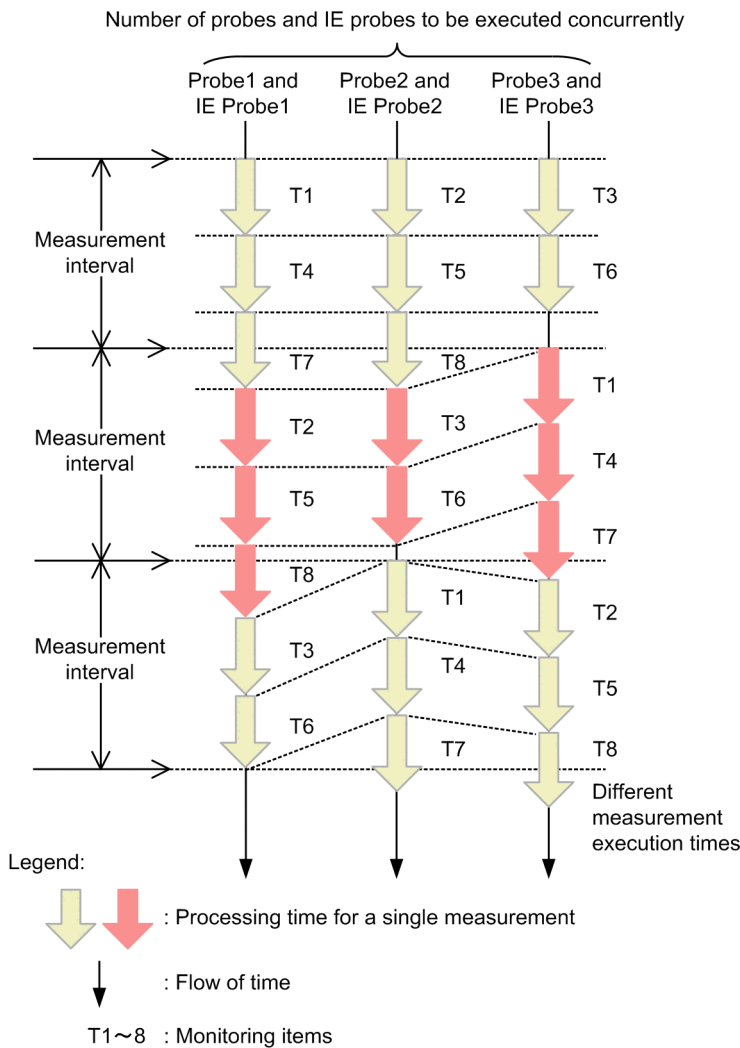
You must consider each parameters for both the probe and the IE probe.

(a) Maximum number of measurement conditions for a probe and an IE probe

PFM - Agent for Service Response can measure multiple Internet services concurrently. The number of measurement conditions that can be measured concurrently is specified as the maximum number of measurement conditions for a probe and an IE probe in the Probe action condition settings file (`esp.conf`). If the number of concurrent measurement conditions that is specified is greater than the set maximum number of measurement conditions for a probe and an IE probe, any excess measurement conditions will be processed sequentially.

In the example shown below, the maximum number of measurement conditions for a probe and an IE probe is 3, and the number of measurement conditions to be executed concurrently is 7. This example assumes that all measurement conditions terminate at the same time.

Figure 5–1: Example of measurement when the number of measurement conditions to be executed concurrently is greater than the maximum number of measurement conditions for a probe and an IE probe



The probes used to measure the services function as threads. The number of threads to be generated is the same as the maximum number of measurement conditions for the probe and the IE probes in the probe and the IE Probe action condition settings file. Therefore, when you determine the maximum number of measurement conditions for a probe and an IE probe, take into account the performance of the host where PFM - Agent for Service Response is run.

(b) Timeout value

The purpose of the timeout value is to abort the monitoring so as not to affect the other IE scenario monitoring when the response performance of the IE scenario is extremely degraded. When a timeout occurs, PFM - Agent for Service Response treats it not as the degraded response performance of the IE scenario, but as the abnormal state. Specify the timeout value to each IE scenario.

The maximum processing time permitted for a single measurement is the timeout value that is set as a measurement condition. Set the timeout value to be smaller than the measurement interval, so that a single measurement is completed before the next measurement begins.

The target service's total response time depends on the status, such as the number of requests that arrive concurrently at the server providing the target service, and the status of the network connecting the server and PFM - Agent for

Service Response. Specify for the timeout value a value that is greater than the minimum total response time when the service is running normally, so that a measurement is completed within the timeout value.

The following shows the recommended procedure for setting the timeout value for measuring by the IE probe:

1. Replay the IE scenario placing the maximum load on the system, and estimate an approximate value of the measurement time.
2. Specify the timeout value greater than the value acquired by the above procedure 1, and measure by the IE probe.
3. Based on the measurement results, specify the timeout value more than the greatest values of the actual observed values.

(c) When a measurement cannot be completed within the measurement interval

Depending on the combination of the maximum number of measurement conditions for a probe and an IE probe, the timeout value, and the measurement interval, some measurements may not be completed within the measurement interval, thus disrupting the execution of measurements in a specific interval. To insure that measurement processing is completed for all measurement conditions within the specified measurement interval even if a timeout occurs, the number of measurement conditions, the maximum number of measurement conditions for a probe and an IE probe, the timeout value, and the measurement interval must all satisfy the following condition:

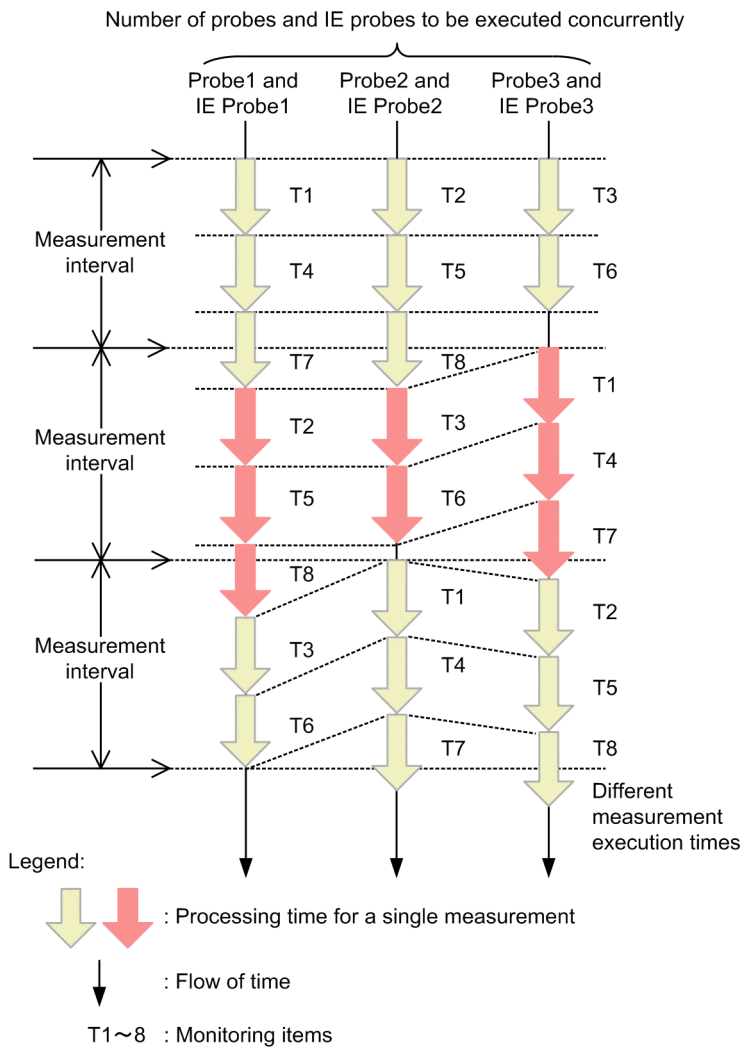
Minimum measurement interval =

((number of measurement conditions + (maximum number of measurement conditions - 1)) / maximum number of measurement conditions) x maximum timeout value

Round off the result.

Following is an example in which this condition is not satisfied.

Figure 5–2: Example when measurement processing cannot be executed within the specified interval



This example measures eight measurement items (T1 through T8) in an environment in which the maximum number of measurement conditions for a probe or an IE probe is 3. Because the first T7 and T8 are not completed within the measurement interval, the measurement execution times for the second T2 and T3 are delayed, and this delay increases further at the end of the second T8. Thus, the delay in the measurement execution time accumulates to a point where performing the measurement at the specified interval becomes impossible. If this occurs, a warning message (KAVK08160-W or KAVK10100-W) is output to the log file. Check and, if necessary, revise the maximum number of measurement conditions for a probe or an IE probe, the measurement interval, and the timeout value.

(2) Notes about Agent Collector's collection interval settings

PFM - Agent for Service Response uses the Probe Daemon and the IE Probe Daemon to measure a target's response time. The measurement result is output once to a report file. Agent Collector collects the most recent measurement result stored in the report file. Depending on the Agent Collector's collection interval settings and the Probe Daemon and the IE Probe Daemon's measurement interval settings, part of the performance data may not be stored. Therefore, you must take into account the following:

- Relationship between Agent Collector's collection interval and Probe Daemon's measurement interval and IE Probe Daemon's measurement interval:

Specify the settings in such a way that Agent Collector's collection interval is equal to or greater than Probe Daemon's measurement interval and IE Probe Daemon's measurement interval. A guideline is to set Agent Collector's collection interval to twice the value of Probe Daemon's measurement interval and IE Probe Daemon's measurement interval.

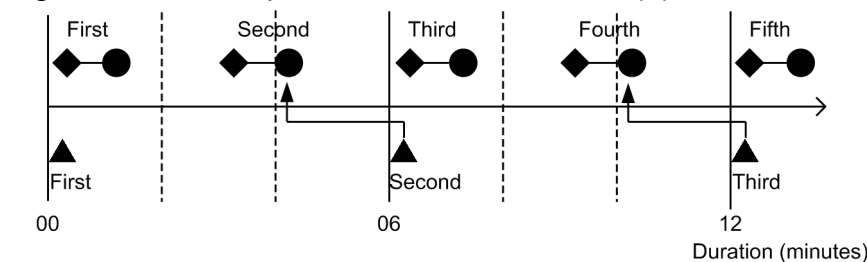
- Relationship between Agent Collector's collection interval and Probe Daemon's timeout value and IE Probe Daemon's timeout value:

Specify the settings in such a way that Agent Collector's collection interval is greater than Probe Daemon's timeout value or IE Probe Daemon's timeout value.

Example 1:

The following figure shows the Probe Daemon's measurement schedule or the IE Probe Daemon's measurement schedule and Agent Collector's collection schedule under these conditions: Agent Collector's collection interval is set to 360 seconds (6 minutes), the Probe Daemon's measurement interval or the IE Probe Daemon's measurement interval is 240 seconds (4 minutes), and the Probe Daemon's timeout value or the IE Probe Daemon's timeout value is 60 seconds (1 minute).

Figure 5–3: Example of collection schedule (1)



Legend:

- ◆ : Measurement by Probe Daemon and IE Probe Daemon starts
- : Measurement by Probe Daemon and IE Probe Daemon ends
- ▲ : Collection of performance data by Agent Collector
- ← : Data collection

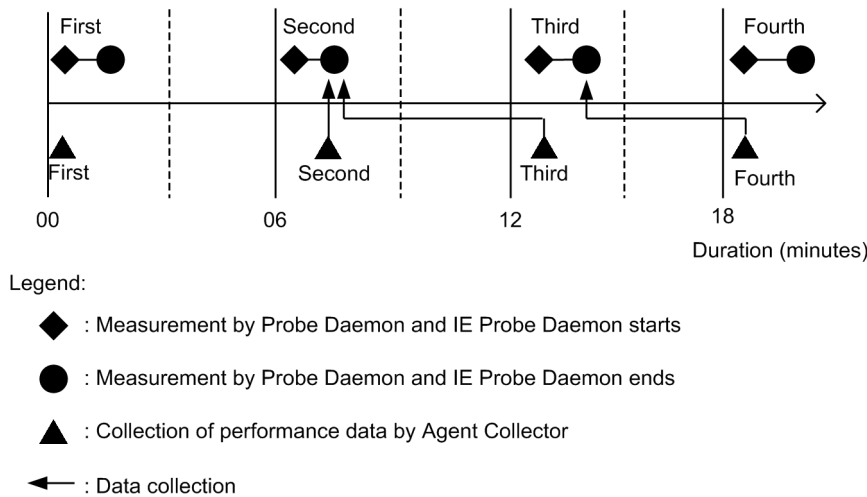
In this example, the third measurement result is not collected because the fourth measurement is completed before the result of Probe Daemon's third measurement or IE Probe Daemon's third measurement is collected by Agent Collector.

You can set Agent Collector's collection interval from PFM - Web Console. You use the measurement condition registration file to set the Probe Daemon's measurement interval or IE Probe Daemon's measurement interval. For details about setting Agent Collector's collection interval, see the chapter that describes agent monitoring in the *JP1/Performance Management User's Guide*. For details about the measurement condition registration file, see [8.3 Measurement condition registration file \(esptask.xml\)](#).

Example 2:

The following figure shows the Probe Daemon's measurement schedule or IE Probe Daemon's measurement schedule and Agent Collector's collection schedule when Agent Collector's collection interval and the Probe Daemon's measurement interval or IE Probe Daemon's measurement interval are both set to 360 seconds (6 minutes), and when the Probe Daemon's timeout value or IE Probe Daemon's timeout value is 60 seconds (1 minute).

Figure 5-4: Example of collection schedule (2)



In this example, the following shows the procedure for collecting data.

1. When the Agent Collector collects the Probe Daemon's or the IE Probe Daemon's measurement results for the first time, the Agent Collector does not collect the measurement result because the Probe Daemon or the IE Probe Daemon does not complete their measurement. The Agent Collector succeeds in collecting the measurement results for the second or later times.
2. Assume that the second collection of the Agent Collector is late due to the heavy burden on the machine or so. In this case, if the Agent Collector collects the measurement result after the Probe Daemon or the IE Probe Daemon completes their measurement, the Agent Collector collects their second measurement result.
3. When the Agent Collector collects the measurement result for the third time, the Probe Daemon's or the IE Probe Daemon's second measurement result is collected, but the Agent Collector does not store the measurement result because the collected result is already stored in the above procedure 2.
4. When the Agent Collector collects the measurement result for the fourth time, the Probe Daemon's or the IE Probe Daemon's third measurement result is collected.

In this example, although the performance data of the Probe Daemon's or the IE Probe Daemon's third measurement is collected, the Agent Collector does not store the data so that the performance data from the second to the fourth measurement (i.e. 12 minutes) lacks. Into this lack of the performance data, you can interpolate the data using the previously collected performance data.

For details about how to interpolate the data into the lack of the performance data, see [3.4.4 Interpolating performance data](#). Hitachi recommends that you properly specify the Agent Collector's collection interval and the Probe Daemon's or the IE Probe Daemon's measurement interval in order to prevent the lack of the performance data.

(3) Notes about service monitoring

The following notes are on the service monitoring:

1. If the port number for a probe and an IE probe defined in the measurement conditions for DHCP has already been used (such as when the machine on which this product is installed is running as a DHCP client), this product may not be able to monitor DHCP correctly.
2. PFM - Agent for Service Response ignores cookie information specified in the `meta` HTML tags that are acquired during monitoring of HTTP(S) and Web transactions.

3. With respect to an embedded resource acquisition error during Web transaction monitoring, this product continues measurement processing even if acquisition of embedded resources based on the default settings fails. To treat an embedded resource acquisition error as a monitoring error, specify the following settings in the Probe action condition definition file (`esp.conf`):

Section name: `WEBTRANS Probe`

Key name: `skip_emb_rsc_error`

Value to be set: `N`

4. In Web transaction monitoring, the `GET` method is used to redirect the `POST` method.
5. In Web transaction monitoring, if response determination is to be performed on HTML whose character set is not `Shift_JIS` on Japanese OS or `GB18030` on Chinese OS, specify the correct character set for the corresponding step.

You use the `<DEFAULT_CHARSET>` or `<CHARSET>` tag in the Web transaction file to specify a character set.

When the character set does not specified in the `<DEFAULT_CHARSET>` or `<CHARSET>` tag, `Shift_JIS` is assumed for Japanese OS, `GB18030` is assumed for Chinese OS and `US-ASCII` is assumed for other OS.

If the HTML character set cannot be specified with the `<DEFAULT_CHARSET>` or `<CHARSET>` tag, do not specify multi-byte characters in a character string used for response determination.

6. If FTP monitoring is to be performed in an environment in which a Windows firewall is in effect, reception of the FTP server's response message for logout (`QUIT` command entry) may fail. To avoid this, specify the following settings in the Probe action condition definition file (`esp.conf`):

Section name: `FTP Probe`

Key name: `ignore_quit_resp_rcv_error`

Value to be set: `Y`

7. In Web transaction monitoring, if a URL in a request to be issued contains the hash mark (`#`), PFM - Agent for Service Response treats the character string following the `#` as a fragment specification (with its location specified in HTML), and deletes the fragment part before issuing the request. Thus, if a defined URL or substitute string for a variable string contains a `#` character that is not intended to be the delimiter for a fragment, add a `#` character at the end of the defined URL.
8. In Web transaction monitoring, measurement may fail if the acquired HTML character set is not `Shift_JIS` on Japanese OS, and if the response determination information or substitute string for dynamic session management support contains multi-byte characters. Make sure that there are no multi-byte characters in the response determination information or in the substitute string for dynamic session management support.

For Chinese OS, measurement may fail if the acquired HTML character set is not `GB18030`, and if the response determination information or substitute string for dynamic session management support contains Chinese characters.

9. Notes about searching elements that contain substitute strings in Web transaction monitoring:

When a substitute string is obtained from HTML, elements containing the substitute string are searched for.

In this case, the specifications of this product are as follows:

(i) If an element with the specified name does not have the end tag (`</element-name>`), its start tag (`<element-name>`) up to the start tag of the next element with the same name is treated as the element. If there is no element with the same name, the start tag through the end of the HTML file is treated as the element.

(ii) If the end tag of an element with the specified name (`</element-name>`) is preceded by the start tag of an element with the same name (`<element-name>`), up to the start tag of the element with the same name is treated as the element.

(iii) If an element with the specified name is the null element (`<element-name/>`) and its attribute value is not enclosed in quotation marks (`"` or `'`), and if the attribute value is continued to the end of the null element (`/>`), the value up to `/` is treated as the attribute value.

In the example below, the value of the `value` attribute is `user01/`:


```
<input type=hidden name=userid value=user01/>
```

To use user01 as the value of the value attribute, change the specification as follows:

Suggestion 1: Change the null element to the start tag:

```
<input type=hidden name=userid value=user01>
```

Suggestion 2: Separate the attribute value and the end of the null element with a space:

```
<input type=hidden name=userid value=user01 />
```

Suggestion 3: Enclose the attribute value in quotation marks:

```
<input type=hidden name=userid value="user01"/>
```

10. In Web transaction monitoring, if a substitute string contains a character that is treated as a delimiter in the URL, such as the ?, &, or =, PFM - Agent for Service Response replaces it with a variable string as is and issues the request. If you want to encode the characters treated as the delimiters in the URL string, specify the `<SUBSTITUTE_FORCE_URL_ENCODE>` tag in the Web transaction file. For details about the `<SUBSTITUTE_FORCE_URL_ENCODE>` tag, see *8.5.2 Format and definition of the Web transaction measurement conditions*.
11. Measurement fails on a POP3 server that does not support POP3 UIDL commands. Some older versions of POP3 servers may not support UIDL commands.
12. In Web transaction monitoring, if a substitute string is to be searched for in the acquired HTML and the attribute value of some element specified in the HTML contains < or >, the substitute character search fails, resulting in an invalid measurement result.
13. In Web transaction monitoring, a transaction that uploads files using the POST method (to transfer files from this product to the monitored server) cannot be monitored successfully. Specifically, this applies when the following conditions overlap in the definition:
 - The POST method is used.
 - The message body is in the format `multipart/form-data`.
 - The message body contains a part (delimited by a separator) that specifies the `filename` attribute of the `Content-Disposition` header.
14. If the network connection between this product and the monitoring target goes through a proxy function, such as *JP1/Cm2/Internet Gateway Server*, the following items may not be monitored correctly:
 - DNS
 - DHCP
 - FTP
 - TCP
15. To use GB18030 as encoding type in Chinese OS, you cannot use the 4 bytes characters. If you use them, the measurement might not perform correctly.
16. When PFM - Agent for Service Response is started or reloaded, the definitions in the Web transaction file that are registered in the measurement condition registration file (`esptask.xml`) are verified. If the verification results indicate a syntax error[#], the Probe Daemon (a measurement process) cannot start. Correct the syntax error, and restart PFM - Agent for Service Response.

#

The following are examples of syntax errors:

- An XML tag contains an error (a format error in the Web transaction file).
- The user to be authenticated is specified, but no password is specified (including a situation where a password is not correctly registered with the `esppasswd` command).

17. If an OS to be monitored is Window Server 2012 or later and the failover function is used, the DHCP service cannot be measured.
18. The measurement of HTTP(S) and the Web transaction supports the following protocols in communication of SSL performed between a probe and the Web servers for the monitor.
- TLSv1.0
 - TLSv1.1
 - TLSv1.2

About SSLv2.0 and SSLv3.0 which are the protocol that is lower than the above, PFM - Agent for Service Response disables it. However, you can enable the `enable_low_level_ssl_protocol` key to general section of ESPCONF by setting when Web server aimed for monitor permits communication by these protocols. But we do not recommend that you enable SSLv2 and SSLv3 which are the protocol that is lower. For more information about `enable_low_level_ssl_protocol` key, refer to "[Table 8-3 Definition in the General section](#)".

5.2.3 Notes on IE scenarios

The following notes are on IE scenarios:

(1) Operations and actions in Internet Explorer that can be recorded and measured as IE scenarios

You can record as IE scenarios the operations and actions in the static window such as the Web page transition by navigating in the Internet Explorer, selecting the radio button, the check box, and the button on the Web page. These page transitions time is measured.

The following table shows whether you can operate in the recording mode of the IE Recorder the recorded operations and actions:

Table 5–2: Operations and actions in Internet Explorer that can be recorded and measured as IE scenario

Classification		Action	Record	Remarks
Mouse operations	--	--	--	Records the operations occurred by mouse operations (such as button operations). The mouse operations themselves are not recorded.
	Click	Y	N	Records the operations as the button operations when you click the button. The click operations themselves are not recorded.
	Double-click	Y	N	Records the operations as the button operations when you double-click the button. The double-click operations themselves are not recorded.
	Click secondary button	Y	N	--
	Vertical scroll wheel	Y	N	--
	Horizontal scroll wheel	Y	N	--
Keyboard operations (Keystroke operations)	--	--	--	Records the operations occurred by keystroke actions as the HTML operations or the browsing operations. The keystroke actions themselves are not recorded.

Classification		Action	Record	Remarks
Keyboard operations (Keystroke operations)	Enter characters	Y	N	Records the values that are entered as the HTML operations or so.
	Use shortcut keys	Y	N	Records the corresponding menu operations.
	Use accelerator keys	Y	N	
	Enter other keys	Y	N	--
Browsing operations	--	--	--	--
	Help [F1]	N	N	--
	Toggle between full-screen and regular-view of the browser window [F11]	N	N	--
	Move forward through the items on a Web page, the Address bar, or the Favorites bar [TAB]	Y	N	--
	Move back through the items on a Web page, the Address bar, or the Favorites bar [Shift]+[TAB]	Y	N	--
	Go to your home page [Alt]+[HOME]	N	N	--
	Go to the next page [Alt]+[Right Arrow]	Y	Y	Pressing Alt key and Right Arrow key is ineffective.
	Go to the previous page [Alt]+[Left Arrow] or [Back Space]	Y	Y	Pressing Alt key and Left Arrow key is ineffective.
	Display a context menu [Right-click] [Shift]+[F10]	Y	N	Pressing Shift key and F10 key is ineffective.
	Move to the next frame [Ctrl]+[TAB] [F6]	Y	N	Pressing F6 key is ineffective.
	Move to the previous frame [Shift]+[Ctrl]+[TAB]	Y	N	--
	Scroll up [Up Arrow]	Y	N	--
	Scroll down [Down Arrow]	Y	N	--
	Move up one screen at a time [Page UP]	Y	N	--
	Move down one screen at a time [Page Down]	Y	N	--
	Move to the beginning of the page	Y	N	--

Classification		Action	Record	Remarks
Browsing operations	[HOME]	Y	N	--
	Move the end of the page [END]	Y	N	--
	Find on this Web page [Ctrl]+[F]	N	N	--
	Refresh the current Web page [F5] [Ctrl]+[R]	Y	Y	Pressing F5 key, or Ctrl key and R key are ineffective.
	Refresh Web page forcedly [Ctrl]+[F5]	N	N	Refresh Web page that has same time stamp.
	Cancel the current task [ESC]	N	N	--
	Open a new file [Ctrl]+[O] [Ctrl]+[L]	N	N	--
	Open a new window [Ctrl]+[N]	N	N	--
	Close the current window [Ctrl]+[W]	Y	N	Records operations such as closing the tab.
	Save the current page [Ctrl]+[S]	N	N	--
	Print the current page [Ctrl]+[P]	N	N	--
	Click a link [Enter] [Click]	Y	Y	Regarded as the same operation as clicking a link operation of the HTML operations.
	Display the Search bar [Ctrl]+[E]	N	N	--
	Display the Favorites bar [Ctrl]+[I]	N	N	--
	Display the History bar [Ctrl]+[H]	N	N	--
	Select multiple items [Ctrl]+[Click]	Y	N	--
	Cut [Ctrl]+[X]	N	N	--
	Copy [Ctrl]+[C]	N	N	--
	Paste [Ctrl]+[V]	N	N	--
	Select all [Ctrl]+[A]	N	N	--

Classification		Action	Record	Remarks
Dialog box operations	--	--	--	Does not record the operations of entering items in a dialog box, such as enter text operations and button operations, but obtains and replays the entered data, such as entered values and results of button operations.
	Enter texts operations	Y	#1	Records the entered values.
	Button operations	Y	#1	If you close a dialog box using other button, the operation is not replayed. ^{#2}
	Other input operations	Y	#1	Records those operations, but does not replay them when replaying (uses the recorded data only).
HTML operations	--	--	--	Records the operations concerning entering items and navigating Web pages.
	Links	Y	Y	Records the link operations such as A tag and AREA tag operations.
	INPUT TEXT (Enter text)	Y	Y	--
	INPUT PASSWORD (Enter password)	Y	Y	--
	INPUT FILE	N	N	--
	INPUT CHECKBOX	Y	Y	--
	INPUT RADIO	Y	Y	--
	INPUT HIDDEN	Y	Y	--
	INPUT SUBMIT	Y	Y	--
	INPUT RESET	Y	Y	--
	INPUT BUTTON	Y	Y	Records executing the scripts.
	INPUT IMAGE	Y	Y	--
	INPUT SEARCH	Y	Y	--
	INPUT TELEPHONE	Y	Y	--
	INPUT URL	Y	Y	--
	INPUT EMAIL	Y	Y	--
	INPUT NUMBER	Y	Y	--
INPUT RANGE	Y	N	--	
Script operations	--	--	--	Does not record processing within a script that has no operations such as navigating Web pages, HTML operations, and button operations, but records the operations (such as navigating Web pages, HTML operations, and button operations) that occur due to a script process. ^{#4}
	Navigating Web pages	Y	Y	Some operations that are implemented in a script may not be recorded, but the Web page transitions are recorded.
	Drawing	Y	N	Does not record drawing processes (such as buttons on the screen) that are implemented in a script. ^{#5}
	Mouse operations	Y	N	Same as the <i>Mouse operations</i> classification.

Classification		Action	Record	Remarks
Script operations	Mouse operations	Y	N	Does not record the mouse operations themselves that are within the script, but records button operations that occur due to mouse operations. #3, #6
	Keyboard operations (keystroke operations)	Y	N	Same as the <i>Keyboard operations</i> classification. Does not record the enter text operations themselves that are within the script, but records them as HTML operations that occur due to keystroke operations.
	Dialog box operations	Y	#1	Same as the <i>Dialog box operations</i> classification. Does not record the dialog box operations themselves that occur due to the script, but obtains and replays the entered values and the results of button operations.
ActiveX control operations	--	--	--	Not records the operations of the ActiveX control embedded in the page except the Web page transition.
	Flash/Flex	Y	Δ	#3
	Shockwave	Y	Δ	#3
	QuickTime	Y	Δ	#3
	Windows Media Player	Y	Δ	#3
	Java Applet	Y	Δ	#3

Legend:

In Action column Y: You can operate those operations in the record mode of the IE Recorder, N: You cannot operate those operations in the record mode of the IE Recorder.

In Record column Y: Recordable, Δ: Not recordable, but there is an alternative means of measuring, N: Not recordable.

#1

Replays are based on the results of operations such as the values entered in dialog boxes and button operations, but the operations on some dialog boxes may not be replayed correctly. Make sure that you replay in advance the operations and check whether the recorded operations are replayed correctly after you record these operations.

If replaying is suspended with the dialog box displayed or so when you check, PFM - Agent for Service Response does not support these kinds of dialog boxes.

#2

The operations in the dialog box are not recorded, but the last click button operation is recorded and replayed.

#3

The operations in the contents are not recorded, but since the Web page transitions that occur due to these operations are recorded, it may be possible to replay them. When replaying them, the measured time for displaying a window includes the measured time for downloading the contents themselves. After displaying the window, the measured time for replaying the operation at that time includes the measured time to communicate within the contents.

#4

Replays may not be possible depending on the timing of the Web page transitions, HTML operations, and button operations that occur due to script processes.

Be sure to replay an operation after it is recorded, to confirm that it can be replayed correctly.

#5

Drawing itself is not recorded. Therefore, if the script is run before the drawing of buttons, etc. is completed when measuring Web pages with script operations such as on-screen buttons, the operation cannot be replayed.

#6

If the script performs asynchronous communication linked to mouse operation, no mouse event will occur when the operation is replayed. Therefore, the asynchronous communication may not occur, and the time of the asynchronous communication may not be measured.

Operations and actions that are not listed in the above table cannot be recorded or measured as an IE scenario.

The IE Recorder does not support the authentication in the dialog boxes with other forms than the form with user ID and its password textboxes and within the ActiveX control. Also, it does not support the ftp protocol.

(2) Measurement range of replay time

This section describes the replay time measured by the IE probe and the measurement test of the IE Recorder. The following describes the example that you record the operations in ascending order of the No. in the following table list and measure the operations.

Table 5–3: Measurement range of replay time

No.	Operation	Flow of action for measurement	Measure	Tn	Description
1	Enter address	Enter text	N	--	The operation time to enter the text is not measured as the replay time.
		Start the Web page transition	Y	T1	The time from starting the Web page transition to completing it is measured as the replay time, immediately after entering the text.
		Complete the Web page transition ^{#1}	Y		
2	Popup dialog box	Display the dialog box	N	--	The replay time does not contain the time for the operations in the dialog box.
		Response the dialog box	N	--	
3	Start scope A	Start scope A	N	--	--
4	HTML operation (including the Web page transition)	Wait time for replaying ^{#2}	Y	T2	This operation is an action of the HTML operations with the page transition (such as clicking the link or the submit button) that leads to the Web page transition. After the wait time for replaying passes, the time from starting the Web page transition to complete it is measured as the replay time.
		Execute the operation	Y		
		Start the Web page transition	Y		
		Complete the Web page transition ^{#1}	Y		
5	HTML operation (not including the Web page transition) ^{#3}	Wait time for replaying ^{#2}	Y	T3	This operation is an action of the HTML operations without the page transition (such as entering texts and selecting check boxes). After the wait time for replaying passes, the time from starting the operation to complete it is measured as the replay time.
		Execute the operation	Y		
		Complete the operation	Y		
6	Navigation	Wait time for replaying ^{#2}	Y	T4	After the wait time for replaying passes, conduct the navigation and the time from starting the Web page transition to complete it is measured as the replay time.
		Execute the navigation	Y		
		Start the Web page transition	Y		
		Complete the Web page transition ^{#1}	Y		
7	End scope A	End scope A	N	--	--
8	Browsing operation	Wait time for replaying ^{#2}	Y	T5	After the wait time for replaying passes, conduct the browsing operation and the time from starting the Web page transition to complete it is measured as the replay time.
		Execute browsing operation	Y		
		Start the Web page transition	Y		
		Complete the Web page transition ^{#1}	Y		

Legend:

Y: Included in the replay time.

N: Not included in the replay time.

#1

If conducting an operation leads to the multiple Web page transitions, the time when all the page transitions complete is judged to be the completion of the Web page transition.

Take for example the transition to the page with the three frames when you click a link. Since the page transition occurs to the parent frame and the three child frames, the time when all page transitions complete is judged to be the completion of the Web page transition.

#2

If the **Wait to replay** check box in the **Operation Settings** window of the IE Recorder is specified, the wait time for replaying means the waiting the time specified in the **Wait time** text box for the operation to be conducted. Yet, if you specify the **If page transition occurs automatically, perform the next operation immediately**. check box, conducts the next operation immediately if a page transition occurs before the wait time passes. In short, the wait time for replaying varies depending on the replaying situations.

#3

As for the time for the HTML operations (without the page transitions), the time to be spent on its operations is not counted. For example, when replaying the entering texts operation, the time to be spent on entering texts is not replayed. As a result, the time to be spent on entering texts is very close to 0.

You can measure the following replay time, if you record the operations in the above table in order and measure that IE scenario:

- Total replay time
T1 + T2 + T3 + T4 + T5
- Replay time of the scope A
T2 + T3 + T4
- Replay time of each operation
T1, T2, T3, T4, T5

(3) Notes on recording and replaying the IE scenarios

The following notes are on recording and replaying the IE scenarios. If you replay the IE scenario with the unrecordable operations, replaying fails because PFM - Agent for Service Response cannot find the operation target when replaying the next operation to the unrecordable one.

Ask the Web page producer whether or not the following notes are applied to the operation target pages:

1. You cannot record the operations of the pages displayed in the <IFRAME> tags. If the page has the <IFRAME> tags, you can record and replay the operations in the other pages outside the <IFRAME> tags.

If you record the operations in the <IFRAME> tags and replay the operations by using the IE Recorder or the IE probe, the following malfunctions may occur:

- The operations of the <IFRAME> tags are not replayed.
- The operations to be performed after the operations of the <IFRAME> tags are executed cannot be replayed (a script error occurs or suspends replaying).
- If you record and replay the operation in the <IFRAME> tags which opens a new tab, replaying suspends.

The following table shows how to check whether the operations are performed on the pages displayed in the <IFRAME> tags.

How to check	Result	Determination
Display the source, and check whether the operation target tags are surrounded by the <IFRAME> tag and the </IFRAME> tag.	Surrounded by the <IFRAME> tag and the </IFRAME> tag.	The operation is performed on the page in the <IFRAME> tags.

How to check	Result	Determination
Display the page that you want to check by using the IE Recorder, and display the context menu in the target operations.	Other than the context menu of the IE Recorder is displayed.	The operation may be performed on the page in the <IFRAME> tags.
Perform operations such as clicking links or entering texts on the operation target when recording.	Only the navigation operation is recorded.	The operation may be performed on the page in the <IFRAME> tags.

2. You cannot record the operations in the pages that prevent the HTML operations (such as a click event) from triggering the events. For example, the operations in the site that disables the mouse click event by the `setCapture()` method of the JavaScript may not be recorded.

If you record the operations in this kind of sites and replay the operations by using the IE Recorder or the IE probe, the following malfunctions may occur:

- The operations in the Web pages that disable the events are not replayed.
3. The operations in the frame pages cannot be replayed, when the `NAME` attributes for each frame are not specified and their URLs are dynamic. In this case, specify the `NAME` attributes for each frame or change the dynamic URLs for each frame to the static ones. If you record the operations in this kind of frame pages and replay the operations by using the IE Recorder or the IE probe, the following malfunctions may occur:
- The operations in the frame page displayed by the <FRAME> tags are not replayed.
 - If the following operations premise that the operations in the frame page displayed by the <IFRAME> tags are completed, these operations cannot be replayed (for example, script errors occur or replaying is suspended).
4. If you turn off the **Display a notification about every script error** check box in the **Internet Options** windows, the IE Recorder or the IE probe displays the script error dialog box.
5. The script error dialog box is not recorded and replayed. You should revise the scripts so that the script errors do not occur.

Because the IE probe does not display the window, a script error might occur during measurement by the IE probe even if you can replay the operations in the IE Recorder without script errors.

Since the IE probe does not display the window, script errors may occur even if you can replay the operations in the IE Recorder without script errors. If you record the operations in this kind of sites and replay the operations by using the IE Recorder or the IE probe, the following malfunctions may occur:

- The error dialog box appears and then replaying is suspended.

Note that if you make the following settings in Internet Explorer, measurement may be possible without a script error occurring.

- Enable the settings for restricted sites. (Scripts disabled)
Use the following steps to check if these settings are enabled.
 1. Open the target page in Internet Explorer, select **File** and then **Properties** to check the zone in which the page is running.
 2. In **Internet Options**, click the **Security** tab, select **Restricted sites**, and then click the **Sites** button to add the target page.
 3. Click the **Custom level ...** button, and confirm that the following settings are disabled.

Scripting

- **Scripting of Java applets**

- **Active scripting**

- **Allow status bar updates via script**

ActiveX controls and plug-ins

- **Run ActiveX controls and plug-ins**

- Add the target page to the Compatibility View Settings.
6. The behavior of the IE Recorder toward a `Referer` header may be different from that of the Internet Explorer.
- Example:*
- When you replay the operation to open a new window by pressing a **shift** key and clicking a link in the Web page
- Therefore, if the Web sites analyze the `Referer` header and determines their responses, the operations in this kind of sites may not be recorded and replayed correctly.
- If you record the operations in this kind of sites and replay the operations by using the IE Recorder or the IE probe, the following malfunctions may occur:
- The Web server responses the errors because the IE Recorder or the IE probe does not send the requests with the `Referer` header.
7. When you record and replay the operations to the ActiveX control (such as Flash/Flex, Shockwave, QuickTime, and Windows Media Player) or the Java Applet in the monitoring target Web page, only the page transitions are recorded and replayed. Note that since the transition destination URLs are recorded the operations are not replayed correctly if the URLs are dynamic (i.e. different from the ones when recording).
- If you record the operations in this kind of sites and replay the operations by using the IE Recorder or the IE probe, the following malfunctions may occur:
- The operations to the ActiveX control or the Java Applet cannot be replayed.
 - If the following operations premise that the operations to the ActiveX control or the Java Applet are already executed, these operations cannot be replayed (for example, script errors occur or replaying is suspended).
 - If you record the operations to the ActiveX control or the Java Applet and a new tab opens, replaying these operations is suspended.
8. You cannot replay the operations correctly on a Web site if the page used to record operations is different from the page used to replay the operations. For example, if the Web site memorizes the page at logoff and displays the memorized page when the visitors log in again, the operations in this kind of site are not replayed correctly because the page used to replay changes whenever accessed. In this case, record the operations so that the page used to replay is constantly the same as the one when recording. If you record the operations in this kind of sites and replay the operations by using the IE Recorder or the IE probe, the following malfunction may occur:
- The operations to the Web page cannot be replayed correctly (for example, script errors occur or replaying is suspended).
9. Do not perform operations to the pages other than HTML (such as `.doc`, `.xls`, and `.pdf` documents) when recording. If you perform operations to these pages and record these operations, the following malfunctions may occur when replaying these IE scenarios in the IE Recorder and IE probe:
- The following operations which premise that the operation to the pages other than HTML is already done cannot be replayed.
 - You cannot start or operate the same application that displays the document in the IE recorder or the IE probe when replaying.
10. When you use the Internet Explorer, you cannot record and replay the operation to specify the **No** button in the **Security Warning** dialog box. If you record and replay in the IE Recorder or the IE probe, the following malfunction may occur:
- Replaying is suspended at the operation because of which the **Security Warning** dialog box appears.
11. The operations in the dialog box with its title name "IE Recorder" are not recorded and replayed. The title name is case sensitive.
12. You may not record and replay the operations after which the scripts are executed to change the users' input result. The following tables list the examples of the scripts and the problems to occur:

User operation	Example of script that changes the users' input result	Example of problems
Select an item from drop-down list or in check box	Selects the other item than the one selected by the user	<p><i>In recording</i></p> <p>The operation to select the selected item after executing the script is recorded.</p> <p><i>In replaying</i></p> <p>The other item than the one selected by the user is selected. As a result, the error occurs such as KAVK38752-E while performing the subsequent operations.</p>
	Transits the page specified as in the attribute value of the selected item, and selects the default items.	<p><i>In recording</i></p> <p>The operation to select is not recorded and the error KAVK38605-E occurs.</p> <p><i>In replaying</i></p> <p>Because the operation to select is not replayed, the page transition does not occur and the error occurs such as KAVK38752-E while performing the subsequent operations.</p>
Enter text	Changes the characters entered by the user	<p><i>In recording</i></p> <p>The other characters than the one entered by the user are recorded.</p> <p><i>In replaying</i></p> <p>Because the other characters than the one entered by the user are entered, the error occurs such as KAVK38752-E while performing the subsequent operations.</p>

The following shows how to check whether the script changes the users' input result:

How to check	Result	Determination
Replay the operations in the IE Recorder and check whether the input operations such as entering text, select an item from drop-down list or check box are performed in the same way as the ones when recording.	The values different from the values entered (selected) when recording are recorded.	Applicable

If the above procedure is difficult, alternatively you can use the Operation list in the IE Recorder (main) window to check the recorded values:

Operation	Display location of the entered (selected) value	Remarks
Enter text	After the operation name surrounded by "[" and "]"	--
Select an item	The value of the value attribute	You can also check the value in the HTML source.
option tag	Value of Inner text	You can also check the value in the value of the value attribute and the HTML source.

13. If not all the dialog boxes are recorded that appear while displaying the target Web site, the following error message is displayed and replaying is suspended: A popup dialog box which is not recorded while replaying the IE scenario appears. (KAVK38756, if the Logged Message for IE Scenario (PL_IESM) record is collected, 89504 is set in the IE Scenario Result Code field).

Note that the dialog box may appear only once depending on the condition.

For example, the dialog box that appears once whenever starting the application (such as the **Security Warning** dialog box), and the dialog box that appears once for each session (such as the **Authentication** dialog box).

Because the IE Recorder disconnects the sessions when its recording starts, it supports the dialog box that appears once for each session. Yet, it does not support the dialog box that appears once whenever starting the application. As a result, when the dialog box of this type appears, restart the IE Recorder before recording IE scenarios.

14. When you record the operations to the `<INPUT TYPE=IMAGE>` tags, only the click operations can be recorded and replayed. Since the coordinates entered by the mouse cannot be recorded and replayed, the operations cannot be replayed correctly in the pages whose behavior changes depending on the coordinates.
15. Replaying the IE scenarios may be stopped. How to handle this problem depends on the classification and type of the operations performed when replaying is stopped:

How to handle the problem when replaying the IE scenarios

Table 5–4: How to handle the problem when an IE scenario stops replaying

Classification of operation	Type of operation	How to handle
Browse operation	Navigation	Delete the operations. (For details, see 5.2.4 Notes on the navigation)
	Other operations not listed above	Re-create the IE scenarios.
HTML operation	All type	Re-create the IE scenarios.

Note:

If replaying the IE scenarios is stopped, it may be because the response from the Web server is late. In this case, you do not need to cope with this problem.

16. If the page is updated without a page transition, the operations in that page cannot be recorded and replayed correctly. The following shows the examples of the pages and problems:

Example of the pages	Example of the problems
The page with the button such as Add Input Column . If you click the button, displays an added input column (i.e. a part of the page is updated).	The operations to the added input column cannot be recorded.
The page with the drop-down menu (<code>SELECT</code> tag). If you select an item from the drop-down menu, a part of the page is updated depending on the selected item.	The operations to the updated part cannot be recorded.
The page with the tree view. If you click the root node, the tree items expand.	The operations to the tree view cannot be recorded.
The page is generated by the script that is executed when <code>onload</code> event occurs. For example, the script sets the items in the pull-down menu.	The operations to the updated part by the script using <code>onload</code> event cannot be recorded.

17. If the script is executed by the users' operation and changes the information of the operated tag, the operations in that page cannot be recorded and replayed correctly. The following table shows the examples of the pages and problems.

Example of the pages	Example of the problems
The page with the tree view. If you click the inner text [+] (representing the collapsed status), the trees expand and the inner text change itself into [-] (representing the expanded status).	The recorded inner text of the operation target tags is [-], which is the inner text after the user click it. The error <code>KAVK38752-E</code> occurs when replaying operations.

18. If the scripts that uses the `onblur` and `onkeyup` attributes in the HTML tags changes the page status, the operations in the pages with these kinds of the scripts are not replayed correctly. The following table shows the example of the pages:

Example of the pages
When the user enters texts in the text area, the buttons or the check boxes in the page turns activated/deactivated.

19. The page that opens a new window (or a new tab) by HTML operations or Browser operations may display a blank page (with its title blank and nothing in the IE window). Because a blank page does not affect recording and replaying, there is no problem if you continue your operation.
20. If you reset the entered contents in the form as described below, the operations in that page may not be recorded.

Example of operations to reset the data in the form
<i>Click the button created by the <code><input type="reset"...></code> tag.</i>
After executing the operations by the user, <code>document.forms.reset()</code> of the JavaScript is executed.

If you perform this kind of operations, the following problem may occur:

Example of the problem
After resetting the form, the operations such as clicking operation in that page cannot be recorded.

21. In the page that is updated by `location.reload()` of the JavaScript, the HTML operations cannot be recorded after the page is updated by the method. If you record the operations in the above page, the following problem occurs while recording:

Example of the problem when recording
The operations such as clicking operation in that Web page cannot be recorded.

If you replay the IE scenario a part of whose operations are not recorded, the following problem may occur:

Example of problem when replaying the IE scenario with a part of its operations not recorded
<i>The operations in the updated Web page cannot be replayed.</i>
When replaying the next operation to the operation updating the page, the following error messages are displayed: KAVK38752-E There is no tag that will be operated on specified position. KAVK38753-E There is no tag that will be operated. KAVK38754-E There is no frame that will be operated. KAVK38755-E There is no tab that will be operated. KAVK38756-E A popup dialog box which is not recorded while replaying the IE scenario appears.

22. If you record and replay the operations to execute the script that generates `onclick` events such as `click()` of the JavaScript, the following problems may occur:

Example of symptoms
<i>If you click once, the operations to click the multiple tags are recorded.</i>
<i>If you click the button that selects all check boxes, the operation to click the <code>input</code> tag that is automatically checked is recorded.</i>
If the operations recorded as clicking the multiple tags by clicking once are replayed, the following error messages are displayed and the operations cannot be replayed: KAVK38752-E There is no tag that will be operated on specified position. KAVK38753-E There is no tag that will be operated. KAVK38754-E There is no frame that will be operated. KAVK38755-E There is no tab that will be operated. KAVK38756-E A popup dialog box which is not recorded while replaying the IE scenario appears.

In this case, by deleting the operations that are not performed by the user from the Operation list, the operations may be replayed. For details about how to handle, see the next note (No. 23).

23. The following describes how to handle the problem when the operations that are recorded as clicking the multiple tags by clicking once are replayed.

(i) Back up the IE scenario file.

(ii) From the **Operation list** in the **IE Recorder (main)** window, delete the other operations than the ones that are performed by the user from the multiple recorded operations.^{#1}

(iii) Check whether the IE scenario can be replayed correctly.

#1

The recording order of the operations is uncertain due to the behavior of the scripts. As a result, the recording positions of the user operation among the recorded operations are uncertain. Therefore, if you delete the operations by the procedure 2 but the IE scenario cannot be replayed correctly, by deleting the other operations the IE scenario may be replayed correctly.

Note:

The operations to select the `<SELECT>` tags can be replayed correctly only when the operations to select and the `<OPTION>` tags are recorded at the same time. If the multiple operations (the operations to select and the `<OPTION>` tags) followed by the `<SELECT>` tags are recorded at the same time, you do not need to edit the **Operation list**.

24. You cannot access by using the IE Recorder to the pages that use the functionality of the Adobe Reader. You cannot measure the IE scenarios recorded the operations in these pages using by the IE probe.

For example, do not perform the operations to the pages that use PDF (Adobe Reader) as the plugin in the HTML documents.

25. You cannot record or replay operations for a Web site for which the completion of a Web page transition cannot be detected.

For example, this note applies to the following Web page.

Web page example	HTML example
A page on which a JavaScript page transition occurs automatically before the entire HTML page is loaded	<pre><html> <body> <form name="form1" action="next.html"> <script> document.form1.submit(); </script> </form> </body> </html></pre>

26. You cannot record or replay IE scenarios for a Web site that uses a security dialog box for authentication.

27. You cannot use IE scenarios for operations using the file download dialog box.

When you record IE scenarios, do not record operations using the file download dialog box.

28. If the last operation recorded in an IE scenario involves displaying a dialog box (to close its own window, for example), the attempt to execute measurement might fail when replaying the IE scenario.

In such a case, add one more operation (such as moving to another page by entering an address) after the last operation in the IE scenario.

29. When you use the `window.showModalDialog` method to specify HTML and create a modal dialog box, operations such as button clicks on the dialog box cannot be recorded or replayed.

30. If you have updated Internet Explorer, you may not be able to replay IE scenarios that were created before the update. For example, if the dialog box titles displayed in `window.confirm` and `window.alert`, etc. are changed in the Internet Explorer specifications, an IE scenario replay error may occur after updating Internet Explorer. If this occurs, recreate the IE scenario.

31. If a Web page does not support screen sizes of about 200 to 300 dots (260 x 200) in the browser, a script error may occur and replay will not be possible.

32. For Web pages that enter cached information on the page (such as Web pages that automatically enter user IDs and other information from cache onto a login screen), such information automatically entered from cache is not recorded

when using IE Recorder. Therefore, the subsequent operations may be different from during replay, and replay may not be possible.

33. If you used an IE probe started from a Windows service to measure a Web page that maintains data on the client side in `window.localStorage`, the operation in Windows may result in a script error. If a script error occurs, measurement is not possible.
34. If Internet Explorer Enhanced Security Configuration is enabled on the host for PFM - Agent for Service Response, the measurement results for the IE probe may be result code 6 (IE SCENARIO REPLAY ERROR) when the monitoring target Web page uses a script or ActiveX control, even if replay is successful in IE Recorder, and measurement may not be possible.

If this happens, check the Web sites in **Trusted sites** and **Local intranet**, and add the following items so that measurement with an IE probe will be possible.

- If `about:security_jpcvIERec.exe` has been added to the Web site
Check if `about:security_jpcvieprobed.exe` has also been added. If not, add it.
- If `about:security_jpcvIERec.exe` has not been added to the Web site
Check that `about:security_jpcvieprobed.exe` has also not been added to the Web site. If it has been added, delete it.

(4) Notes on the operations in the IE Recorder

1. Do not use the shortcut keys in the Internet Explorer (the system controls the shortcut keys not to take effects, but part of the shortcut keys may take effect). Since the operations using the shortcut keys in the Internet Explorer are not recorded, the operations may not be replayed correctly. For details about the shortcut keys in the Internet Explorer, see your Internet Explorer documentation.

2. Use the mouse instead of the keyboard to operate in the displayed HTML page. For example, if you click the **Submit** button in the survey form using the keyboard, the button operation may not be recorded.

The operations to enter texts are not recorded until the following operations are performed:

- Move focus from the text box to other materials.
- Click the button

If you record and replay the operation in the above page by using the IE Recorder or the IE probe, the following malfunctions may occur.

- The operation to click the **Submit** button is not replayed.
 - The part of operations to enter texts in the form with the text boxes is not replayed.
3. The operations to move the mouse are not recorded. For example, if you display the submenu by moving the mouse (not clicking) and select an item from the submenu, the operation to display the submenu is not replayed correctly because that operation is not recorded. If you record and replay the operation in the above page by using the IE Recorder or the IE probe, the following malfunctions may occur:
 - If the page matches all the following conditions, the operations in the page cannot be replayed correctly (script errors occur or replaying is suspended).
 - (i) The operation for the mouse to move over tags is recorded by JavaScript.
 - (ii) JavaScript receives the mouse click event, and operates based on the recorded operations by (i).
 - The visual effects or the operations to the submenus that are changed by moving the mouse cursor cannot be replayed.
 4. You cannot specify and change the character set to display the HTML page in the IE Recorder. If the page is displayed incorrectly (a happenstance of incorrect and unreadable characters occurs), check whether the character set specified in the target HTML page is correct.

5. In the IE Recorder, you can display the HTML source code of the Web pages that forbid to be displayed their HTML source code.
6. In the IE Recorder, from **View** menu, choose **Source**, and the source code is displayed encoded in the UTF-8 encoding format.
7. Store the IE scenario files to the default folder (*installation-folder\agtv\probe\iescena*). If you store the IE scenario file to the other folders without the *iescena.dtd* file, the error occurs. If you store the IE scenario files to the other folders, copy the *iescena.dtd* to the destination folders in advance.
8. If replaying is suspended while replaying the Navigate operation or the different Web site is displayed from the one when recording, you may replay the operations by deleting the Navigate operation.

The following describes an example that you delete the Navigation operation and then the operations can be replayed correctly.

Example:

If you click the tag in the following HTML page, the IE Recorder catches and record the Navigate operation (a page transition) and click operation in this order. As a result, the recorded order of the operations is different from the actual order of the operations. When you replay the operations in the recorded order, the operations cannot be replayed correctly. In order to replay correctly, you must delete the Navigate operation.

```
function funcl() {
    Processing to perform the page transition
}
<a onclick="return javascript:funcl()"href="#">
```

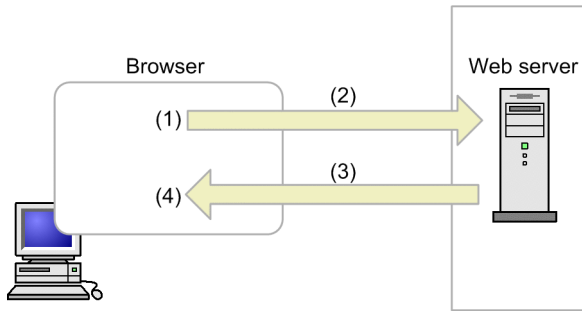
9. Since the sessions of the browser are disconnected whenever you create, start to record, or replay IE scenarios in the IE Recorder, you must respond, if necessary, to the **Authentication** dialog box every time you create, start to record, or replay IE scenarios.
10. Type the characters in a text box to enter text. For example, if you enter texts using the accessibility feature by the script, the operations to enter texts cannot be recorded correctly. Yet, the operations using the AutoComplete feature that does not enter texts is recorded correctly.
11. If you use the IE Recorder to operate in the pages that check whether the visitor uses the Internet Explorer, the page judges that the browser you use is other than the Internet Explorer. You do not use the IE recorder to operate in the pages that returns errors if the visitor uses the browser other than the Internet Explorer. Note that if the scripts use `navigator.appName` to identify the browser, the scripts judge the browser to be the Internet Explorer. In this case, this note is not applicable.
12. If you use the IE Recorder to operate in the pages that close the window using the script, the tabs with the blank pages may remain unclosed in the IE Recorder (main) window. If the tabs with the blank pages remain activated, select the tab that is otherwise activated in the IE Recorder. Note that the remained tabs do not affect the IE Recorder operations. If you select the tabs with the blank pages, the IE Recorder automatically hides that tab.
13. The replay time of the operations between the operation to generate a new window and the operation previous to the Navigate operation includes the time for generating the new window when measuring the IE scenario.
14. Do not navigate the page in the IE Recorder or operate the tags in the Internet Explorer window. If you do, the following malfunction may occur:
 - When the next operation is replayed, an error occurs such as there is no tag that will be operated (KAVK38752-E) and replaying is suspended.
15. Do not specify response determination for navigation in the Operation list for IE scenarios. Even if you specify, response determination will not be detected.

The response determination function supports only the operations performed by the user to issue the page transition #. And then, it does not support the pages to be not replayed and to be not complete navigation.

#

In an IE scenario, the page transition means that the requests are sent to the server from the browser by operations on the browser, the responses are received and the pages on the browser are update.

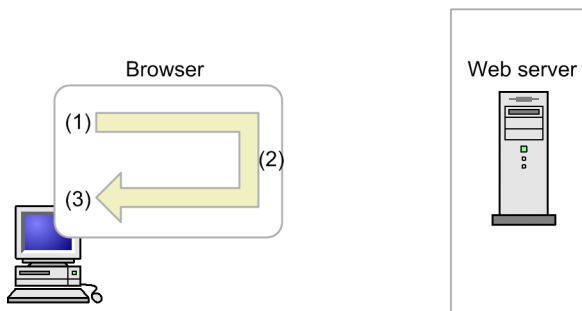
When the page transition is issued, flow to update the pages on the browser



- (1) Operating on the browser
- (2) Request is send to the Web server from the browser.
- (3) Response from the Web server
- (4) Update the pages on the browser completes

The update pages on the browser without the page transition means that by operations on the browser, no request is send to the server from the browser and the pages on the browser are re-displayed.

When the page transition is not issued, flow to update the pages on the browser



- (1) Operating on the browser
- (2) Update pages on the browser without requests to the server
- (3) Update the pages on the browser completes

(5) Notes on starting and stopping the IE probe from the Windows services

1. If you do not set `Y` in the `ie_service_flag` in the [General] section of the Probe action condition definition file, you cannot start the IE Probe Daemon service from Windows services. To start the IE Probe Daemon service, from Windows **Start** menu, choose **All Programs, Performance Management, Agent Option for Service Response**, and then **IE Probe**.
2. If you set `Y` in the `ie_service_flag` in the [General] section of the Probe action condition definition, you cannot start the IE Probe Daemon service by selecting Windows **Start** menu, **All Programs, Performance Management, Agent Option for Service Response**, and then **IE Probe**.
3. If you measure IE scenarios, use the log-on account for the Extensible Service IE Probe service to record IE scenarios and check in advance whether the IE scenarios is replayed correctly before you measure the IE scenarios.
If the account for measurement is different from the log-on account for the Extensible Service IE Probe service, the error such as `KAVK38756-E` may occur when replaying the IE scenarios.

4. If you measure the IE scenarios created before upgrading PFM - Agent for Service Response, use the log-on account for the Extensible Service IE Probe service and the IE Recorder to check in advance whether the IE scenario is replayed correctly before you measure the IE scenarios.

(6) Notes on the operation

1. Do not use the Internet Explorer while the IE Recorder and the IE probe are running. If the Internet Explorer is running, the IE Recorder and IE probe may not operate correctly. If you operate in the HTML pages that move the focus to the already opened Internet Explorer, the IE Recorder or the IE probe do not operate correctly. If you use the Internet Explorer, make sure in advance to stop the IE Recorder and the IE probe.
2. If you display the real-time report of the `PL_IESM` records on the multiple PFM - Web Consoles at the same time, not all the differentials based on the last display are displayed. When you check the `PL_IESM` records, display the historical report.
3. If you use the IE probe to measure the IE scenarios, the dialogs displayed while measuring the IE scenarios appear on the actual display. Yet, since the IE probe automatically replays the recorded operations, these dialog boxes immediately disappear. Hitachi recommends that in order to avoid manually operating the displayed dialog boxes you refrain from using the machine to perform manual operation.
4. If navigation errors occur while recording or replaying the operations, recording or replaying the operations is suspended. Yet, the Internet Explorer allows the pages to ignore the navigation errors and continue their services. As a result, there are pages where you do not notice the navigation errors when using the Internet Explorer. You need to make sure in advance that the navigation errors do not occur, before planning to monitor the performance of the Web sites (check whether the HTTP error status codes are output to the Web server logs).
5. Assume that you connect the sites that store the connection information in the Cookie or the Web server. If you disconnect the sites improperly (the session is disconnected) and reconnect these sites, the different pages appears or the connection is disconnected. When you monitor these Web sites and, for example, the measurement is suspended due to the timeout, the measurement of the following operations fails. When the measurement fails, remove the causes of failure according to the specifications of these Web sites.
6. You can increase the measurement accuracy if you need a measurement independent of the cache status of Internet Explorer. To do so, select **Tools**, and then **Internet Options**. Then, in the Internet Options window, on the **General** page, click the **Settings** button under **Browsing history**. In the **Temporary Internet Files and History Settings** window that opens, select the following item:
Every time I visit the webpage
7. If the target Web site prevents multiple simultaneous logins by same user and the timeout occurs while measuring the site, you may not be able to log out from the site, the logging session remains and then, the measurement fails at subsequent measurement intervals. In this case, make sure that you can log in the site before measuring. Also, adjust the measurement interval and timeout value that are defined in the measurement condition registration file (`esptask.xml`).
8. If the measurement of IE scenarios involves server authentication or client authentication, there is no need to register the certification files with PFM - Agent for Service Response. Register the certification files with Internet Explorer for the user who executes measurement.
9. In a measurement of IE scenario, the protocol to use in communication of SSL with the Web server for the monitor is chosen based on the setting of "the Internet option" of the user who carried out a record and making of IE scenario. When you do not want to use communication in SSLv3.0, invalidate it by any of the following method.
 - Method to invalidate with the Web server for the monitor
Invalidate SSLv3.0 with the Web server for the monitor.
 - Method to invalidate by setting of Internet Explorer working on the host that PFM - Agent for Service Response works

After having logged in by the user who carried out a record making of the IE scenario, choose "Advanced" tab of the "Internet Options" DIALOG. Turn off a check box of "Use SSL 3.0" in the item of Security, and turn on an "Use TLS 1.0", "Use TLS 1.1" and "Use TLS 1.2" check box instead.

5.2.4 Notes on the navigation

The `navigation` is the page transition that is recorded by the operations in the IE Recorder. If the page transition occurs when the user does not operate in the pages or the page transition occurs in no relation to the user operations, the navigation is recorded.

This section describes the recording status of the navigation, how to replay the navigation and how to handle errors.

(1) Recording status of the navigation and how to handle

The following table shows the recording status of the navigation and how to handle the problems.

You may solve the problems if you handle these problems as the following table explains, but not all the problem can be solved. Also, since the multiple causes may lead to the problems, you may solve the problems by combining the proposed solutions in the following table.

Note that you back up the IE scenario in advance before you edit the **Operation list**. For details about how to back up the IE scenario, see [3.5.1 Backup](#).

Table 5–5: Recording status of the navigation and how to handle

No.	Recording status after operation	Recording status	How to handle ^{#1}	Reference
1	The input operation is not recorded, only the navigation is recorded.	The operations in the ActiveX control (such as Flash), the Java Applet, or the script's own window (such as the operations in the window created by <code>createPopup</code>) cannot be recorded. But since the page transition occurs by these operations, only the navigation is recorded. ^{#2}	Specify the Wait time in the Operation Settings window.	(a)
		The IE Recorder sometimes may not be able to catch the input operations while the page transition occurs. But since the page transition is recorded, only the navigation is recorded.	Re-execute to record.	(b)
		If you record the Web sites that perform page transitions automatically by using timers, only the navigation is recorded because the page transitions occur without the input operations.	Specify the Wait time in the Operation Settings window.	(c)
2	The input operation is recorded, and then the navigation is recorded.	If the multiple page transitions occur (such as when some of its frame pages are displayed after the Web page is completely displayed), the second and later transitions are recorded as the navigation.	Delete the operation.	(d)
		When the multiple page transitions occur, before the page transition to the operation target page occurs, the early page transitions		(e)

No.	Recording status after operation	Recording status	How to handle ^{#1}	Reference
2	The input operation is recorded, and then the navigation is recorded.	are interrupted and the next page transitions occur. In this case, the second or later page transitions are recorded as the navigation.	Delete the operation.	(e)
		If the frame page transition occurs in parallel with another frame page transition (such as when the frame page transition occurs in parallel with the page transition of the frame page where you perform a click operation), the navigation is recorded without detecting the page transitions' completion.	<ul style="list-style-type: none"> Delete the operation. For the next operation, specify the Wait time in the Operation Settings window. 	(f)
3	The navigation is recorded, and then the input operation is recorded.	If the script in the Web page catches the input operations earlier than the IE Recorder, the page transitions occur immediately and the navigation is recorded just before the input operations.	Delete the operation.	(g)

#1

For details about how to handle, see Table 5-6.

#2

Usually for the operations in the ActiveX control, the Java Applet, and the scripts' own window, only the navigations are recorded by the page transitions to occur. Note that the solutions described in the Table 4-6 are to replay the recorded navigations correctly, not to record the operations correctly.

Table 5–6: How to handle the navigations

Type	How to handle
Specify the wait time for operations	In the Operation Settings window, change the wait time for the operation, if necessary, to adjust the time to complete the page transition. You may replay correctly without adjusting the wait time, but when you monitor the pages that refreshes themselves every certain seconds or minutes, navigation errors occur and replaying is suspended because the page transitions forcedly occur due to the unmatched wait time. In this case, you may be able to replay the operations correctly if you increase the wait time.
Re-record	Delete the navigation with a problem and the subsequent operations, and then re-record the operations.
Delete the operation	If the replaying stops at the navigation or a replay error occurs when replaying, delete the navigate operation.
Specify the wait time for the next operation	If an error occurs when replaying the operation next to the navigation operation, customize the wait time for the next operation in the Operation Settings window to adjust the timing of the page transition so that the operations may be replayed correctly. [#]

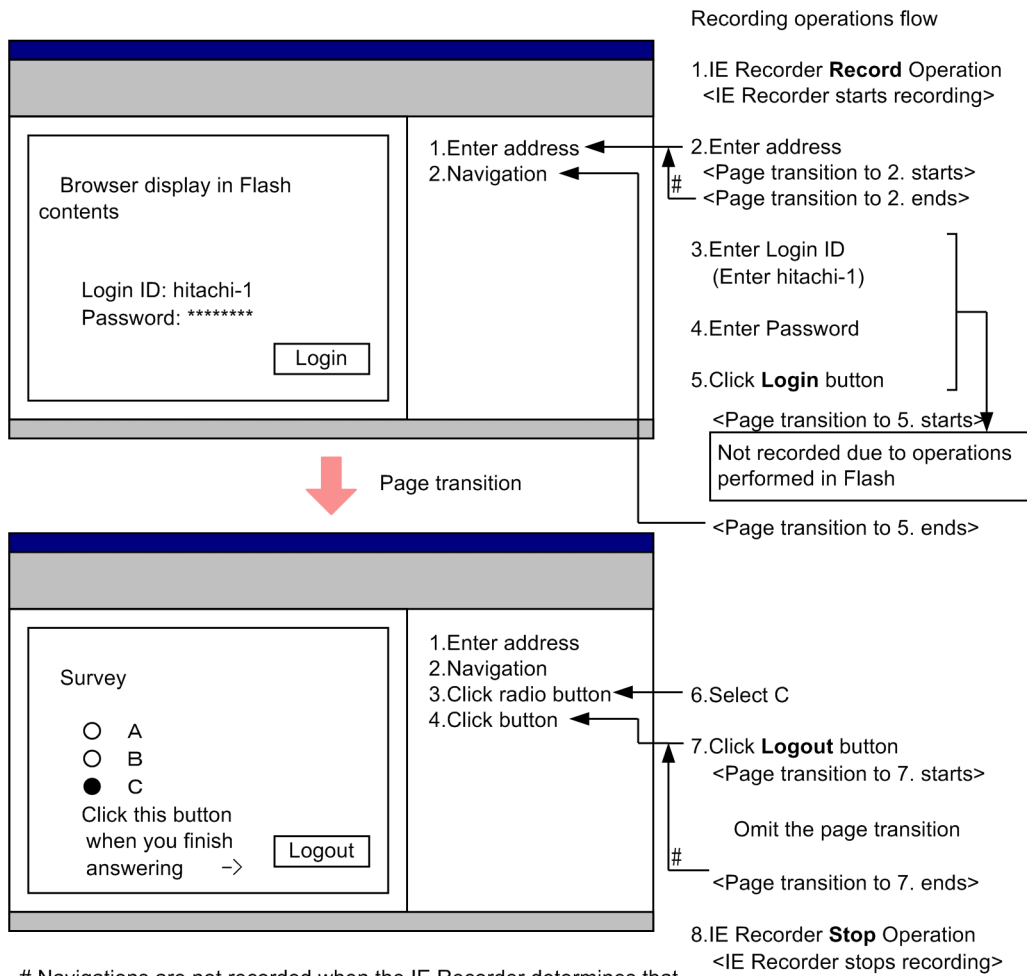
#

When the **Wait to replay** check box is specified in the **Operation Settings** window, the operation waits for the time specified in the **Wait time** to pass.

Since the navigation is performed forcedly after the time specified in the **Wait time** passes, errors may occur when replaying the subsequent operations. The error contents vary depending on the contents of the IE scenario and the monitoring target page. For example, the following errors occur: There is no tag that will be operated., A popup dialog box which is not recorded while replaying the IE scenario appears., or There is no tag that will be operated on specified position. (such as KAVK38753-E, KAVK38756-E, or KAVK38752-E).

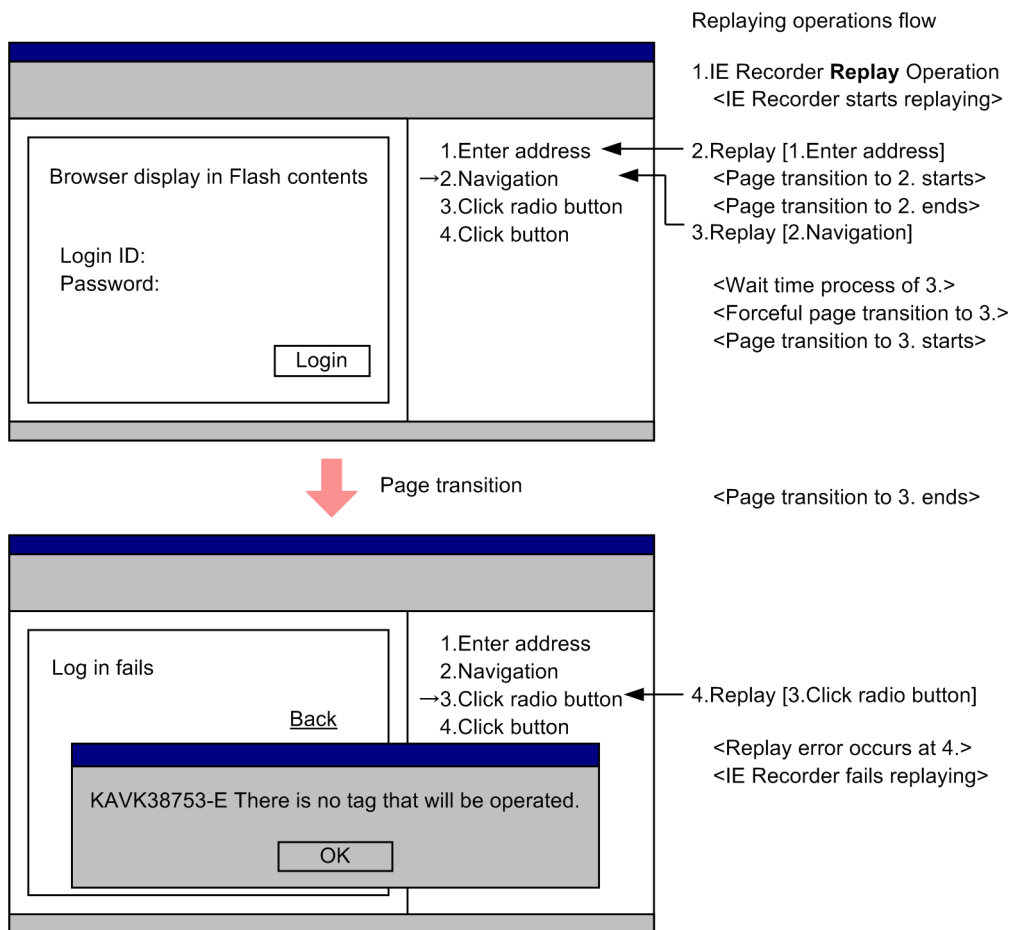
(a) When the operations in Flash are not recorded and only the navigations are recorded (unmanageable)

Figure 5–5: Recording example of the page using Flash



Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

Figure 5–6: Replaying example of the page using Flash



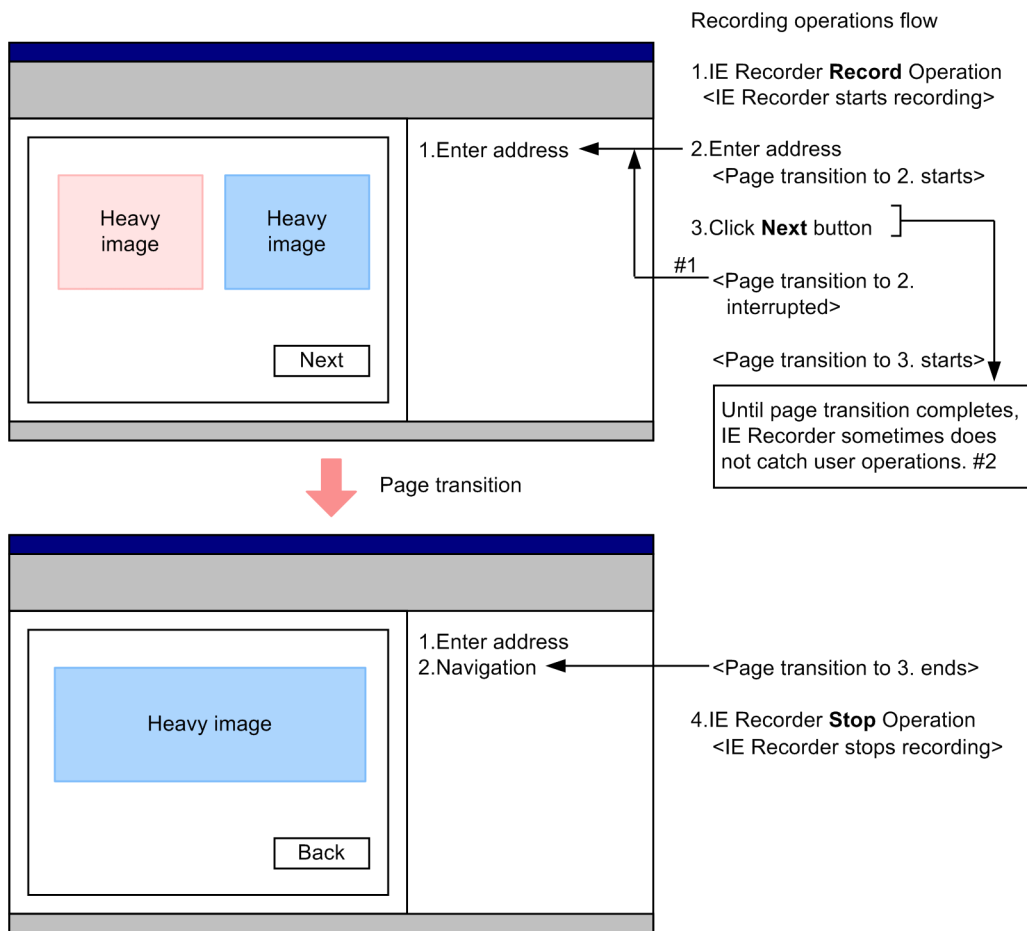
Commentary:

The operations in the Flash are not recorded as the [2. Navigation], but the page transition in no relation to the user operations is detected and recorded as the [2. Navigation].

<Replay error occurs at 4.> occurs frequently when the recorded URL of [2. Navigation] is dynamic.

(b) When the click operation is performed during the page transition, the click operation is not recorded but the navigation is recorded

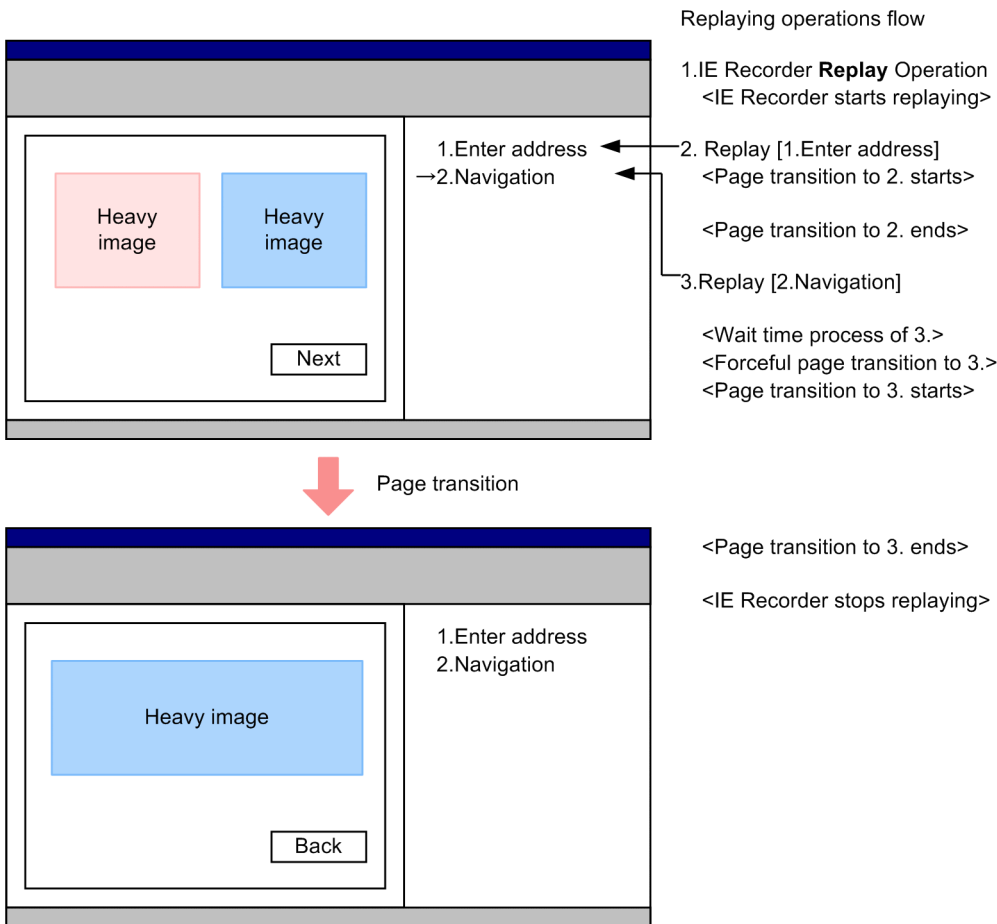
Figure 5–7: Recording example of the page that takes time to display



#1 Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

#2 Until page transition complete mouse input and key input are not caught, but sometimes these inputs are caught.

Figure 5–8: Replaying example of the page that takes time to display



Commentary:

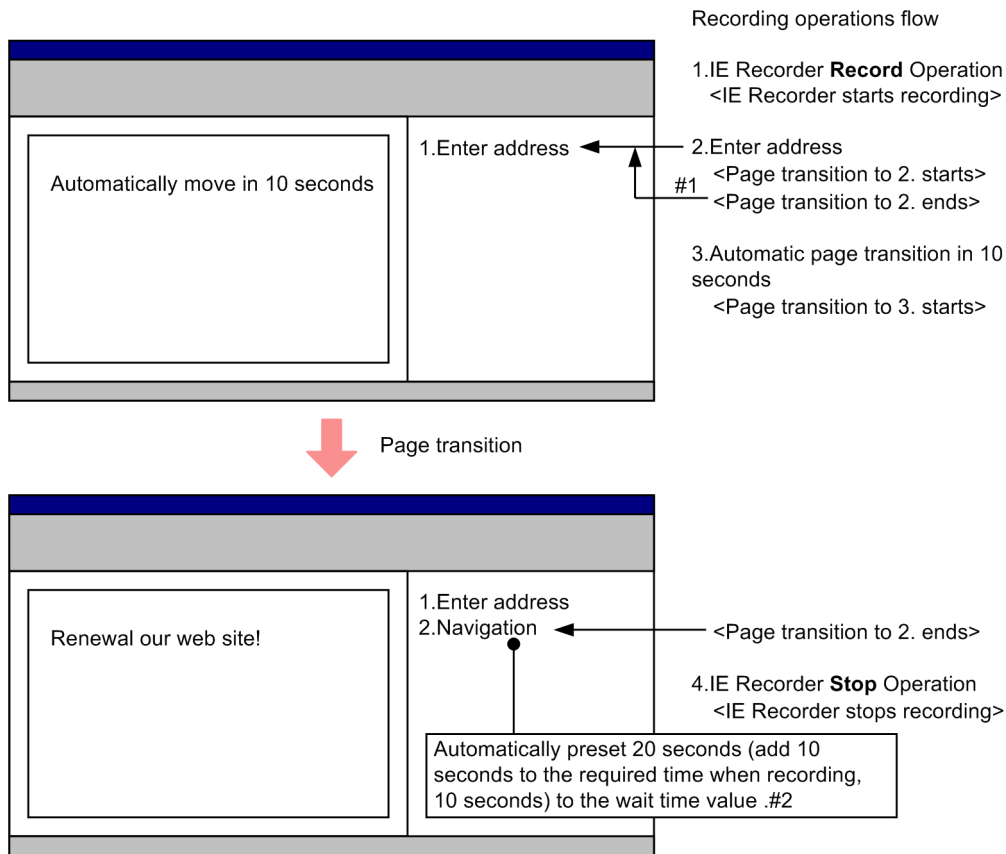
If the page displays the many large images or the multiple frames that take time to display at the same time, the IE Recorder may record only the navigation without catching the user operations when the timing is off.

The [2. Navigation] of the above example is assumed to be recorded when the timing is off.

When replaying [2. Navigation], waits for the time specified in <Wait time process of 3.> to pass and then the page transition to the recorded URL occurs (<Forceful page transition to 3.>). The example above is assumed to be a page transition to the static URL. As a result, although the click operation is not recorded, the target page is displayed. Yet, to correct the recording content, delete [2. Navigation] and re-record the operation of clicking the button in the IE scenario.

(c) The page transition occurs automatically after 10 seconds when recording, but when replaying the page transition occurs automatically after 30 seconds

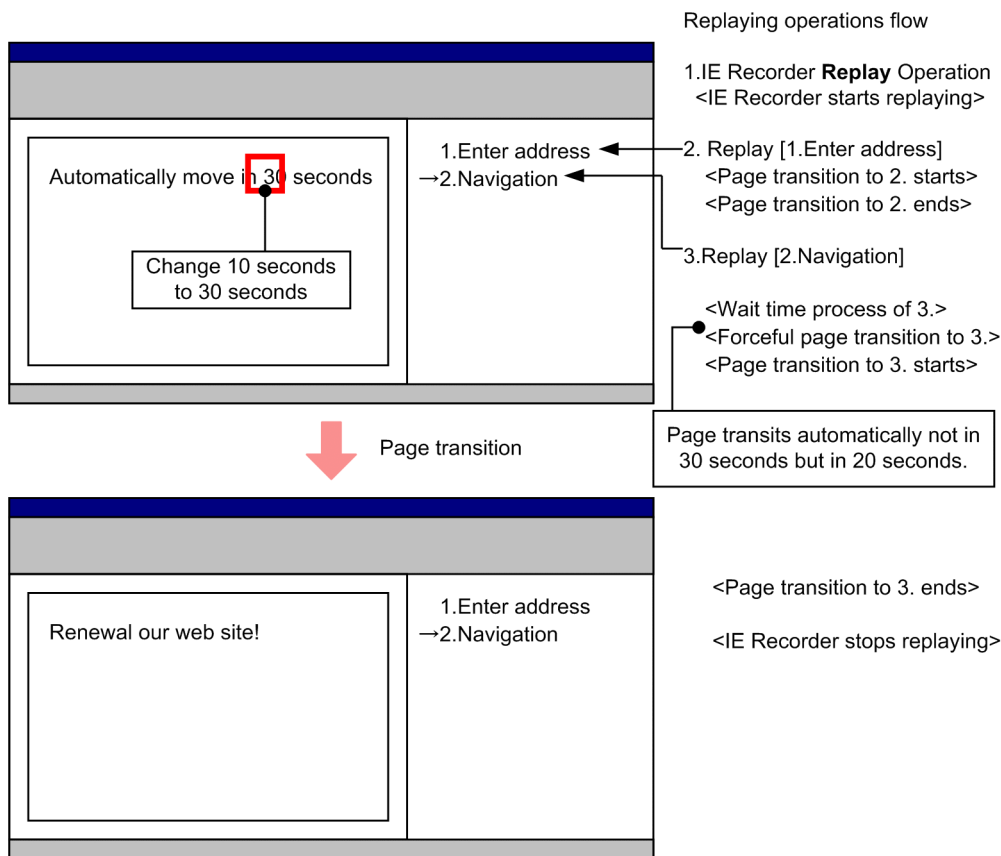
Figure 5–9: Recording example of the page transition after a certain amount of time



#1 Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

#2 IE Recorder automatically preset the calculated value (add 10 seconds to the required time when recording) to the wait time value.

Figure 5–10: Replaying example of the page transition after a certain amount of time



Commentary:

If you record the page that transits automatically to the target page by REFRESH parameter of the META tag, the automatic page transition is recorded as the navigation ([2. Navigation] (The wait time is set to 20 seconds when recording.)).

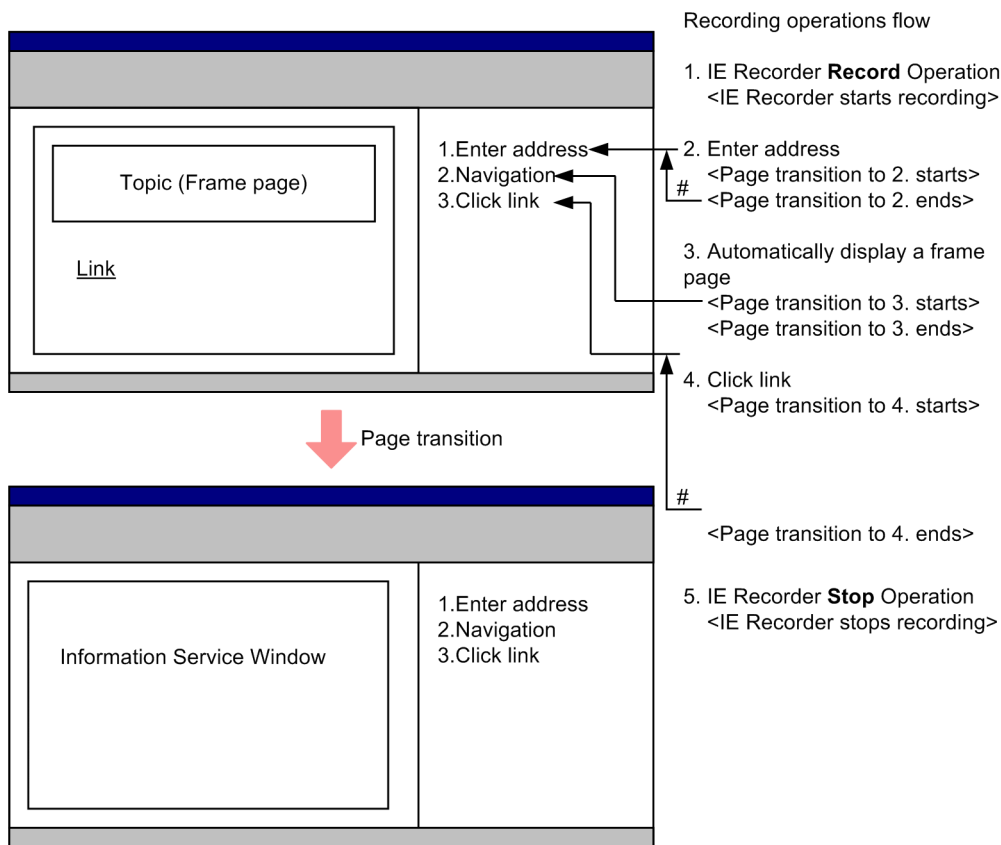
If the page setting of the elapsed time is not changed, the operations are replayed correctly. If the page setting of the elapsed time is changed longer than recorded time (change 10 seconds to 30 seconds), the page transition to the recorded URL is performed forcibly (<Forceful page transition to 3.>) because the page transition does not occur after 20 seconds pass at <Wait time process of 3.> after 3.Replay [2.Navigation].

Therefore, you may not measure the actual response time because the page transition forcibly occurs earlier than the page anticipates.

You can measure the anticipated response time if you specify longer than 30 seconds (such as 40 seconds) as the **Wait time** in the **Operation Settings** window on the IE Recorder.

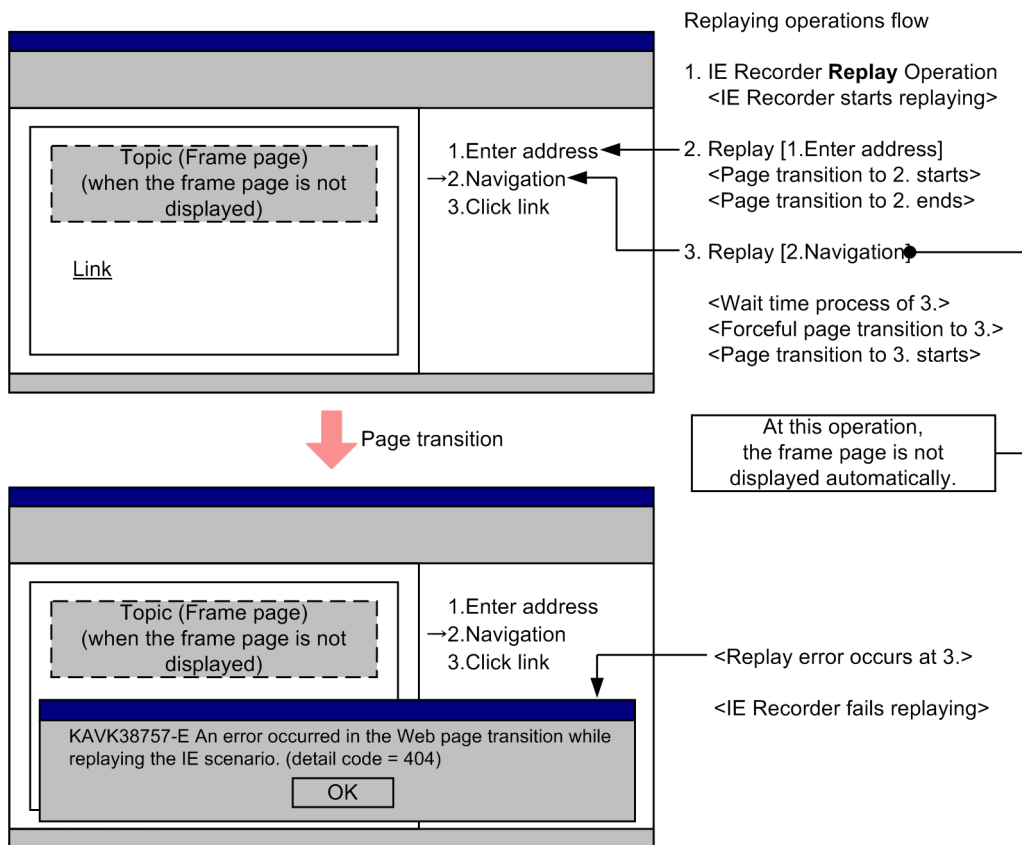
(d) Although the frame page is displayed when recording, the frame page is not displayed when replaying

Figure 5–11: Recording example of the page transition after a certain amount of time



Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

Figure 5–12: Replaying example of the page transition after a certain amount of time



Commentary:

The frame page may be displayed after the Web page transitions complete. The frames page displayed is detected as the page transition but since its transition occurs separately from the Web page transitions it is recorded as the navigation ([2.Navigation]).

This case assumes that the frames page may not be displayed depending on the situations.

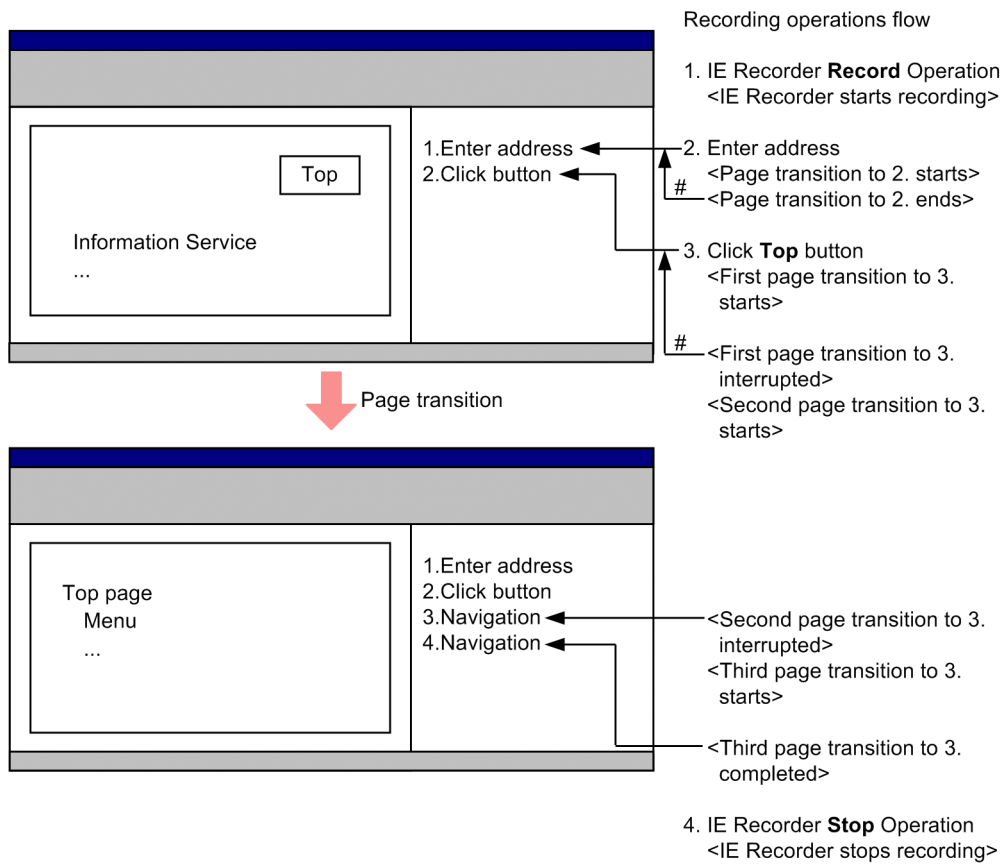
If you replay the IE scenario when the frame page is not displayed, the page forcedly transits to the recorded URL (<Forceful page transition to 3.>) because the page transition does not occur when replaying the navigation.

The example above assumes that the URLs are dynamic, and as a result a navigation error occurs.

If you do not operate in the frame page, you do not have to wait for the frame page to complete displaying. In this case, delete [2.Navigation] and you can replay the IE scenario, not concerned about the frame pages.

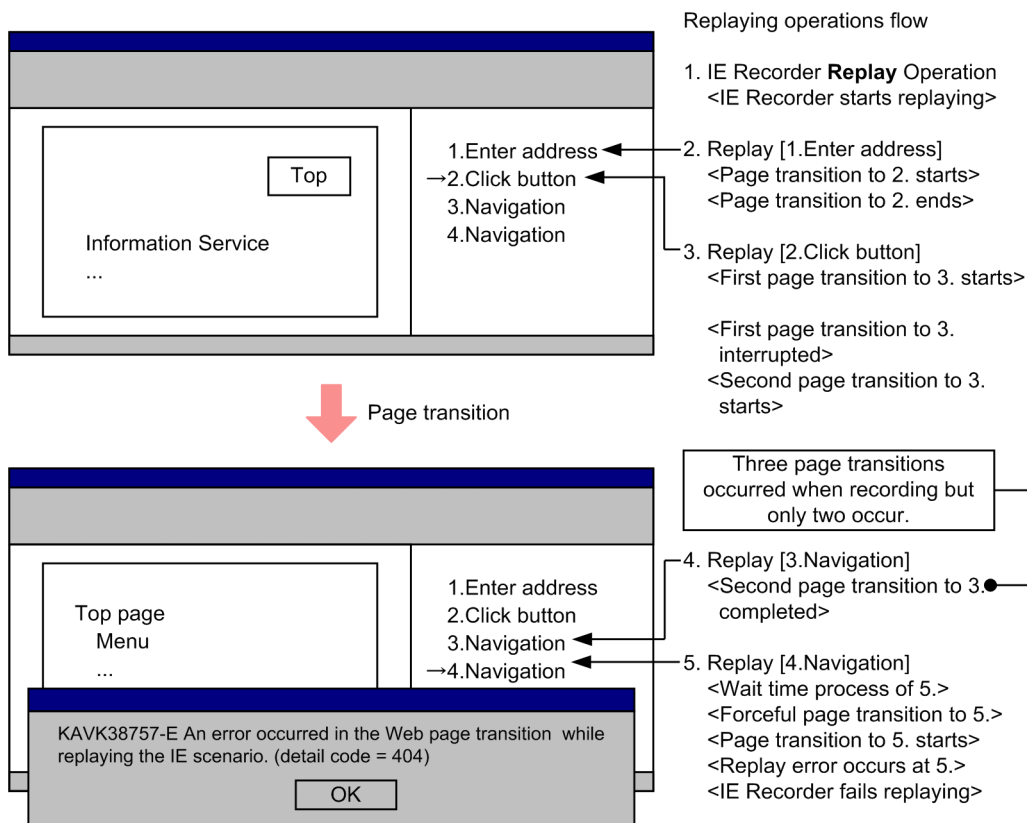
(e) Although the page transitions are interrupted twice after clicking the link to move to the target page when recording, the page transition interrupted once to move to the target page due to the change of the Web system

Figure 5–13: Recording example of the interrupted page transitions



Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

Figure 5–14: Replaying example of the interrupted page transitions



Commentary:

If [2.Click button] is performed and the target Web page is displayed in the third transition after the two interrupted page transitions, the interrupted page transitions are treated as one navigation. The first page transition is not recorded in relation to the [2.Click button], but the second and the third page transitions are recorded as two separate navigations.

This case assumes that the count of the interrupted page transitions decreases by one due to the Web system maintenance or so.

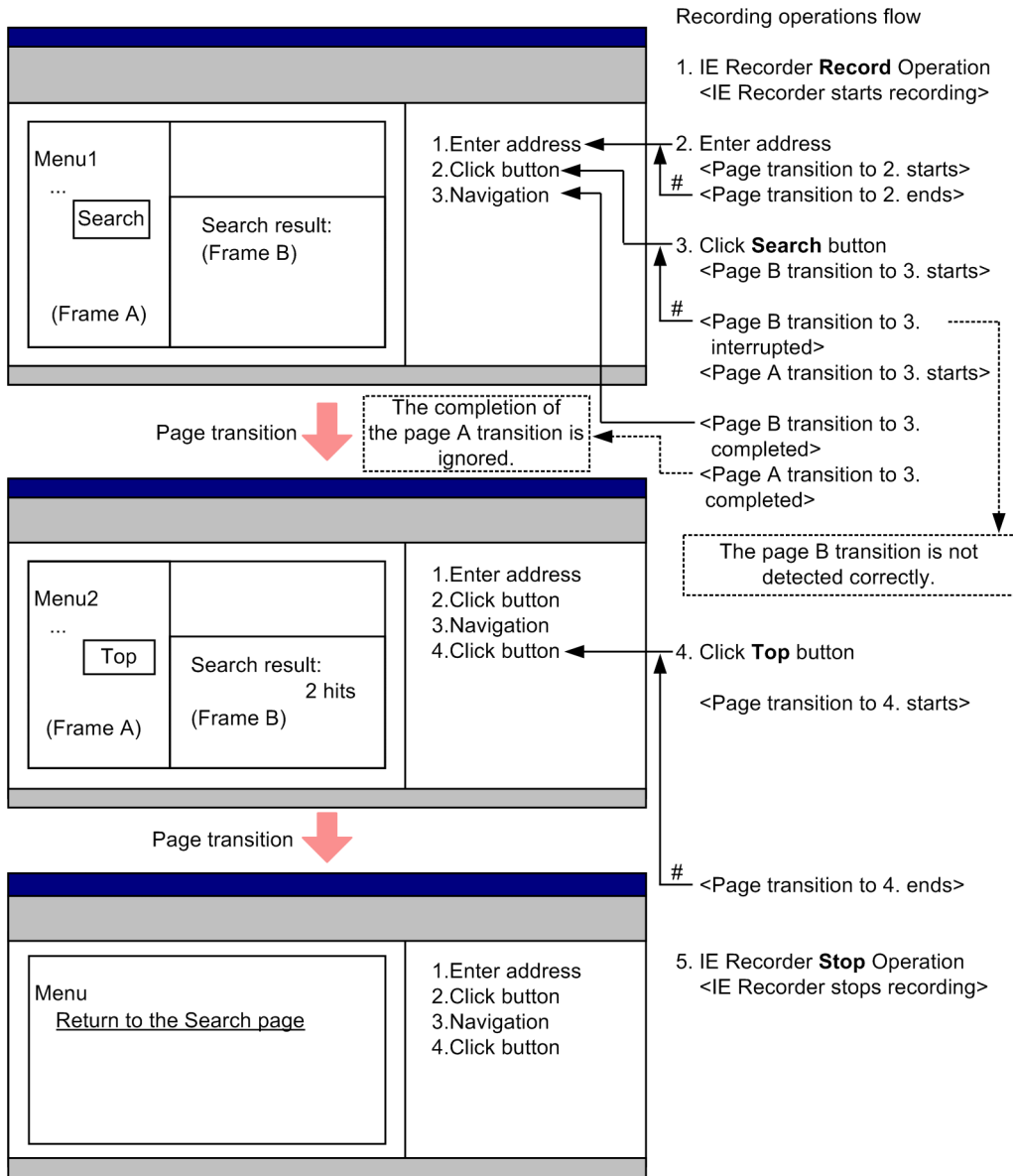
When replaying, since the page transition corresponding to 5.Replay [4.Navigation] does not occur, the page transition to the recorded URL is performed forcibly (<Forceful page transition to 5.>).

This example assumes that the URLs are dynamic and the navigation errors occur.

If the count of the page transitions decreases due to the Web system maintenance, delete either [3.Navigation] or [4.Navigation] and you may be able to replay the IE scenario correctly (i.e. you do not have to re-record the IE scenario to handle this problem).

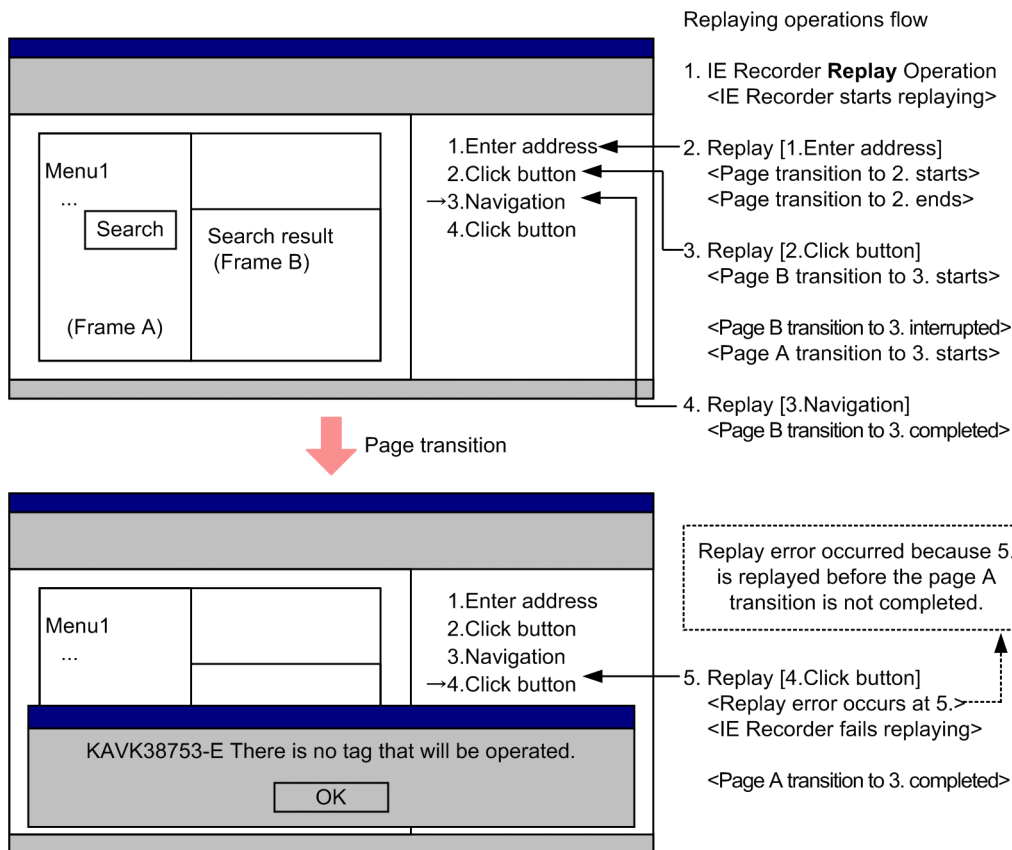
(f) When recording and replaying the Web page in which the page transitions of the menu frame and the result frame are parallel, the following message is displayed and replaying is suspended: **There is no tag that will be operated.**

Figure 5–15: Recording example of the page with two frame pages that transit in parallel with each other



Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

Figure 5–16: Replaying example of the page with two frame pages that transit in parallel with each other



Commentary:

If the search result frame (Frame B) and the menu frame (Frame A) transit in parallel with each other by [2. Click button], each page transition cannot be detected correctly. The example above assumes that the transition of the frame A cannot be detected correctly.

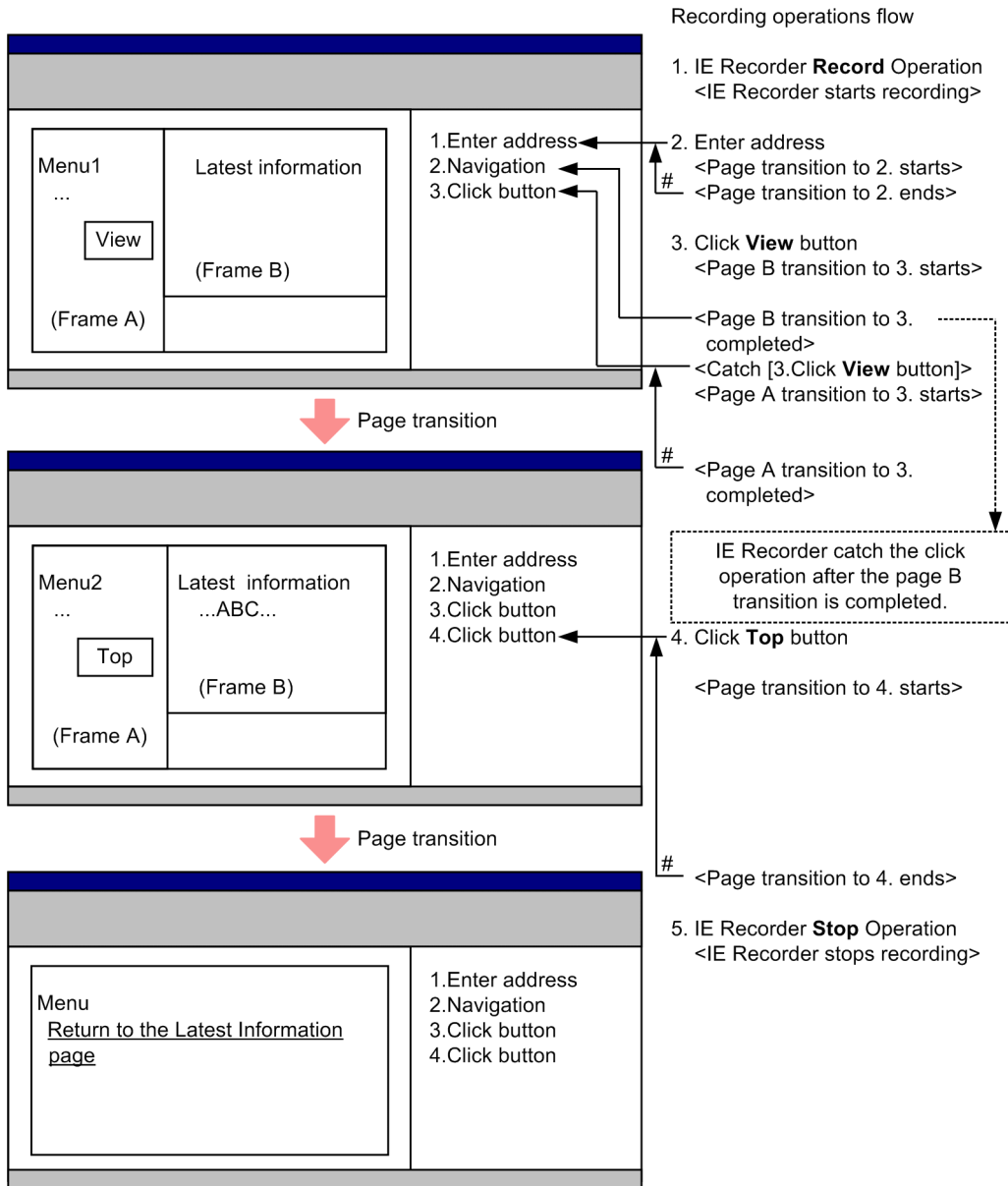
(after 3. Replay [2. Click button] is replayed) the transition of the frame B is started (<Page B transition to 3. starts>) and then the transition of the frame A is started (<Page A transition to 3. starts>), but the IE Recorder cannot distinguish each frame. As a result, the IE Recorder mistakes that the transition of the frame B is interrupted (<Page B transition to 3. interrupted>) and treat it as the termination of the page transitions.

Therefore, since the IE Recorder does not wait for the page transition of the frame A to finish and judges that all the page transitions are completed (<Page B transition to 3. completed>), the IE Recorder replays the next operation (5. Replay [4. Click button]). Yet, since the page transition of the frame A does not terminated yet, a replay error occurs.

In this case, you cannot replay the operations correctly if you delete [3. Navigation]. If you can estimate the approximate transition time of the frame A, specify the **Wait time** in the **Operation Settings** window for the operation [4. Click button] subsequent to [3. Navigation] (i.e. wait for the next operation to be performed until the page transition of the frame A terminates) so that you can replay the IE scenarios.

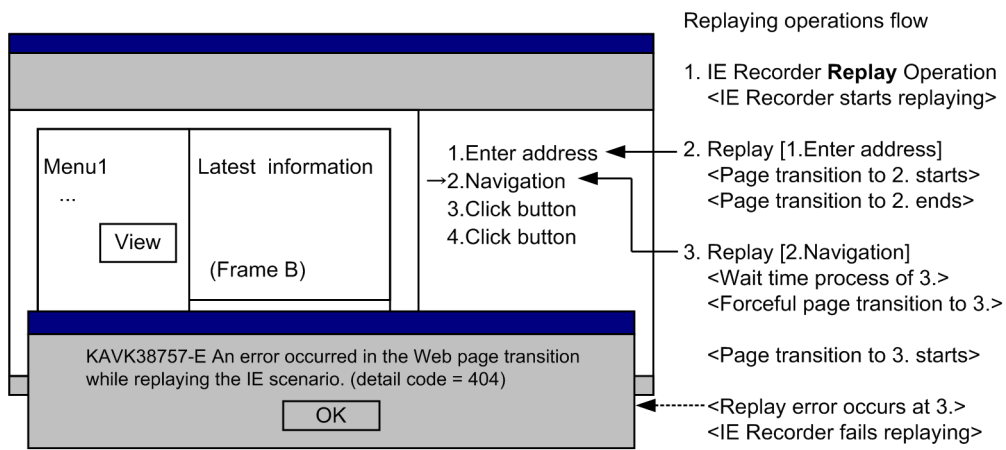
(g) After the click operation, the script catches the click event and performs the page transition forcedly before the IE Recorder catches the click event

Figure 5–17: Recording example of the page transitions earlier than the click operation



Navigations are not recorded when the IE Recorder determines that the previous operation leads to the page transition.

Figure 5–18: Replaying example of the page transitions earlier than the click operation



Commentary:

If the script catches the click operation in the Web page and transits the page immediately, the IE Recorder determines that this page transition has nothing to do with the click operation. Then, the IE Recorder records the click operation, but the operations are recorded separately because the IE Recorder cannot recognize the relationship between the previously recorded navigation and the click operation. As a result, when replaying this IE scenario, the forced page transition to the recorded URL occurs because the click operation leading to the page transition is not performed (<Forceful page transition to 3.>). This example assumes that the URLs are dynamic and the navigation errors occur.

In this case, you can replay this IE scenario if you delete [2.Navigation].

(2) Behaviors when the navigation error occurs

The navigation error occurs when the monitoring target server responds error status codes because that the requested Web page is not found or when the Web page cannot be displayed because that the monitoring target server does not start.

The following table shows the IE Recorder's and the IE probe's behavior when the navigation errors occur.

Table 5–7: IE Recorder's and IE probe's behavior when the navigation error occurs

Status when the navigation error occurs		Behavior when the navigation error occurs	Mode after the navigation error occurs
IE Recorder	Editing mode	The IE Recorder displays the error pages in the same way as the Internet Explorer.	Editing mode
	Recording Mode	The IE Recorder stops recording and displays the message dialog box (KAVK38760). The IE scenarios are saved that are recorded until the navigation error occurs.	
	Measurement Test	The IE Recorder stops replaying and displays the message dialog box (KAVK38757).	
	Recording Mode	--	
	Replay Report	The IE Recorder stops replaying and displays the replay report (KAVK38757).	
IE probe	Measuring	The IE Recorder stops replaying and outputs to the report and the PL record (Result Code 89102).	The IE Probe Daemon is waiting the measurement request from the IE Master Daemon.

(3) How to check the user operations when navigation errors occur

If navigation errors occur while you create or replay IE scenarios, check in advance whether the user operations can lead to the navigation errors. The following describes how to check the user operations:

1. Check whether the user operations lead to no errors in the Internet Explorer window.
2. If you cannot check the errors in the IE Recorder window, during the operations in the Internet Explorer check whether the error status codes of the HTTP protocol are not output to one of the following logs:
 - The communication trace between the Internet Explorer and the Web server
 - Log of the Web server

(4) How to handle the error `There is no tag that will be operated although the Web page does not change`

Follow the procedures described below if you do not change the monitoring target page but the errors occur such as `KAVK38752-E There is no tag that will be operated on specified position.` or `KAVK38753-E There is no tag that will be operated.`

1. Back up the IE scenario file.
2. Specify the **Wait time** in the **Operation Settings** window of the operation where an error occurred, and check to replay the IE scenario.

Use as a standard the time to complete the page transitions after the very operation leading to the page transitions of the multiple child frames, and specify the **Wait time**. After specifying, perform measurement tests and make sure that the IE scenarios are replayed correctly. If the IE scenarios are not replayed correctly, increase the **Wait time**.

This specified wait time is included in the replay time of the IE scenario by the IE probe or the measurement test.

Supplement:

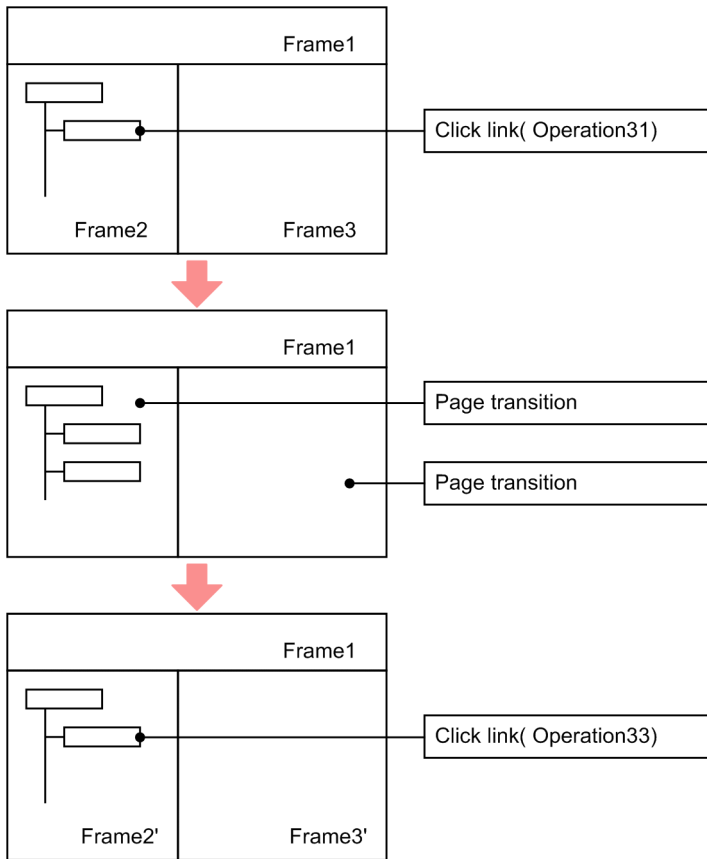
If you can replay the IE scenarios by the IE Recorder but the error above occurs when you perform the measurement test, you may be able to replay the scenarios by the above procedure:

The following shows the example that if you do not change the monitoring target page but the errors occur such as `KAVK38752-E There is no tag that will be operated on specified position.`

Example:

The IE scenario where you record the HTML operations in the transited pages after the operation for the multiple child frame transitions to occur at the same time

Figure 5–19: Example of the IE scenario that contains the operations for the page transitions of the multiple child frames to occur at the same time



Operation 31

Click the link operation (the page transitions of the frame 2 and the frame 3 occur at the same time by this operation)

Operation 32

Navigation

Operation 33

Click the link operation (the operation in the frame 2') -> The error KAVK38752-E occurs.

6

Operation in a Cluster System

This chapter describes the installation, setup, uninstallation, unsetup of PFM - Agent for Service Response in a cluster system and the operating procedures when PFM - Agent for Service Response is operated in a cluster system.

6.1 Overview of cluster systems

A cluster system links multiple server systems so that they can be operated as a single system. PFM - Agent for Service Response can be operated in the following cluster system:

- High-availability (HA) cluster system

This section describes the configuration in which PFM - Agent for Service Response is applied to a cluster system. For an overview of cluster systems and details about the system configuration for operating Performance Management in a cluster system, see the chapter that describes system construction and operations in a cluster system in the *JPI/Performance Management User's Guide*.

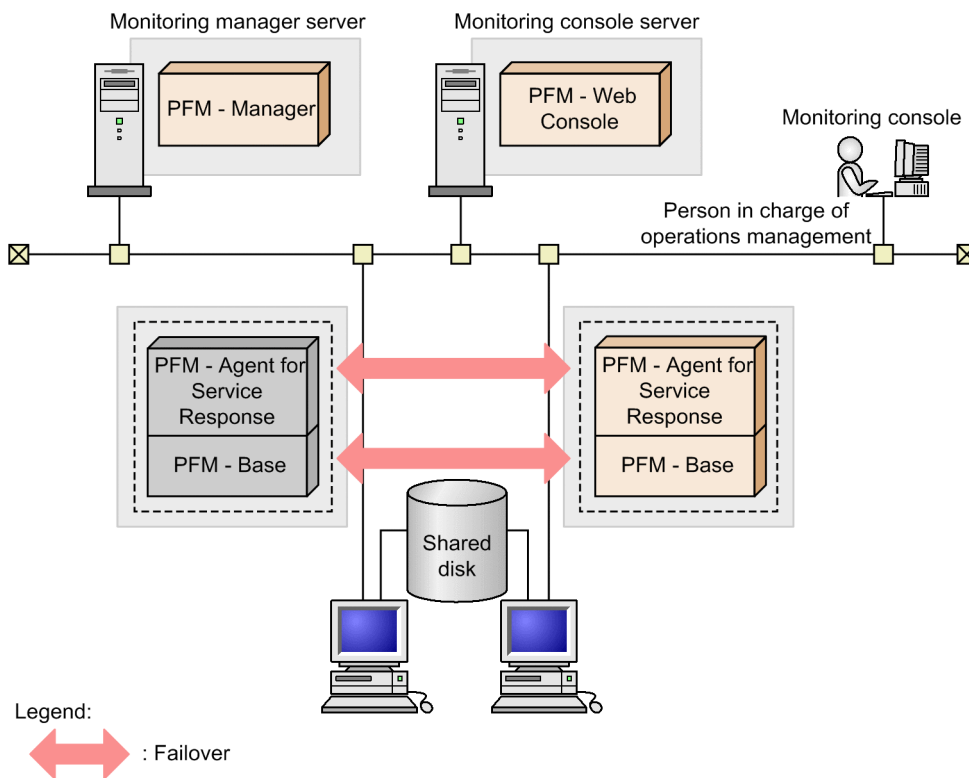
In this chapter, the term *cluster system* refers to an HA cluster system.

6.1.1 HA cluster systems

(1) Configuration of PFM - Agent for Service Response in an HA cluster system

PFM - Agent for Service Response can be operated in an HA cluster system. To do so, PFM - Agent for Service Response must be configured as shown below.

Figure 6–1: Example of configuration of PFM - Agent for Service Response in an HA cluster system



As shown in Figure 6-1, PFM - Agent for Service Response stores necessary data, such as definition and performance information, on the shared disk and inherits this information in the event of a failover. If a single logical host contains multiple Performance Management programs, each uses the same shared folder.

6.2 Processing at failover

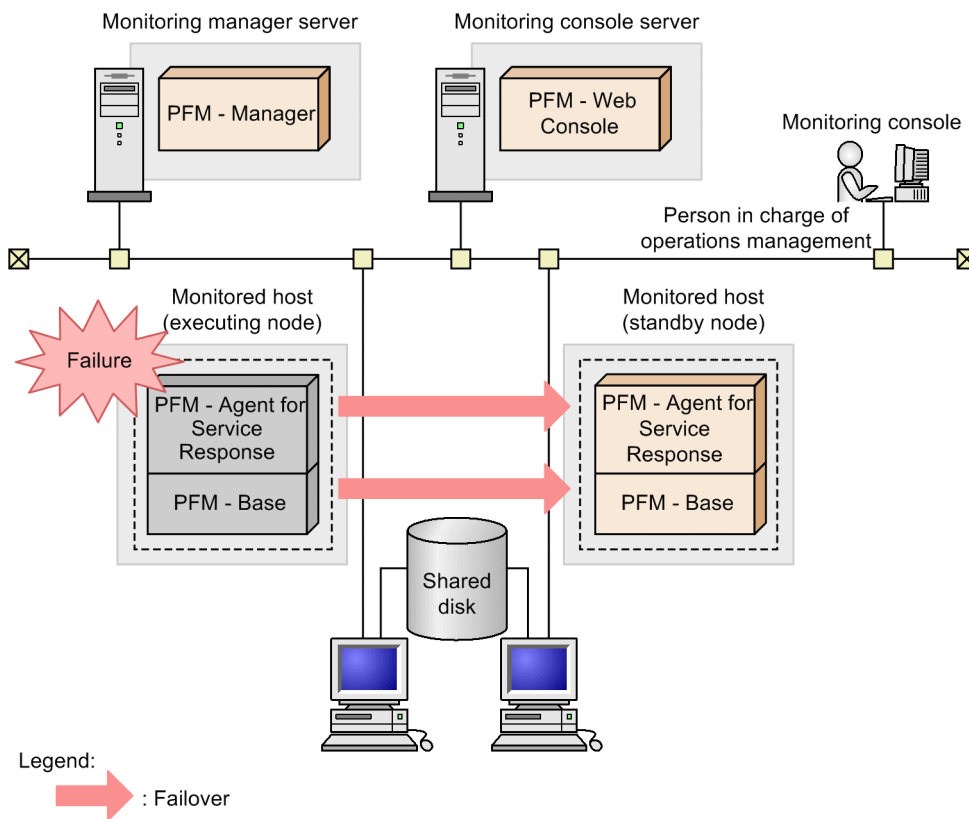
If a failure occurs on the executing host, control transfers to the standby host.

This section describes failover processing in the event of a failure on PFM - Agent for Service Response. It also describes the effects a failure of PFM - Manager on PFM - Agent for Service Response.

6.2.1 Failover when an error occurs

The following figure shows the processing when failover occurs on a host that is running PFM - Agent for Service Response.

Figure 6–2: Processing when failover occurs



If PFM - Web Console is used while PFM - Agent for Service Response is engaged in failover processing, the message `There was no answer (-6)` is displayed. When this message is displayed, wait until failover processing is completed.

Once PFM - Agent for Service Response has failed over, an attempt to use PFM - Web Console connects you to the PFM - Agent for Service Response that has started at the target node, so that you can perform operations.

6.2.2 Effects of PFM - Manager stopping

PFM - Manager stopping affects the entire Performance Management system.

PFM - Manager provides centralized management of the agent information for PFM - Agent for Service Response that is running at all the nodes. It also controls both alarm event notifications when thresholds are exceeded during performance monitoring by PFM - Agent for Service Response, and the execution of actions based on alarm events. Therefore, when PFM - Manager is stopped, the Performance Management system is affected as described in the following table.

Table 6–1: Effects of PFM - Manager stopping on PFM - Agent for Service Response

Program	Effects	Action
PFM - Agent for Service Response	<p>If PFM - Manager is stopped while PFM - Agent for Service Response is running, the following occurs:</p> <ul style="list-style-type: none"> • Collection of performance data continues. • Because alarm events cannot be reported to PFM - Manager, the alarm events for each alarm definition are saved, and notification for each event is reattempted until PFM - Manager starts. When the number of saved alarm events exceeds 3, the oldest alarm event is overwritten. If PFM - Agent for Service Response stops, the saved alarm events are deleted. • Notifications of alarm status already sent to PFM - Manager are reset when PFM - Manager restarts. Alarm statuses are refreshed once PFM - Manager has checked the status of PFM - Agent for Service Response. • An attempt to stop PFM - Agent for Service Response takes time because notification of this event cannot be sent to PFM - Manager. 	<p>Start PFM - Manager. An active PFM - Agent for Service Response can continue to operate. Because alarms may not be notified as expected, after PFM - Manager has been recovered, check the <code>KAVE00024-I</code> messages that have been output to PFM - Agent's common message log.</p>

You should evaluate your operating procedures, taking into account the effects of PFM - Manager stopping. Apart from system crashes, events such as a configuration change or maintenance may require stopping of PFM - Manager. You should stop for maintenance purposes only when the stopping will have the least effects on operations.

6.3 Installation and setup

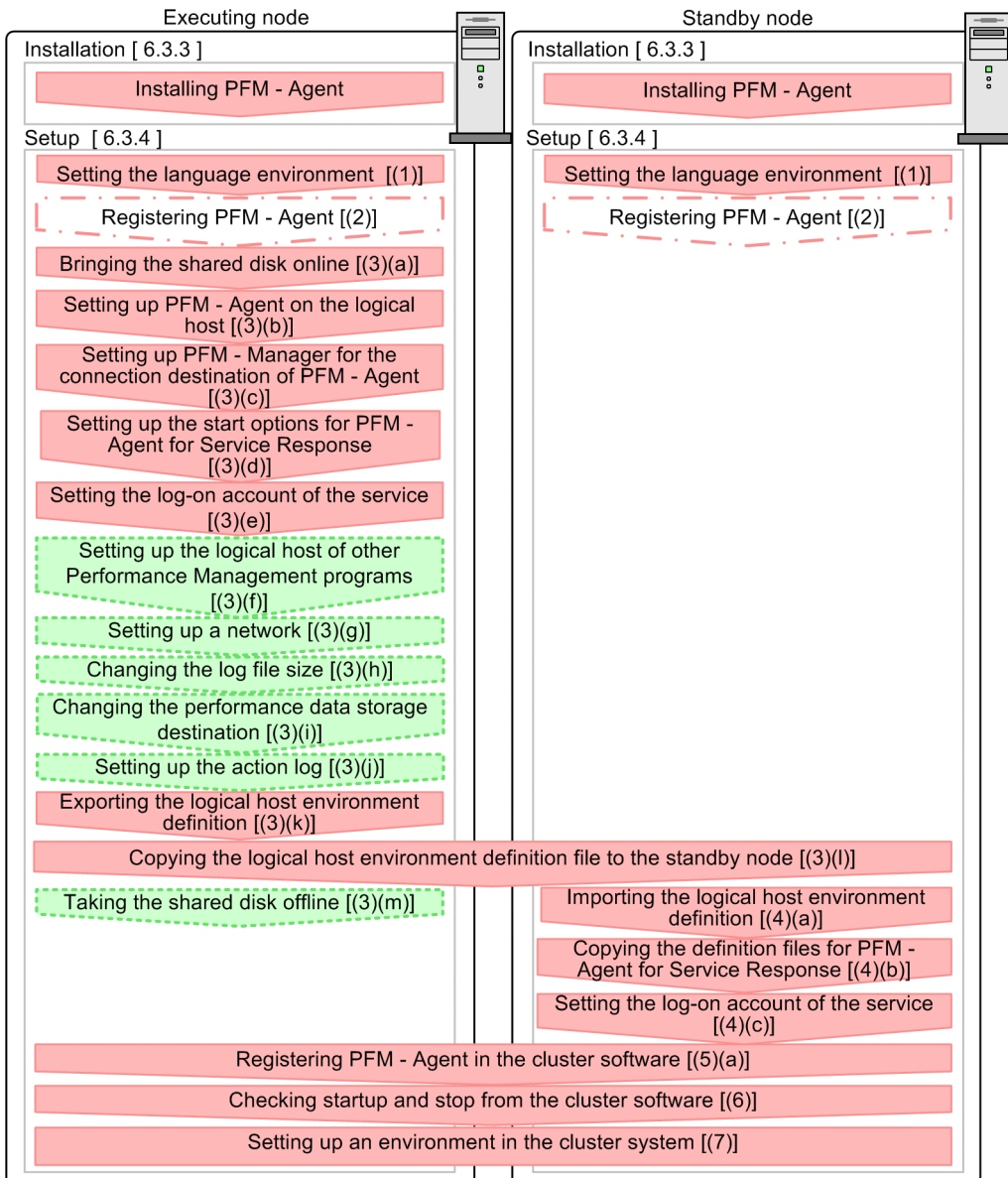
This section describes the procedures for constructing and setting up an environment for PFM - Agent for Service Response in a cluster system.

For details about the procedures for constructing and setting up environment for PFM - Manager, see the chapter that describes construction and operation in a cluster system in the *JP1/Performance Management User's Guide*.

6.3.1 Flow from installation to starting operation

The following figure shows the flow of installing and setting up PFM - Agent for Service Response for logical host use in a cluster system.

Figure 6–3: Flow of installing and setting up PFM - Agent for Service Response for logical host use in a cluster system



Legend:
 [] : See the indicated section
 [] : Required setup item
 [] : Setup item that is required depending on the case
 [] : Optional setup item

Note:

- When a PFM - Agent is set up in a logical host environment, the PFM - Agent definitions in the physical host environment are not inherited. A new environment is created when a logical host environment is set up.
- If you have set up PFM - Agent for Service Response in a logical host environment, do not run PFM - Agent for Service Response in the physical host environment. After the logical host environment has been created, if the service start method for PFM - Agent for Service Response in the physical host environment is set to **Automatic**, change it to **Manual**.

Note that you, for setup commands that require user input, you can select whether to execute such commands interactively or non-interactively.

If you execute a setup command interactively, you need to enter values in accordance with the command directives.

If you execute a setup command non-interactively, user input during command execution is not required because such input can be provided instead by values in option specifications or in definition files. Also, batch processing or remote execution can automate setup operations to reduce administrator workload and operating costs. Commands in the non-interactive mode are convenient in the following cases:

- You want to change the password used for connecting to monitoring targets on a regular basis.
- You want to improve the efficiency of the procedure for adding multiple monitoring targets.

For details about commands, see the manual *JPI/Performance Management Reference*.

6.3.2 Before installation

This subsection describes the prerequisites and required information for starting installation and setup.

(1) Prerequisites

To use PFM - Agent for Service Response in a cluster system, the following prerequisites must be satisfied.

(a) Cluster system

Confirm that the following conditions are met:

- The cluster system is controlled by the cluster software.
- The cluster software is configured to control the startup and termination of the PFM - Agent for Service Response running on logical hosts.
- Both the executing and standby systems are configured to suppress error reporting to Microsoft.

Notes:

- In Windows, a dialog box for reporting an error to Microsoft is displayed when an application error occurs. This dialog box may cause failover to fail; therefore, reporting of the error must be suppressed. For details about the suppression procedure, see the documentation that comes with the OS.
- In Windows, if an application error occurs, a dialog box will be displayed to report the error to Microsoft. If this dialog box is displayed, a failover could not occur. Therefore, you must disable error reporting. If the nodes have not been set up to disable error reporting, take the following steps.

In Windows Server 2008

1. Choose **Control Panel > System and Security > Action Center > Maintenance**.
2. In **Check for solutions to problem reports**, click **Settings**.
3. In the Choose when to check for solutions to problem reports dialog box, choose **Never check for solutions (not recommended)**.
4. Click the **OK** button.

In Windows Server 2012

1. Choose **Control Panel > System and Security > Action Center > Maintenance**.
2. In **Check for solutions to unreported problems**, click **Settings**.
3. In the **Windows Error Reporting Configuration** dialog box, choose **I don't want to participate, and don't ask me again**.
4. Click the **OK** button.

In Windows Server 2016

1. Right-click the Windows **Start** menu and then choose **Run** from the displayed menu.
2. Enter `gpedit.msc`, and then click the **OK** button.
The Local Group Policy Editor appears.
3. Click **Computer Configuration, Administrative Templates, Windows Components**, and then **Windows Error Reporting**.
4. In the right pane, right-click **Disable Windows Error Reporting**, and then from the displayed menu, choose **Edit**.
The setting window appears.
5. In the setting window, select the **Enabled** check box.
6. Click the **OK** button.

- If you upgrade from a version 08-00 of PFM - Agent for Service Response to a newer one while it is operating in a cluster system, you must copy the measurement condition registration file on the shared disk in advance. For details about, see [6.3.4 Setup](#).

(b) Shared disk

Make sure that the following conditions are satisfied:

- A shared disk is available to each logical host and information can be inherited from the executing node to the standby node.
- The shared disk is physically connected to each node by means of a Fibre Channel or SCSI.
Performance Management does not support a configuration in which a disk replicated by a network drive or via a network is used as a shared disk.
- In the event of a failover, the shared disk can be forced offline (for example, by the cluster software) to achieve failover even if some processing using the shared disk continues due to a problem.
- Each instance of Performance Management programs on the same logical host uses the same directory on the shared disk.

Note that you can change the location of the Store database to another folder on the shared disk.

(c) Logical host names and IP addresses

Make sure that the following conditions are satisfied:

- Each logical host has a logical host name and a corresponding logical IP address, and this information can be inherited from the executing node to the standby node.
- The logical host names and logical IP addresses are set in the `hosts` file and name server.
- If DNS operation is used, the host name without the domain name is used as the logical host name, not the FQDN name.
- All physical and logical host names are unique throughout the system.

Notes:

- Do not specify a physical host name (that is, a host name displayed by the `hostname` command) as a logical host name. If it is specified, normal communication processing may not be achieved.
- A logical host name must consist of 1 to 32 bytes of alphanumeric characters. None of the following symbols or the space character can be used:
`/ \ : ; * ? ' " < > | & = , .`

- A logical host name cannot begin with `localhost`, an IP address, or the hyphen (-).

(d) Settings when IPv6 used

Because Performance Management supports network configurations for IPv4 environments and IPv6 environments, you can use Performance Management in a network configuration that contains both IPv4 and IPv6 environments. PFM - Agent for Service Response can communicate with PFM - Manager by using IPv6.

Note, however, that this applies only when Windows or Linux runs on a host with PFM - Manager installed.

For details about the scope of communication in the IPv4 and IPv6 environments, see *K. About Communication in IPv4 Environments and IPv6 Environments*.

To use IPv6 for communication, IPv6 must be enabled on both the PFM - Manager host and the PFM - Agent host by using the `jpccconf ipv6 enable` command.

In addition, before installing PFM - Agent for Service Response, you need to enable the use of IPv6 on the PFM - Agent for Service Response host. You have to execute the `jpccconf ipv6 enable` command to enable this setting. If this setting is already enabled, however, you do not need to execute the command. If you want to check whether the use of IPv6 is enabled, execute the `jpccconf ipv6 display` command.

The following describes when you need to execute this command.

Cases when the `jpccconf ipv6 enable` command needs to be executed:

- When switching from an IPv4 environment to an IPv6 environment on each host
- When switching the PFM - Manager environment from IPv4 to IPv6 in an environment in which both IPv4 and IPv6 are used

Cases when the `jpccconf ipv6 enable` command does not need to be executed:

- When each host already operates in an IPv6 environment
- When PFM - Manager operates in an IPv6 environment in an environment in which both IPv4 and IPv6 are used

The following shows an example of executing the `jpccconf ipv6 enable` command:

```
jpccconf ipv6 enable
```

Execute the `jpccconf ipv6 enable` command on both the executing node and the standby node. For details about the conditions or occasions for executing the `jpccconf ipv6 enable` command and the `jpccconf ipv6 display` command, see the chapter that describes network configuration examples in an environment that includes IPv6 in the *JP1/Performance Management Planning and Configuration Guide*.

(2) Information required to set up PFM - Agent for Service Response for logical host use

To set up PFM - Agent for Service Response for logical host use, you must provide the information listed in the table below, in addition to the environment information that is needed to set up a normal PFM - Agent for Service Response.

Table 6–2: Information required to set up PFM - Agent for Service Response for logical host use

Item	Example
Logical host name	jp1-halsr

Item	Example
Logical IP address	172.16.92.100
Shared disk	S:\jrp1

When multiple Performance Management programs are installed on a single logical host, the programs share the same folder on the shared disk.

For details about the capacity required on the shared disk, see [A. Estimating System Requirements](#).

(3) Making the logical host subject to failover in the event of a PFM - Agent for Service Response failure

If you employ a system configuration in which PFM - Agent for Service Response operates on a logical host, you should evaluate whether or not the entire logical host should be subject to failover in the event of a PFM - Agent for Service Response failure.

If a PFM - Agent for Service Response failure results in failover of the entire logical host, a job application that is running on the same logical host will also result in failover, which will affect the job.

Hitachi recommends that you use one of the following cluster software settings so that errors on PFM - Agent for Service Response do not affect system operations on the same logical host:

- Do not monitor operation of PFM - Agent for Service Response
- Do not allow detection of errors in PFM - Agent for Service Response errors to result in failover

6.3.3 Installation

Install PFM - Base and PFM - Agent for Service Response on both executing and standby nodes.

The installation target is the local disk. Do not install PFM - Agent for Service Response on a shared disk.

The installation procedure is the same as for a non-cluster system. For details about the installation procedure, see [3.1.3 Installation procedure](#).

6.3.4 Setup

This subsection describes the setup required to operate Performance Management in a cluster system.

(1) Setting the language environment

Windows has several locations for setting the language environment. The setting must be the same for all of them.

For details about how to set the language environment, see the section describing how to set the language environment in the *JPI/Performance Management Planning and Configuration Guide*.

(2) Registering PFM - Agent for Service Response

To add PFM - Agent for Service Response to an existing Performance Management system, you must perform setup to register PFM - Agent for Service Response.

You use PFM - Manager and PFM - Web Console to register PFM - Agent for Service Response.

When the version of PFM - Manager is 09-00 or later, you do not need to perform the procedure explained here, because PFM - Agent is automatically registered. However, you must manually register the PFM - Agent instances whose data model version is not provided in the PFM - Manager release notes. For details about data model versions for PFM - Agent for Service Response, see *H. Version Compatibility*.

The procedure for doing so is the same as for a non-cluster system. For details about this procedure, see *3.1.4 PFM - Agent for Service Response setup procedure*.

(3) Setting up a logical host environment on the executing node

You must set up a logical host environment for PFM - Agent for Service Response on the executing node.

Note:

Before starting this setup, stop all services of Performance Management programs in the entire Performance Management system. For details about how to stop services, see the chapter that describes startup and termination of Performance Management in the *JP1/Performance Management User's Guide*.

(a) Bringing the shared disk online

Make sure that the shared disk is online. If it is not online, bring it online using a cluster software operation or volume manager operation.

(b) Setting up a logical host environment for PFM - Agent for Service Response

Execute the `jpccconf ha setup` command to create a logical host environment. This command creates a logical host environment by copying necessary data to the shared disk and setting definitions for a logical host.

To set up a logical host environment for PFM - Agent for Service Response:

1. Execute the `jpccconf ha setup` command to create a logical host environment.

Execute the command as follows:

```
jpccconf ha setup -key SR -host jp1-halsr -d S:\jp1
```

Use `-lhost` to specify the logical host name. This example specifies `jp1-halsr` as the logical host name. If you use DNS, specify the logical host name without the domain name.

Specify for the environment folder name in `-d` the name of a folder on the shared disk. For example, if `-d S:\jp1` is specified, `S:\jp1\jp1pc` is created and then files for the logical host environment are created.

2. Execute the `jpccconf ha list` command to check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all
```

Make sure that the created logical host environment is valid.

(c) Setting up PFM - Manager for the connection destination of PFM - Agent for Service Response

Execute the `jpccconf mgrhost define` command to set the PFM - Manager that manages PFM - Agent for Service Response. When the version of PFM - Manager is 09-00 or later, you do not need to perform the procedure explained here, because PFM - Agent for Service Response is automatically registered.

To set the connection-target PFM - Manager:

1. Execute the `jpccconf mgrhost define` command to set the connection-target PFM - Manager.

Execute the command as follows:

```
jpccconf mgrhost define -host jp1-hal -host jp1-halsr
```

Specify the host name of the connection-target PFM - Manager in the `-host` option. If the connection-target PFM - Manager runs on a logical host, specify the logical host name of the connection-target PFM - Manager in the `-host` option. This example specifies `jp1-hal` as the PFM - Manager's logical host name.

Use `-lhost` to specify the logical host name of PFM - Agent for Service Response. This example specifies `jp1-halsr` as the logical host name of PFM - Agent for Service Response.

Although the above example shows interactive execution, you can also execute the `jpccconf mgrhost define` command non-interactively. For details about the `jpccconf mgrhost define` command, see the chapter that explains the commands in the manual *JPI/Performance Management Reference*.

(d) Setting up the start options for PFM - Agent for Service Response

For the start options for cluster operation, change the settings of the Probe action condition definition file.

1. Set the shared folder in `shared_directory` in the `[Cluster]` section of the Probe action condition definition file.

Because PFM - Agent for Service Response shares information during switchover between the executing and standby systems, creates the files shown in the table below under the shared file storage folder.

Table 6–3: Shared file storage folders

Type of shared file	Shared file storage folder
Report file	<code>folder-on-shared-disk\jp1pc\agtv\probe\report</code>
Temporary report file	<code>folder-on-shared-disk\jp1pc\agtv\probe\tmp</code>
Measurement condition registration file	<code>folder-on-shared-disk\jp1pc\agtv\probe\task\esp</code>

The following describes the notes on shared file storage folder.

- The required folders must have been created in advance under the folder on the shared disk.
- The files related to the measurement condition registration file (`esptask.dtd`, `esptask.xml`) under `installation-folder\agtv\probe\task\esp` must have been copied in advance to the folder on the shared disk.

Note:

You can copy the related files to the measurement condition registration file (`esptask.dtd`, `esptask.xml`) to the folder on the shared disk, after setting up a logical host environment.

- If you perform either of the following operations, the measurement condition registration file is created under the folder on the shared disk.
 - To specify the measurement condition on PFM - Web Console
 - To perform the simplified registration of IE scenario on the IE Recorder
- If you edit the measurement condition registration file directly, edit the file on the physical host and then copy to the folder on the shared disk, or edit the measurement condition registration file on the shared disk directly.

You must specify both of the following settings in the `[Cluster]` section of the Probe action condition definition file (`esp.conf`).

- To specify the path corresponding to *folder-on-shared-disk* in the above table as the value of the `shared_directory`
- To specify `Y` as the value of the `cluster_flag`

The following shows an example of the configuration under the directory on the shared disk. In this example, you must specify `T:\shdsk` in `shared_directory` in the `[Cluster]` section of the Probe action condition definition file.

Example: Specify `T:\shdsk` as the folder on the shared disk:

```
T:\shdsk\jplpc\agtv\probe\report
T:\shdsk\jplpc\agtv\probe\tmp
T:\shdsk\jplpc\agtv\probe\task\esp
```

2. Set `Y` as the value of the `ie_service_flag` in the `[General]` section of the Probe action condition definition file.

If you measure the IE scenario, you must define this item.

Note:

When you upgrade PFM - Agent for Service Response, the Probe action condition definition file does not have the `ie_service_flag` entry in the `[General]` section. Add and set the `ie_service_flag` in the file.

For details about setting other start options, see [3.1.4 PFM - Agent for Service Response setup procedure](#). For details about the Probe action condition definition file, see [8.2 Probe action condition definition file \(esp.conf\)](#).

If you use the Web Recorder to define the Web transactions, define the Web Recorder action condition definition file (`wr.conf`). For details about the Web Recorder action condition definition file, see [8.4 Web Recorder action condition definition file \(wr.conf\)](#).

If you use the IE Recorder to define the IE scenarios, define the IE Recorder action condition definition file (`jpcvierec.conf`). For details about the IE Recorder action condition definition file, see [8.8 IE Recorder action condition definition file \(jpcvierec.conf\)](#).

If you use the user-defined commands, define the command registration file (`espcommand.xml`). For details about the command registration file, see [8.6 Command registration file \(espcommand.xml\)](#).

(e) Setting the log-on account for the service

The following shows the procedure for setting the log-on account for the Extensible Service IE Probe service on a logical host.

1. From the **Start** menu of Windows, choose **Settings, Control Panel, Administrative Tool**, and then **Services**.
2. Select Extensible Service IE Probe service, from the **Action** menu, choose **Properties**, then the Properties of Extensible Service IE Probe dialog box appears.
3. Click the **This account** button on the **Log On** tab, then the **Browse** button is activated.
4. Specify a user account[#] that executes the service in the **Account** text box. Click the **Browse** button, and you can specify the user account in the **Select User** dialog box.

#

Specify the user account that executes the service is the same as the account for measurement that you use to check replaying the operations in the IE Recorder.

5. Enter the password in the **Password** and **Confirm password** text boxes, and then click the **OK** button.

(f) Setting up the logical host environments of other Performance Management programs

If you have other PFM - Manager or PFM - Agent programs to be set up on the same logical host in addition to PFM - Agent for Service Response, set them up at this stage.

For details about the setup procedure, see the chapter that describes operations in a cluster system in the *JPI/Performance Management User's Guide*, or in the applicable PFM - Agent manual.

(g) Setting up a network

These settings are required only when the Performance Management programs run in a network environment that uses a firewall. If you establish communication between Performance Management programs via a firewall, use the `jpccconf port` command to set the port numbers.

For details about how to set port numbers, see the chapter that describes installation and setup, and the chapter that describes construction and operations in a cluster system, in the *JPI/Performance Management Planning and Configuration Guide*.

You must also set the IP addresses if you will be specifying IP addresses in operating Performance Management in a network environment connected to multiple LANs. To do this, directly edit the contents of the `jpchosts` file.

For details about how to set IP addresses, see the chapter that describes installation and setup for Windows in the *JPI/Performance Management Planning and Configuration Guide*.

Note:

Once you have edited the `jpchosts` file, copy it from the executing node to the standby node.

(h) Changing the log file size

Performance Management's operating status is output to a log file unique to Performance Management. This log is called the *common message log*; it consists of two files with a default size of 2,048 kilobytes each. This setting is required only when you wish to change this file size.

For details, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

(i) Changing the performance data storage destination

Perform this setting only if you want to change the folder where the database of performance data managed by PFM - Agent is saved, backed up, exported, or imported.

For details, see [3.4.1 Changing the performance data storage destination](#).

(j) Setting up the action log

This setting is required to output action log when alarm occur. The action log stores history information that is output in conjunction with the alarms for thresholds related to system load and other conditions.

For details about how to set up the action log, see [I. Outputting Action Log Data](#).

(k) Exporting the logical host environment definition

After you have created a logical host environment for PFM - Agent for Service Response, you must export the environment definition to a file. This export processing involves output of the definition information for the Performance Management program set up on the logical host to a file in the batch mode. If you are setting up other Performance

Management programs on the same logical host, export the environment definitions after all setup processes have been completed.

To export the logical host environment definition:

1. Execute the `jpccconf ha export` command to export the logical host environment definition.

Output to an export file the definition information for the logical host environment that has been created so far. You can assign any name to the export file.

For example, to export the logical host environment definition to the `lhostexp.txt` file, execute the following command:

```
jpccconf ha export -f lhostexp.txt
```

Although the above example shows interactive execution, you can also execute the `jpccconf ha export` command non-interactively. For details about the `jpccconf ha export` command, see the chapter that explains the commands in the manual *JPI/Performance Management Reference*.

(l) Copying the logical host environment definition file to the standby node

Copy the logical host environment definition file exported in (k) *Exporting the logical host environment definition* from the executing node to the standby node.

(m) Taking the shared disk offline

Using a cluster software operation or volume manager operation, take the shared disk offline to complete the task. If you plan to continue using the shared disk, there is no need to take it offline.

(4) Setting up a logical host environment for the standby system

Set up a logical host environment for PFM - Agent for Service Response on the standby node.

(a) Importing the logical host environment definition

Import the export file that was copied from the executing node to the standby node.

To specify settings for executing at the standby node the Performance Management program on the logical host created at the executing node, use the `jpccconf ha import` command. If multiple Performance Management programs have been set up on a single logical host, the settings for all the programs are imported in the batch mode.

When executing this command, there is no need to keep the shared disk in online status.

To import the logical host environment definition:

1. Execute the `jpccconf ha import` command to import the logical host environment definition.

Execute the following command:

```
jpccconf ha import -f lhostexp.txt
```

Although the above example shows interactive execution, you can also execute the `jpccconf ha import` command non-interactively. For details about the `jpccconf ha import` command, see the chapter that explains the commands in the manual *JPI/Performance Management Reference*.

This command changes settings in such a way that the environment for the standby node becomes the same as in the export file. As a result, setup is performed for starting PFM - Agent for Service Response on the logical host.

If fixed port numbers were set by the `jpccconf port` command during setup, they are also set in the same manner.

2. Execute the `jpccconf ha list` command to check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all
```

Make sure that the displayed information is the same as when `jpccconf ha list` command is executed at the executing node.

(b) Copying the definition files for PFM - Agent for Service Response

You must copy from the executing node to the standby node the definition files created in (3)(d) *Setting up the start options for PFM - Agent for Service Response*.

1. Copy from the executing node to the standby node the Probe action condition definition file (`esp.conf`).
`installation-folder\agtv\probe\conf`
2. If you define the Web transactions, copy from the executing node to the standby node the Web Recorder action condition definition file (`wr.conf`) and the Web transaction files.
`installation-folder\agtv\probe\conf`
`installation-folder\agtv\probe\webtrans`
3. If you define the IE scenarios, copy from the executing node to the standby node the IE Recorder action condition definition file (`jpccvrierec.conf`) and the IE scenario files.
`installation-folder\agtv\probe\conf`
`installation-folder\agtv\probe\iescena`
4. If you use the user-defined commands, copy from the executing node to the standby node the command registration file (`espcommand.xml`) and user-defined commands.
`installation-folder\agtv\probe\conf`
`installation-folder\agtv\probe\user`
5. If you register the passwords, copy from the executing node to the standby node the password file (`esp.pdb`).
`installation-folder\agtv\probe\passwd`
6. If you want to apply server authentication and client authentication for HTTPS measurement, copy the certificate file to the standby node.

(c) Setting the log-on account for the service

Perform the procedure shown in (3)(e) *Setting the log-on account for the service* on the standby node.

(5) Registering in the cluster software

To run a Performance Management program in a logical host environment, you must register the program in the cluster software and set up the environment in such a way that the Performance Management program starts and terminates from the cluster software.

This subsection describes the settings for registering PFM - Agent for Service Response in the cluster software.

(a) Registering PFM - Agent for Service Response in the cluster software

This subsection describes the settings for registering PFM - Agent for Service Response in the cluster software.

For PFM - Agent for Service Response, you register in the cluster software the services listed in the table below.

! Important

For details about dependency settings when using a logical host for PFM - Manager in a cluster system, see the chapter that describes construction and operation in a cluster system in the *JPI/Performance Management User's Guide*.

Table 6–4: PFM - Agent for Service Response services to be registered in the cluster software

No.	Name	Service name	Dependency
1	PFM - Agent Store for ServiceResponse [<i>LHOST</i>]	JP1PCAGT_VS [<i>LHOST</i>]	IP address resource Physical disk resource
2	PFM - Agent for ServiceResponse [<i>LHOST</i>]	JP1PCAGT_VA [<i>LHOST</i>]	Cluster resources listed in row 1 above.
3	PFM - Action Handler [<i>LHOST</i>]	JP1PCMGR_PH [<i>LHOST</i>]	IP address resource Physical disk resource
4	Extensible Service IE Probe	JP1PCVIE#1,#2	IP address resource Physical disk resource
5	Extensible Service Probe	JP1ESP#1,#3,#4	IP address resource Physical disk resource

#1

You do not need to register the Extensible Service IE Probe service and Extensible Service Probe service in the cluster software because they are started and stopped under control of the PFM - Agent for Service Response service. However, if you want to monitor the Extensible Service IE Probe service and the Extensible Service Probe service, register them in the cluster software.

If you registered the Extensible Service IE Probe service and Extensible Service Probe service in the cluster software, stop them before you attempt to stop the PFM - Agent for ServiceResponse service or PFM - Agent Store for ServiceResponse service. If you do not stop them, the cluster software might detect an error in these services.

#2

You do not need to register this service unless you want to monitor IE scenarios.

#3

If the task is not registered or if a Web transaction file contains an XML syntax error, the Extensible Service Probe service stops.

#4

You do not need to register this service unless you want to monitor Internet services and Web transactions.

Replace *LHOST* with the logical host name. For example, if the logical host name is `jp1-halsr`, the service is PFM - Agent Store for Service Response [`jp1-halsr`], and the service name is `JP1PCAGT_VS [jp1-halsr]`.

For WSFC, register these services as WSFC resources. Set each resource as follows:

- In **Resource Type**, register the resource as **Generic Service**.
- Set **Dependencies** as shown in Table 6-4.
- Do not set **Startup parameters** or **Registry Replication**.
- Set the **Policies** tab in Properties by taking into account whether you want a failover to occur in the event of a Performance Management program failure.

For example, to trigger a failover when a failure occurs in PFM - Agent for Service Response, set the **Policies** tab as follows:

- Select the **If resource fails, attempt restart on current node** radio button.
- Select the **If restart is unsuccessful, fail over all resources** in this service or application check box[#].

- In principle, set **Maximum restarts in the specified period:** to **3**.

#

In the case of Windows Server 2012 or later, the **If restart is unsuccessful, fail over all resources in this Role** check box is used instead.

Note:

A service registered in the cluster is started and stopped from the cluster. Set **Startup type** to **Manual** so that the service will not be started automatically during OS startup. Immediately after setup is performed by the `jpccconf ha setup` command, the service is set to **Manual**.

(6) Checking startup and stop

Make sure that the Performance Management programs function normally by starting and terminating the programs from the cluster software on each node.

(7) Setting up an environment in the cluster system

When you have finished setting up the Performance Management programs, set up an environment for them so that PFM - Web Console can be used to display monitored program operating status reports as appropriate to the operations, and so that it can send notifications to the user in the event of a problem on a monitored program.

For details about how to set up an environment for the Performance Management programs, see the chapter that describes construction and operation in a cluster system in the *JP1/Performance Management User's Guide*.

6.4 Uninstallation and unsetup

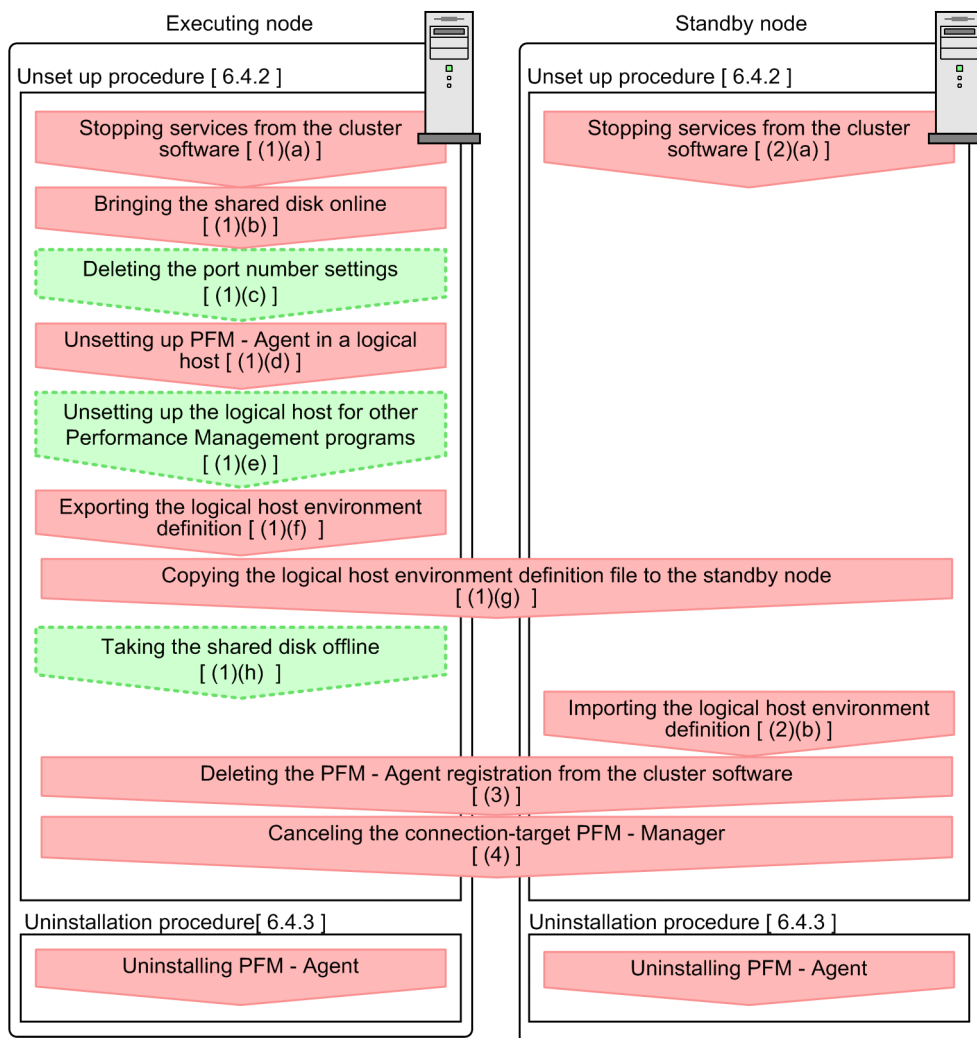
This section describes the procedures for uninstalling and unsetting up a PFM - Agent for Service Response that is running in a cluster system.

For details about uninstalling and unsetting up PFM - Manager, see the chapter that describes construction and operation in a cluster system in the *JPI/Performance Management User's Guide*.


6.4.1 Flow of PFM - Agent for Service Response uninstallation and unsetup

The following figure shows the flow of uninstalling and unsetting up a PFM - Agent for Service Response that is running in a cluster system.

Figure 6–4: Flow of uninstalling and unsetting up PFM - Agent for Service Response running on a logical host in a cluster system



Legend:

 : Required setup item

 : Optional setup item

[] : See the indicated section

6.4.2 Unsetting up PFM - Agent for Service Response

Unsetup the logical host environment. This subsection describes the unsetup procedures for the executing node and the standby node. Unsetup the executing node first, and then the standby node.

The following describes the procedures for unsetting up PFM - Agent for Service Response.

Note:

You must stop all services of the Performance Management programs running on the executing and standby nodes where you are unsetting up PFM - Agent. For details about how to stop services, see the chapter that describes construction and operation in a cluster system in the *JPI/Performance Management System Configuration and User's Guide*.

(1) Unsetting up the logical host environment on the executing node

You unsetup the logical host environment for PFM - Agent for Service Response on the executing node.

(a) Stopping services from the cluster software

Stop the Performance Management programs and services that are running on the executing nodes from the cluster software. For details about how to stop the programs and services, see the cluster software documentation.

(b) Bringing the shared disk online

Make sure that the shared disk is online. If it is not online, bring it online using a cluster software operation or volume manager operation.

(c) Deleting the port number settings

This procedure is required only when the `jpccconf port` command was used to set port numbers during setup in an environment that uses a firewall.

For details about how to delete port numbers, see the chapter that describes installation and setup for Windows and the chapter that describes operations in a cluster system in the *JPI/Performance Management Planning and Configuration Guide*.

(d) Unsetting up PFM - Agent for Service Response in a logical host environment

To unsetup PFM - Agent for Service Response in a logical host environment:

Note:

If a logical host environment is deleted while the shared disk is offline, the logical host settings are deleted from the physical host, but the folders and files are not deleted from the shared disk. In such a case, you must bring the shared disk online and manually delete the `jp1pc` folder under the environment folder.

1. Execute the `jpccconf ha list` command to check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all -host jp1-halsr
```

You must check the current settings before you unsetup the logical host environment. Check information such as the name of the logical host and the shared disk path.

2. Execute the `jpccconf ha unsetup` command to delete the logical host environment for PFM - Agent for Service Response.

Execute the command as follows:

```
jpccconf ha unsetup -key SR -host jpl-halsr
```

The `jpccconf ha unsetup` command deletes the settings for starting PFM - Agent for Service Response on the logical host. It also deletes files related logical host from the shared disk.

3. Execute the `jpccconf ha list` command to check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all
```

Make sure that PFM - Agent for Service Response has been deleted from the logical host environment.

(e) Unsetting up the logical host environment for other Performance Management programs

At this point, unsetup other Performance Management programs from the same logical host (in addition to unsetup PFM - Agent for Service Response).

For details about the unsetup procedure, see the chapter that describes operations in a cluster system in the *JPI/Performance Management User's Guide* or in the applicable PFM - Agent manual.

(f) Exporting the logical host environment definition

After you have deleted PFM - Agent for Service Response from the logical host, you must export the environment definition to a file.

Performance Management uses a method that matches the environment of the standby system to that of the executing system by exporting and importing the environment definitions

When the environment definition exported from the executing node (definition from which the Performance Management definition has been deleted) is imported to the standby node, the system compares it with the environment definition existing in the standby node (definition that still contains the Performance Management definition) to determine the differences (the part deleted at the executing node). The system then deletes the Performance Management environment definition.

To export the logical host environment definition:

1. Execute the `jpccconf ha export` command to export the logical host environment definition.

Output the definition information of the logical host environment for Performance Management to a file. You can use any desired export file name.

For example, to export the logical host environment definition to the `lhostexp.txt` file, execute the following command:

```
jpccconf ha export -f lhostexp.txt
```

Although the above example shows interactive execution, you can also execute the `jpccconf ha export` command non-interactively. For details about the `jpccconf ha export` command, see the chapter that explains the commands in the manual *JPI/Performance Management Reference*.

(g) Copying the logical host environment definition file to the standby node

Copy the logical host environment definition file exported in (f) *Exporting the logical host environment definition* from the executing node to the standby node.

(h) Taking the shared disk offline

Using a cluster software operation or volume manager operation, take the shared disk offline to complete the task. If you plan to continue using the shared disk, there is no need to take it offline.

(2) Unsetting up the logical host environment on the standby node

Copy the file you exported from the executing node to the standby node, and then unsetup the logical host environment on the standby node. Note that the shared disk does not need to be online when you do this.

(a) Stopping services from the cluster software

Stop the Performance Management programs and services that are running on the standby nodes from the cluster software. For details about how to stop the programs and services, see the cluster software documentation.

(b) Importing the logical host environment definition file

Import the export file copied from the executing node onto the standby node in order to commit the file to the standby node. At the standby node, there is no need to take the shared disk offline during the import operation

To import the logical host environment definition file:

1. Execute the `jpccconf ha import` command to import the logical host environment definition.

Execute the command as follows:

```
jpccconf ha import -f lhostexp.txt
```

Although the above example shows interactive execution, you can also execute the `jpccconf ha import` command non-interactively. For details about the `jpccconf ha import` command, see the chapter that explains the commands in the manual *JP1/Performance Management Reference*.

This command changes settings in such a way that the environment for the standby node becomes the same as in the export file. As a result, the settings for starting PFM - Agent for Service Response on the logical host are deleted. If you have unsetup other Performance Management programs on the logical host, these settings are also deleted. If fixed port numbers were set up using the `jpccconf port` command during setup, they are also deleted.

2. Execute the `jpccconf ha list -key all` command to check the logical host settings.

Execute the command as follows:

```
jpccconf ha list -key all
```

Make sure that the displayed information is the same as when `jpccconf ha list` is executed at the executing node.

(3) Deleting registration from the cluster software

Delete the settings related to PFM - Agent for Service Response from the cluster software on the logical host.

For details about how to delete the settings, see the cluster software documentation.

(4) Canceling the connection-target PFM - Manager

To cancel the connection-target PFM Manager, you need to first delete the service information of the PFM - Agent for Service Response that is connected to the PFM - Manager in question.

For details about how to delete service information, see the section describing how to delete service information in the chapter that explains installation and setup (in Windows) in the *JP1/Performance Management Planning and Configuration Guide*.

To change the connection target to another PFM - Manager, see [6.3.4\(3\)\(c\) Setting up PFM - Manager for the connection destination of PFM - Agent for Service Response](#).

6.4.3 Uninstallation

This subsection explains how to uninstall PFM - Base and PFM - Agent for Service Response.

The uninstallation procedure is the same as for a non-cluster system. For details, see [3.2.3 Uninstallation procedure](#).

Notes:

- When you uninstall PFM - Agent for Service Response, stop all services of the Performance Management programs on the node where PFM - Agent for Service Response is to be uninstalled.
- If you uninstall PFM - Agent for Service Response without deleting the logical host environment, the environment folder may remain. In this case, delete the environment folder.

6.5 Changing the PFM - Agent for Service Response operation method

This section describes how to change the operation of PFM - Agent for Service Response in a cluster system. For details about how to change the operation of Performance Management as a whole, see the chapter that explains cluster system configuration and operation in the *JPI/Performance Management Planning and Configuration Guide*.

6.5.1 Exporting and importing the logical host environment definition file

You must export and import the logical host environment definition file only if you perform any one of the following operations:

- When you set up the logical host environment, you change the node configuration on the logical host.
For details about how to set up the logical host environment, see *6.3.4(3) Setting up a logical host environment on the executing node*.
- When you set up the logical host environment of other Performance Management programs, you perform an operation that requires exporting the logical host environment definition file.
For details about how to set up the logical host environment of other Performance Management program, see *6.3.4(3)(f) Setting up the logical host environments of other Performance Management programs*.
- When you are setting up the network, you set the port numbers.
For details about how to set up the network, see *6.3.4(3)(g) Setting up a network*.

For details about how to export and import the logical host environment definition files, see from *6.3.4(3)(k) Exporting the logical host environment definition* to *6.3.4(4) Setting up a logical host environment for the standby system*.

6.5.2 Changing the definition files of PFM - Agent for Service Response

When you change the definition files mentioned in *6.3.4 (3)(d) Setting up the start options for PFM - Agent for Service Response* at the executing node on the logical host, copy the changed files to the standby node on the logical host.

Similarly, if there are any changes to the definition files that were copied to the standby node on logical host in *6.3.4(4)(b) Copying the definition files for PFM - Agent for Service Response*, copy the changed files to the standby node on the logical host.

6.6 Notes on operating PFM - Agent for Service Response in a cluster system

This section describes the notes on operating PFM - Agent for Service Response in a cluster system.

6.6.1 Notes on using the IE scenarios

If you use the IE scenarios, specify the same settings about the following items on each physical host of the executing and standby nodes.

(1) Setting of the Probe action condition definition file

Change the settings of the Probe action condition definition file to start and stop the IE Probe Daemon service using the Windows services. For details about how to change the settings of the Probe action condition definition file, see [5.1.5\(1\) *Setting the Probe action condition definition file.*](#)

(2) Setting the account for measurement

Create an account for measuring response performance of the operations in the Internet Explorer.

(3) Setting the environment for measuring the IE scenarios

To measure the IE scenarios, log on to the Windows by the account for measurement and set the environment for measuring the IE scenarios. For details, see [5.1.5\(3\) *Setting the environment for measuring the IE scenario.*](#)

(4) Recording the IE scenarios

To record the IE scenarios, log on to the Windows by the account for measurement and record the IE scenarios. For details about how to record, see [5.1.5\(4\) *Recording the IE scenarios.*](#)

(5) Check replaying the IE scenarios in the IE Recorder

To measure the IE scenarios, log on to the Windows by the account for measurement, and check in advance whether the IE scenarios are replayed correctly in the IE Recorder before you measure the IE scenarios.

(6) Setting the log-on account for the service

Set the log on account for the Extensible Service IE Probe service. For details, see [5.1.5\(6\) *Setting the log-on account for the service.*](#)

If the account for measurement is different from the log on account for the Extensible Service IE Probe service, the errors may occur when replaying the IE scenarios, such as error KAVK38756-E.

7

Windows

This chapter describes the display items and settings for Web Recorder and IE Recorder.

7.1 Basic window operations and window transitions

This section describes the basic Web Recorder and IE Recorder window operations and window transitions.

7.1.1 Basic window operations

This subsection describes the basic operations on Web Recorder and IE Recorder windows.

OK button:

Applies the settings you have specified and then closes the window.

Cancel button:

Closes the window without applying the settings.

Apply button:

Applies the settings while keeping the window displayed.

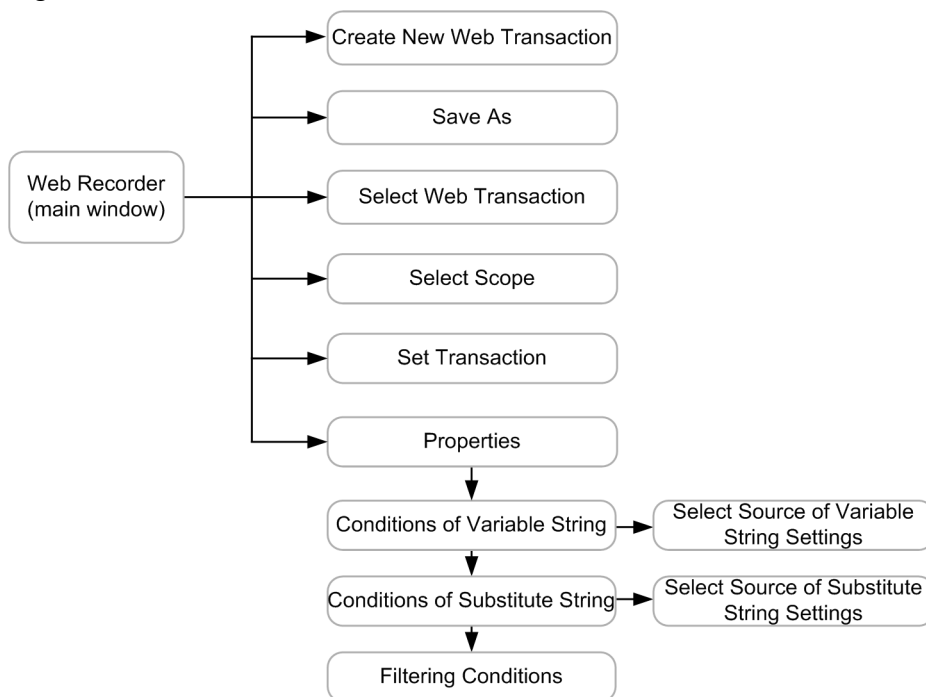
Choosing **About** from the **Help** menu:

Displays the version information.

7.1.2 Window transitions

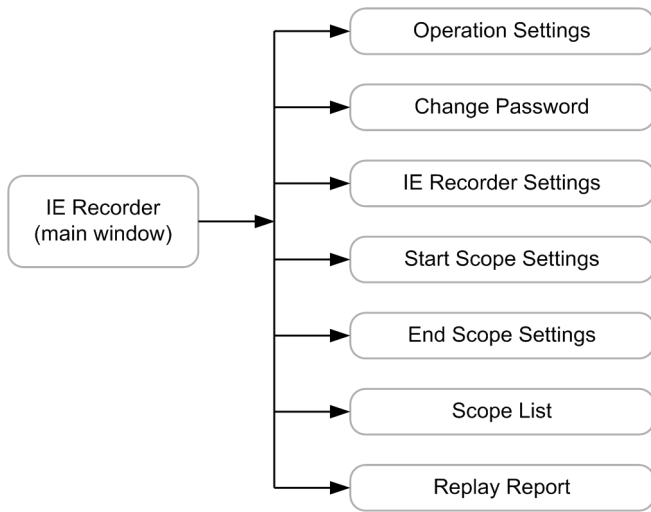
The following figure shows the Web Recorder window transitions.

Figure 7–1: Web Recorder window transitions



The following figure shows the IE Recorder window transitions.

Figure 7–2: IE Recorder window transitions



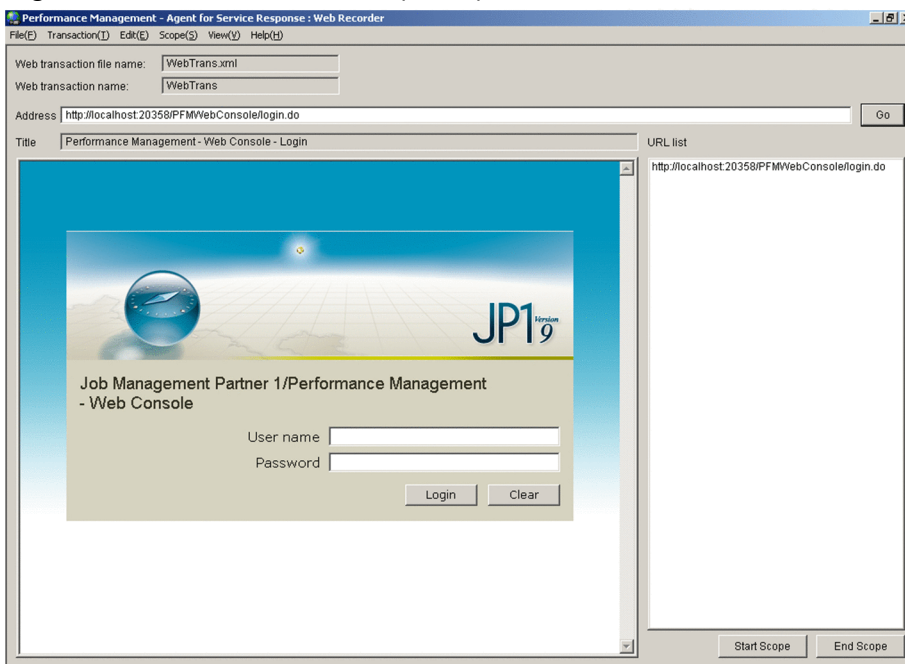
7.2 Web Recorder windows

Web Recorder provides windows for defining a series of Web access operations that are to be monitored as a Web transaction, as well as windows for defining necessary information. This section describes each Web Recorder window.

7.2.1 Web Recorder (main) window

The Web Recorder (main) window is used to define a Web transaction. This window is provided in two modes, the IE mode and the direct entry mode. The IE mode is used to define a Web transaction by displaying Internet Explorer windows and recording the browser operations performed in those windows. The direct entry mode is used to edit the step-by-step information that constitutes a Web transaction.

Figure 7–3: Web Recorder (main) window



The following describes the displayed items.

Web transaction file name:

Displays the name of the Web transaction file that stores the Web transaction that is being edited.

Web transaction name:

Displays the name of the Web transaction that is being edited.

Address:

Field for entering the URL of a Web page. When you enter a URL and then click the **Go** button or the **Enter** key, the page whose URL you have entered is displayed in the IE window section. To use an IP address to specify a host name, use an IPv4 dotted-decimal address (for example: `http://172.16.233.12/example.html`) or an IPv6 hexadecimal address enclosed in square brackets, using colons as separators (for example: `http://[ACE6:45:75:91::1]/example.html`).

Go button:

Displays in the IE window section the Web page whose URL was specified in **Address**.

IE window section:

Shows the Web page whose URL is set in **Address**. The IE window can be used in the same manner as with a normal browser.

Notes:

You should note the following about the IE mode:

- Your navigation operations in the IE window depend on the Internet Explorer settings on the machine where PFM - Agent for Service Response is installed. This means that if an application that affects Internet Explorer operations is running at the same time the Web transaction is being defined, the Web Recorder also picks up and records those effects.
- On the page displayed in the IE window, a script that controls the window itself (for instance, to resize it) may not function normally. A script that opens a new window to display a page can be executed. In such a case, the window is displayed in the same format as the IE window, and normal window components such as menus in Internet Explorer are not displayed. Even when a new window is opened from the IE window, you can continue recording the step information using that window.

Title:

Displays the title of the Web page that is displayed in the IE window.

URL list:

Displays the URLs of the recorded step information and the start and end points of scopes. You select items on this list to insert, edit, and delete step information, and to add and delete start and end points of scopes.

Start Scope and End Scope buttons:

Adds a start or end point to a scope. Clicking the **Start Scope** or **End Scope** button displays the Select Scope window. For details about the Select Scope window, see [7.2.5 Select Scope window](#).

The following table lists and describes the menu items in the Web Recorder (main) window.

Table 7–1: Menu items in the Web Recorder (main) window

Menu bar	Menu command	Function
File	Exit	Exits the Web Recorder (main) window.
Transaction	New	Displays the Create New Web Transaction window and starts recording of a new Web transaction. You specify a name for the Web transaction and the name of the storage file.
	Open	Displays the Select Web Transaction window in which you can select an existing Web transaction to be displayed or edited.
	Save	Saves the recorded or edited Web transaction information.
	Save As	Displays the Save As window for saving the recorded or edited Web transaction information under a different Web transaction name and storage file name.
	Delete Transaction[#]	Deletes the Web transaction's information from the storage file.
	Set Transaction	Displays the Set Web Transaction Conditions window in which you can display and edit settings for a Web transaction.
Edit	Insert	Displays the Properties window for inserting new step information. The new step is inserted above the step information for the URL selected in the URL list.
	Add Last	Displays the Properties window for adding new step information at the end of the URL list.
	Delete	Deletes the step information for the URL that is selected in the URL list.

Menu bar	Menu command	Function
Edit	Property	Displays the Properties window for displaying and editing the step information for the URL that is selected in the URL list.
Scope	Start Scope	Displays the Select Scope window for selecting the information at which a scope start point is to be set. The scope start point identifier is added above the URL that is selected in the URL list as the beginning of the scope.
	End Scope	Displays the Select Scope window for selecting the information at which a scope end point is to be set. The scope end point identifier is added below the URL that is selected in the URL list as the end of the scope.
	Delete Scope	Enables you to select, for deletion purposes, the start or end point identifier of a scope in the URL list. You can choose whether to delete the scope definition (both the start point and the end point) or to delete just the selected start or end point.
	Check Scope	Checks whether or not all scopes have corresponding start and end points.
View	Go	Displays the Web page whose URL is displayed in Address in the IE window.
Help	About	Displays the version information for the PFM - Agent for Service Response.

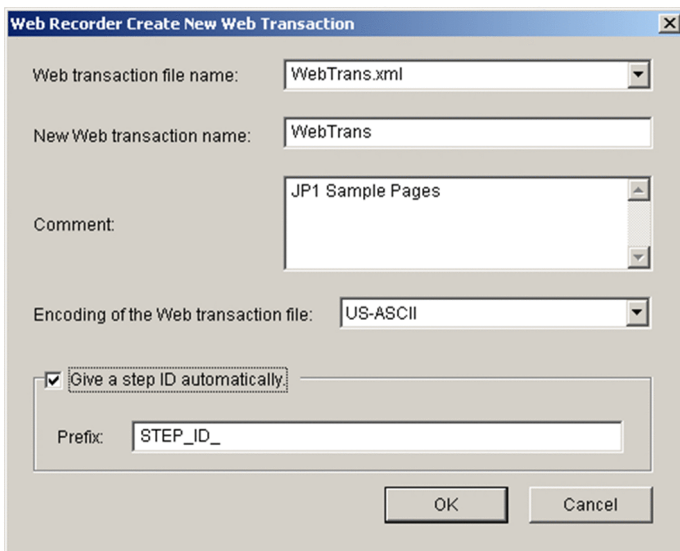
#

Deleting a Web transaction by choosing **Transaction** and then **Delete Transaction** does not delete the Web transaction file itself. To delete the Web transaction file, you must delete it directly.

7.2.2 Create New Web Transaction window

When a new Web transaction is to be created, this window is used to specify the name of the Web transaction file at the intended storage destination, and a name for the Web transaction. To display this window, in the Web Recorder (main) window, from the **Transaction** menu, choose **New**.

Figure 7–4: Create New Web Transaction window



The following describes the displayed items.

Web transaction file name:

Specifies the name of the Web transaction file at the storage destination (as up to 255 bytes). If the new Web transaction is to be saved in an existing Web transaction file, you can select that file's file name from the pull-down menu. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Web transactions to be measured can be saved in a single Web transaction file or different Web transaction files. Use either one according to the user's Web transaction management method.

Web transaction files are stored in the following folder:

```
installation-folder\agtv\probe\webtrans
```

New Web transaction name:

Specifies a name for the new Web transaction to be created (as up to 255 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. The vertical bar character (|) cannot be used in a Web transaction name. The specified Web transaction name must be unique within the specified Web transaction file.

Comment:

Specifies any comment of your choosing (as up to 255 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. This item can be omitted.

Encoding of the Web transaction file:

Specify the encoding of the web transaction file. From the pull-down menu, select **Shift_JIS**, **EUC-JP**, **ISO-2022-JP**, **UTF-8**, **US-ASCII**, or **GB18030**[#]. When on Japanese OS, **Shift_JIS** is selected by default, when on Chinese OS, **GB18030** is selected, and when the other OS, **US-ASCII** is selected.

The encoding you specified here is reflected in the XML declaration (i.e. the first line of the Web transaction file).

#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

Note:

When the Web Recorder automatically records the message body, it is recorded as it is (in other words, not encoded). Since PFM - Agent for Service Response records the page information (such as URL or the page title) in US-ASCII, the encoding of the page information in the Web transaction file can be inconsistent with the encoding you specified here.

In this case, modify the encoding of the page information part in the Web transaction file as you specify here.

Give a step ID automatically. check box

Select this check box if you automatically give step IDs to steps recorded in a newly created Web transaction file. This check box is selected by default.

The format of the automatically given step ID is concatenation of the string specified in the **Prefix** and five-digit number (zero padding). For example, when you specify **STEPID_** as the Prefix, the automatically give step IDs are:

```
STEPID_00001, STEPID_00002, ..., STEPID_99999
```

Prefix:

Specify the prefix of the step ID within the range from 1 to 250 alphanumeric characters, hyphen, underscore, and space characters. You are required to specify the prefix when you select the **Give a step ID automatically.** check box. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted

Note:

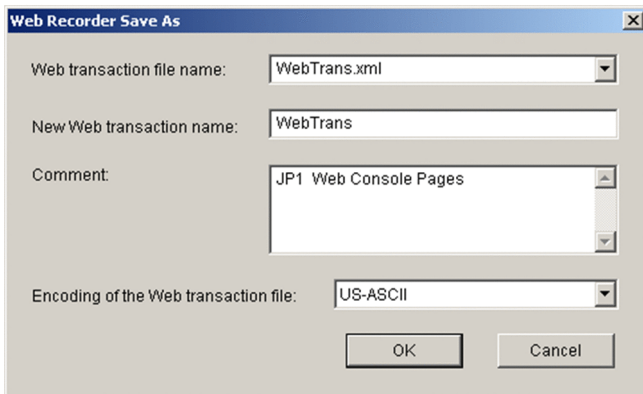
If you give a step ID automatically, note the following:

- The setting of **Give a step ID automatically.** applies only to the automatically recorded steps (i.e. the steps without step IDs) in the newly created transaction. Step IDs are not automatically given to manually inserted steps.
- If the sequence number reaches its maximum number (99999), step IDs are not given to the subsequent steps.

7.2.3 Save As window

The Save As window is used to save defined or edited Web transaction information under a new name. To display this window, in the Web Recorder (main) window, from the **Transaction** menu, choose **Save As**.

Figure 7–5: Save As window



The following describes the displayed items.

Web transaction file name:

Specifies the name of the Web transaction file at the storage destination (as up to 255 bytes). If the Web transaction is to be saved in an existing Web transaction file, you can select that file's file name from the pull-down menu. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. It is recommended that you store all Web transactions recorded for the same PFM - Agent for Service Response in the same Web transaction file. You should check that no Web transactions recorded for other PFM - Agent for Service Response programs are stored in the specified Web transaction file.

Web transaction files are stored in the following folder:

```
installation-folder\agtv\probe\webtrans
```

New Web transaction name:

Specifies a new name for the Web transaction (as up to 255 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. The vertical bar character (|) cannot be used in a Web transaction name. The specified Web transaction name must be unique within the specified Web transaction file.

Comment:

Specifies any comment of your choosing (as up to 255 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. This item can be omitted.

Encoding of the Web transaction file:

Specify the encoding of the Web transaction file. From the pull-down menu, select **Shift_JIS**, **EUC-JP**, **ISO-2022-JP**, **UTF-8**, **US-ASCII**, or **GB18030**[#].

The following describes the default value of this setting:

When you newly create a Web transaction:

Encoding specified in the Create New Web Transaction window.

When you open a file:

Encoding specified in the XML declaration.

The encoding you specified here is reflected in the XML declaration (i.e. the first line of the Web transaction file).

#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

Note:

When the Web Recorder automatically records the message body, it is recorded as it is (in other words, not encoded).

Reference note:

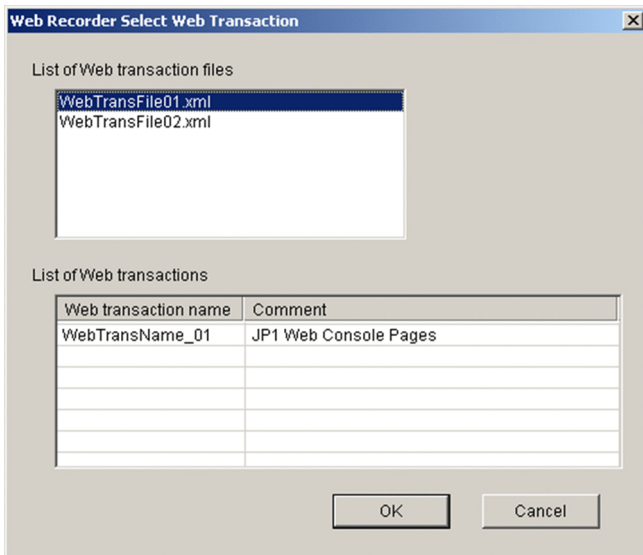
Since PFM - Agent for Service Response records the page information (such as URL or the page title) in US-ASCII, the encoding of this page information in the Web transaction file can be inconsistent with the encoding you specified here.

In this case, modify the encoding of the page information part in the Web transaction file as you specify here.

7.2.4 Select Web Transaction window

The Select Web Transaction window is used to select a Web transaction that is to be displayed or edited in the Web Recorder (main) window. To display the Select Web Transaction window, in the Web Recorder (main) window, from the **Transaction** menu, choose **Open**.

Figure 7–6: Select Web Transaction window



The following describes the displayed items.

List of Web transaction files:

Lists the names of the Web transaction files that are stored under *installation-folder*\agtv\probe\webtrans. In the Web Recorder (main) window, select the Web transaction file containing the Web transaction whose information you wish to display or edit.

List of Web transactions:

Lists the names of the Web transactions stored in the selected Web transaction file, and the comment that was specified for each listed Web transaction. Select the Web transaction that you wish to display or edit in the Web Recorder (main) window.

7.2.5 Select Scope window

When you wish to set a series of page transitions as a scope, you use the Select Scope window to define the scope by setting the scope start point and end point. To display this window, in the Web Recorder (main) window, from the **Scope** menu, choose **Start Scope** or **End Scope**. The following shows the Select Scope window.

Figure 7–7: Select Scope window



Start scope list or End scope list:

- When you select **Start Scope** on the **Scope** menu in the Web Recorder (main) window:
A list of scope names for which no start point has been set is displayed.
- When you select **End Scope** on the **Scope** menu in the Web Recorder (main) window:
A list of scope names for which the start point has been set, but no end point has been set, is displayed.

7.2.6 Set Web Transaction Conditions window

The Set Web Transaction Conditions window is used to set information about a Web transaction, such as information used to identify the transaction, proxy settings, SSL authentication[#], and overall information about the Web transaction's requests. To display this window, in the Web Recorder (main) window, from the **Transaction** menu, choose **Set Transaction**. This window consists of tabs for four pages:

- **Web Transaction Info** page
- **Request Info** page
- **Default Proxy** page
- **SSL Authentication** page[#]

#

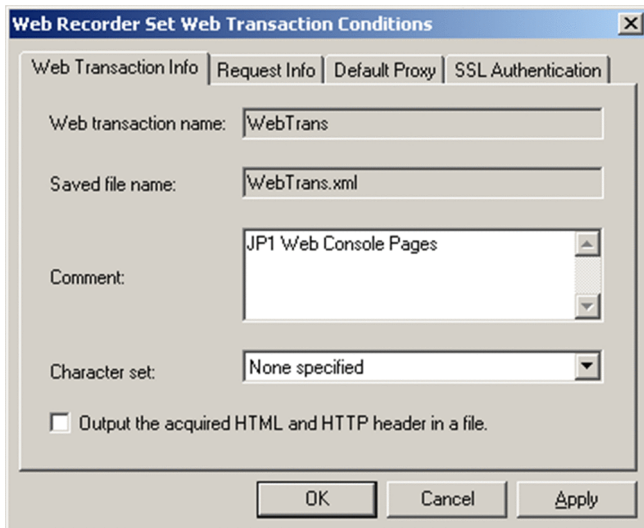
If you specify the SSL authentication settings, these settings are not applied when measuring.

The following subsections describe the items displayed on each page.

(1) Web Transaction Info page

The **Web Transaction Info** page displays identification information for the Web transaction. Each item on this page displays information that was specified when the Web transaction was created.

Figure 7–8: Set Web Transaction Conditions window (Web Transaction Info page)



The following describes the displayed items.

Web transaction name:

Displays the name of the subject Web transaction. This information cannot be changed.

Saved file name:

Displays the name of the Web transaction file that contains the subject Web transaction information. This information cannot be changed.

Comment:

Displays the comment that has been set for the subject Web transaction. This information can be edited (but must not exceed 255 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Character set:

Specify the default character set for the HTML file acquired in the Web transaction. If there are steps whose acquired HTML file that does not specify the character set, PFM - Agent for Service Response assumes its character set to be what you specify here.

From the pull-down menu, select **Shift_JIS**, **EUC-JP**, **ISO-2022-JP**, **UTF-8**, **GB18030[#]** or **None specified**. **None specified** is selected by default. Note that when you select **None specified**, it means *Shift_JIS* on Japanese OS, *GB18030* on Chinese OS, or *US-ASCII* on the other OS.

#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

Note:

If you mistakenly select the character set, the Web transaction monitoring may fail when you set the response determination condition or condition of variable string.

Reference note:

Regardless of the Character set setting, the Web transaction file is output in *Shift_JIS* on Japanese OS, *GB18030* on Chinese OS, or *US-ASCII* on the other OS.

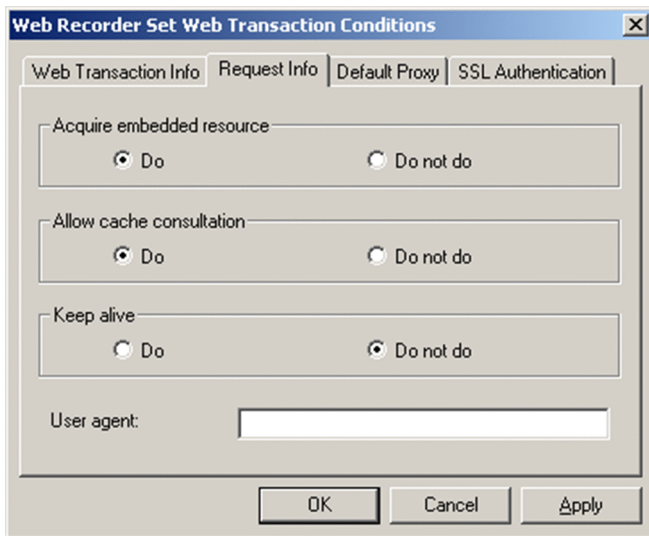
Output the acquired HTML and HTTP header in a file. check box

Select this check box when you output the acquired HTML and HTTP header in a file. This check box is not selected by default.

(2) Request Info page

The **Request Info** page is used to set overall information about the Web transaction's navigation requests.

Figure 7–9: Set Web Transaction Conditions window (Request Info page)



The following describes the displayed items.

Acquire embedded resource:

Enables you to select whether or not resources are to be acquired, such as images embedded in pages. The default is **Do**.

Allow cache consultation:

Enables you to select whether or not accessing the cache is to be permitted. The default is **Do**.

Keep alive:

Enables you to select whether or not the connection is to be kept active. The default is **Do not do**.

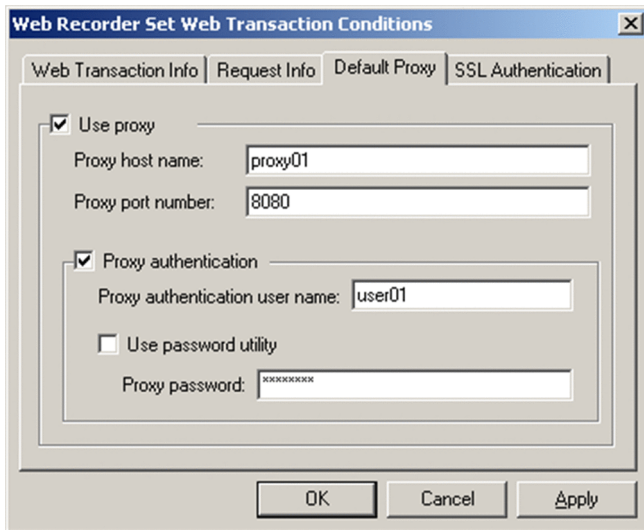
User agent:

Specifies (as up to 255 bytes) the `User-Agent` header to be used during Web transaction monitoring. The default is **PFM - Agent for Service Response (Windows)**. If this item is omitted, the default is used. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

(3) Default Proxy page

The **Default Proxy** page is used to set information related to use of a proxy. The information specified on this page becomes the default proxy settings for all the steps in the corresponding Web transaction.

Figure 7–10: Set Web Transaction Conditions window (Default Proxy page)



The following describes the displayed items.

Use proxy check box:

Specifies that a proxy is to be used. The default is that this check box is not selected.

Proxy host name:

Specifies the proxy's host name or IP address (as up to 255 bytes). When you have selected the **Use proxy** check box, you must specify this information. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. To specify an IPv4 address for the host name, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format using colons as separators (for example: ACE6:45:75:91::1).

Proxy port number:

Specifies the proxy server's port number, in the range 1 to 65535. When you have selected the **Use proxy** check box, you must specify this information.

Proxy authentication check box:

Specifies that proxy authentication is to be performed. The default is that this check box is not selected.

Proxy authentication user name:

Specifies a user name (as up to 64 bytes). When you have selected the **Proxy authentication** check box, you must specify this information. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Use password utility check box:

Specifies that the password utility is to be used to register a proxy password. The default is that this check box is selected. When this item is selected, the password must have been registered by the password utility. If you do not use the password utility, specify a password in **Proxy password**.

Proxy password:

If you have not selected the **Use password utility** check box, specify a password (as up to 64 bytes) that is to be used for proxy authentication. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Note:

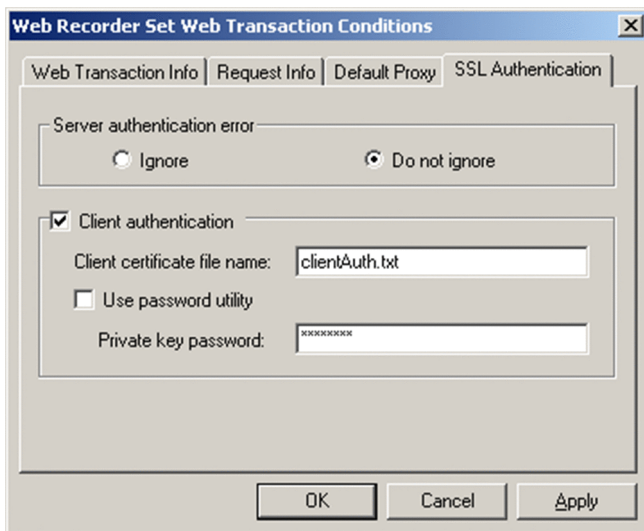
The password specified in **Proxy password** is stored as text in the Web transaction file, so Hitachi recommends that you use the password utility.

(4) SSL Authentication page

The **SSL Authentication** page is used to set information related to SSL authentication.

If you specify the SSL authentication settings, these settings are not applied when measuring.

Figure 7–11: Set Web Transaction Conditions window (SSL Authentication page)



The following describes the displayed items.

Server authentication error:

Enables you to select whether or not errors that occur during server authentication are to be ignored. The default is **Do not ignore**.

Client authentication check box:

Specifies that client authentication is to be performed. The default is that this check box is not selected.

Client certificate file name:

Specifies the file name of the client certificate file (as up to 255 bytes). If you have selected **Client authentication**, you must specify this information. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Use password utility check box:

Specifies that the password utility is to be used. The default is that this check box is selected. When this item is selected, the password must have been registered by the password utility. If you do not use the password utility, specify a password in **Private key password**.

Private key password:

If you have not selected the **Use password utility** check box, specify a private key password (as up to 1,023 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Note:

The password specified in **Private key password** is stored as text in the Web transaction file, so Hitachi recommends that you use the password utility.

7.2.7 Properties window

The Properties window is used to display, add, and edit the information for one step in the Web transaction. To display this window, in the Web Recorder (main) window, from the **Transaction** menu, choose **New**, or from the **Edit**, choose **Property**.

The Properties window consists of tabs for six pages:

- **Page Info** page
- **Request Info** page
- **Web Authentication** page
- **Proxy** page
- **Response Determination** page
- **Variable String** page

The following subsections describe the items displayed on each page. For details about the settings that are recorded automatically when new Web transaction information is created in the IE mode, and about the settings that must be specified when new Web transaction information is created or step information is inserted or added in the direct entry mode, see [4.4.1\(2\) Defining step information](#).

Note:

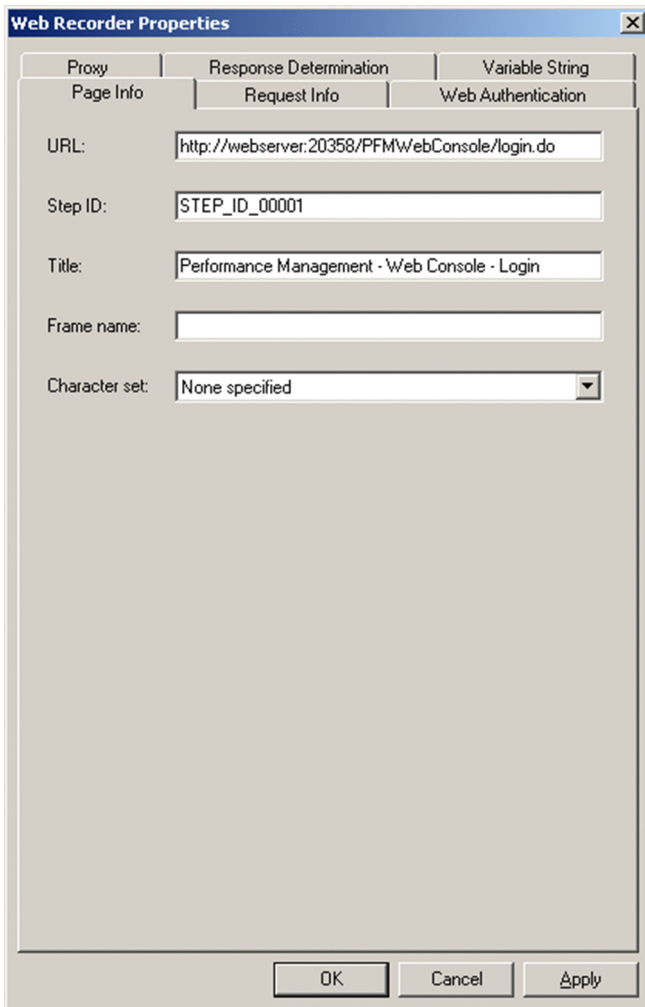
The message body is automatically recorded in the Web Recorder as it is, but the Web Recorder displays it in US-ASCII so that its display may be invalid.

(1) Page Info page

The **Page Info** page is used to set information about a Web page, such as the URL to be accessed, the step ID, the page title, the frame name, and the character set.

In the IE mode, the items on this page are recorded automatically.

Figure 7–12: Properties window (Page Info page)



The following describes the displayed items.

URL:

Specifies the URL of the Web page that is to be accessed (as up to 2,083 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. This item is mandatory. If recording is performed in the IE mode, the target URL is set automatically.

To specify an IPv4 address, use dotted-decimal format (for example: 172.16.233.12/example.html). To specify an IPv6 address, use hexadecimal format enclosed in square brackets, using colons as separators (for example: http://[ACE6:45:75:91::1]/example.html).

Step ID:

Specify the string to uniquely identify steps. You are required to specify the step ID if you are in any one of the following cases:

- The HTML file in this step includes the substitute string for the variable string after this step.
- Outputs the HTML file acquired in this step.

Specifies the step ID using alphanumeric characters, hyphen, underscore, and space in the range 1 to 255 bytes. Note that any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Title:

Specifies the target Web page's title (as up to 1,023 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. This item can be omitted. If recording is performed in the IE mode, the target page's title is displayed automatically.

Frame name:

When the target URL is a frame, this item specifies the name of the frame (as up to 1,023 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted. This item can be omitted. If recording is performed in the IE mode, the target frame name is displayed automatically.

Character set:

Specify the character set for the acquired HTML file. From the pull-down list, select **Shift_JIS**, **EUC-JP**, **ISO-2022-JP**, **UTF-8**, **GB18030[#]**, or **None specified**. **None specified** is selected by default. Note that when you select **None specified**, it means the character set specified in the Set Web Transaction Conditions window.

#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

Note:

If you mistakenly select the character set, the Web transaction monitoring may fail when you set the response determination condition or condition of variable string.

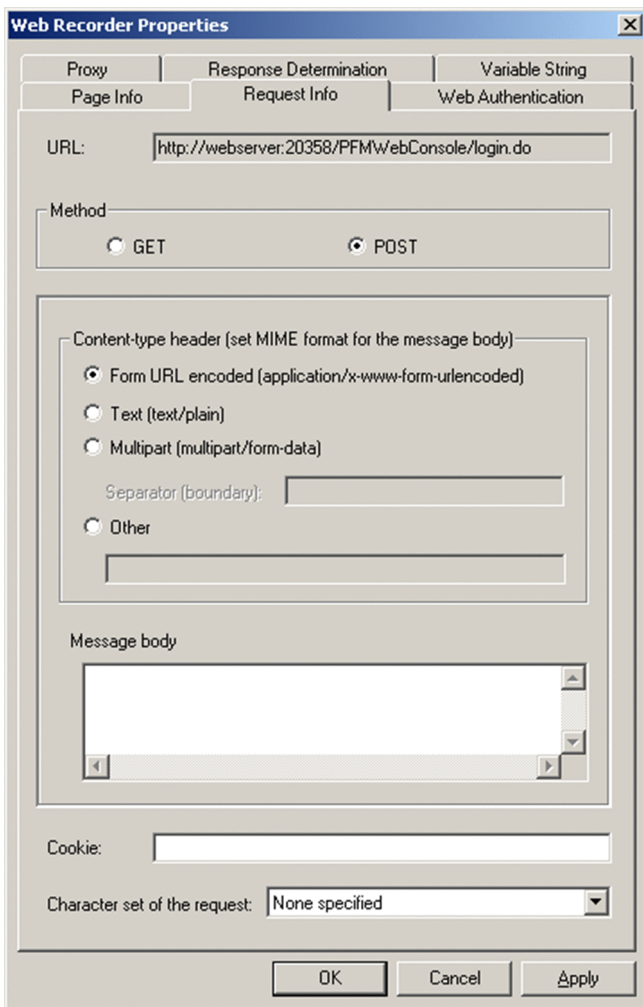
Reference note:

Regardless of the Character set setting, the Web transaction file is output in `Shift_JIS` on Japanese OS, `GB18030` on Chinese OS, or `US-ASCII` on the other OS.

(2) Request Info page

The **Request Info** page is used to set information about the request for step information. If recording is performed in the IE mode, all information except **Cookie** is recorded automatically.

Figure 7–13: Properties window (Request Info page)



The following describes the displayed items.

URL:

Displays the URL of the target Web page. To change this information, you must change the information in **URL** on the **Page Info** page.

Method:

Specifies the request method. The default is **GET**.

Content-type header:

Enables you to select one of the MIME formats listed below for the message body. This item is mandatory when **POST** is selected in **Method**.

- **Form URL encoded**
- **Text**
- **Multipart**
- **Other**

If you select **Multipart**, you must specify in **Separator** the delimiter that is to be used in the message body (as up to 255 bytes). If you select **Other**, you must specify in the field following **Other** a value for the Content-Type header that indicates the message body's MIME type (as up to 255 bytes).

Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Message body:

Specifies the text (as up to 512,000 bytes) that you wish to place in the message body when **POST** has been selected. If you selected **Multipart**, the character string specified in **Separator** under **Content-type header** is used to separate the parts. Even if you selected **Form URL encoded**, you enter the information here in text format; you do not have to enter it in the form URL encoded format. Do not omit specification of a value in **Message body** when you selected **POST** in **Method**. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Note:

You may include sensitive information in the message body, such as a password. Because this information is displayed as text on the screen, you must exercise caution in deciding what to include in the message body. The message body is also stored as text in the Web transaction file, so the Web transaction file must also be handled carefully.

Cookie:

Specifies a cookie header for the request. Normally, there is no need to set this item because PFM - Agent for Service Response uses the cookie acquired during monitoring as required. You should specify this information only when it is necessary.

The specification format is *variable-name=value*. To specify multiple sets (up to eight), use the semicolon (;) as the delimiter. The maximum length of a set is 1,023 bytes. Any spaces, tabs, or linefeed characters preceding or following an entered *variable-name=value* specification are deleted.

Character set of the request:

Specify the character set of the request information (such as URL, message body, and Cookie). Select from the drop-down list either of **Shift_JIS**, **EUC-JP**, **ISO-2022-JP**, **UTF-8**, **GB18030[#]**, or **None specified**. **None specified** is selected by default.

Note that when you select **None specified**, it means **Shift_JIS** on Japanese OS, **GB18030** on Chinese OS, or **US-ASCII** on the other OS.

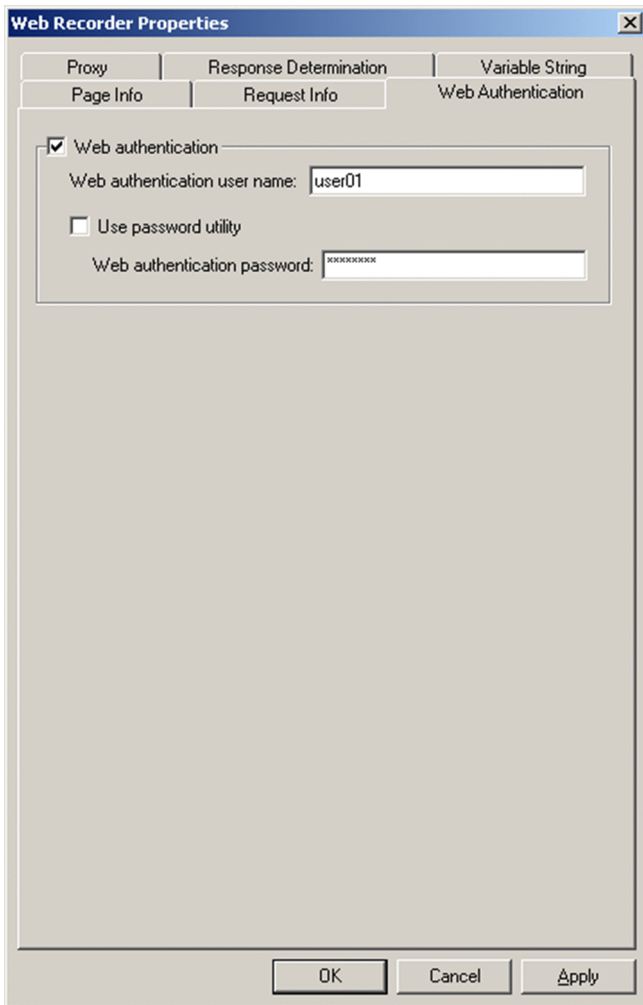
GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

(3) Web Authentication page

The **Web Authentication** page is used to set information needed for Web authentication. You need to specify this page if Web authentication will be required when a request is sent. Because the settings on this page are not recorded automatically even in the IE mode, you must always directly enter the settings on this page when they are needed.

If multiple steps exist for accessing a Web server that requires Web authentication, each step requires a setting for Web authentication.

Figure 7–14: Properties window (Web Authentication page)



The following describes the displayed items.

Web authentication check box:

Specifies that Web authentication is to be performed. The default is that this check box is not selected.

Web authentication user name:

Specifies the user name that is to be used for Web authentication (as up to 64 bytes). When you have selected the **Web authentication** check box, you must specify this information. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Use password utility check box:

Specifies that the password utility is to be used. The default is that this check box is selected. If you do not use the password utility, you must specify **Web authentication password**.

Web authentication password:

If you do not select the **Use password utility** check box, specify the password that is to be used for Web authentication (as up to 64 bytes). Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Note:

The password specified in **Web authentication password** is stored as text in the Web transaction file, so Hitachi recommends that you use the password utility.

(4) Proxy page

The **Proxy** page displays as the default settings the proxy utilization information that was set in the Set Web Transaction Conditions window for the Web transaction. To change settings for the step, manually enter the applicable items. Because the settings on this page are not recorded automatically even in the IE mode, you must directly enter any necessary settings on this page.

Figure 7–15: Properties window (Proxy page)

The screenshot shows the 'Web Recorder Properties' dialog box with the 'Proxy' tab selected. The dialog has three main sections: 'Proxy setting', 'Proxy host name', and 'Proxy authentication'. In the 'Proxy setting' section, three radio buttons are present: 'Use Web transaction's default proxy settings', 'Do not use proxy', and 'Use this setting value' (which is selected). Below this, the 'Proxy host name' is set to 'proxy01' and the 'Proxy port number' is set to '8080'. In the 'Proxy authentication' section, the 'Proxy authentication' checkbox is checked, and the 'Proxy authentication user name' is set to 'user01'. The 'Use password utility' checkbox is unchecked, and the 'Proxy password' field contains masked characters 'XXXXXXXXXX'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

The following describes the displayed items.

Proxy setting:

Enables you to select one of the three values listed below. The default is **Use Web transaction's default proxy settings**.

- **Use Web transaction's default proxy settings**
Specifies that the values specified in the Set Web Transaction Conditions window are to be used as the proxy settings.
- **Do not use proxy**
Specifies that no proxy is to be used.
- **Use this setting value**
Specifies that the values specified on this page (the **Proxy** page) are to be used as the proxy settings.

Proxy host name:

Specifies the target proxy server's host name or IP address (as up to 255 bytes). When you have selected **Use this setting value** in **Proxy setting**, you must specify this information. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

If an HTTP Web page is to be accessed, you can use an IPv4 or IPv6 address to specify the host name.

To specify an IPv4 address, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: ACE6:45:75:91::1).

Proxy port number:

Specifies the port number of the target proxy server. When you have selected **Use this setting value** in **Proxy setting**, you must specify this information.

Proxy authentication check box:

Specifies that proxy authentication is to be performed. The default is that this check box is not selected.

Proxy authentication user name:

Specifies a user name that is to be used for proxy authentication (as up to 64 bytes). When you have selected the **Proxy authentication** check box, you must specify this information. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Use password utility check box:

Specifies that the password utility is to be used. The default is that this check box is selected. If you do not use the password utility, specify a password in **Proxy password**.

Proxy password:

If you have not selected the **Use password utility** check box, specify a password (as up to 64 bytes) that is to be used for proxy authentication. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

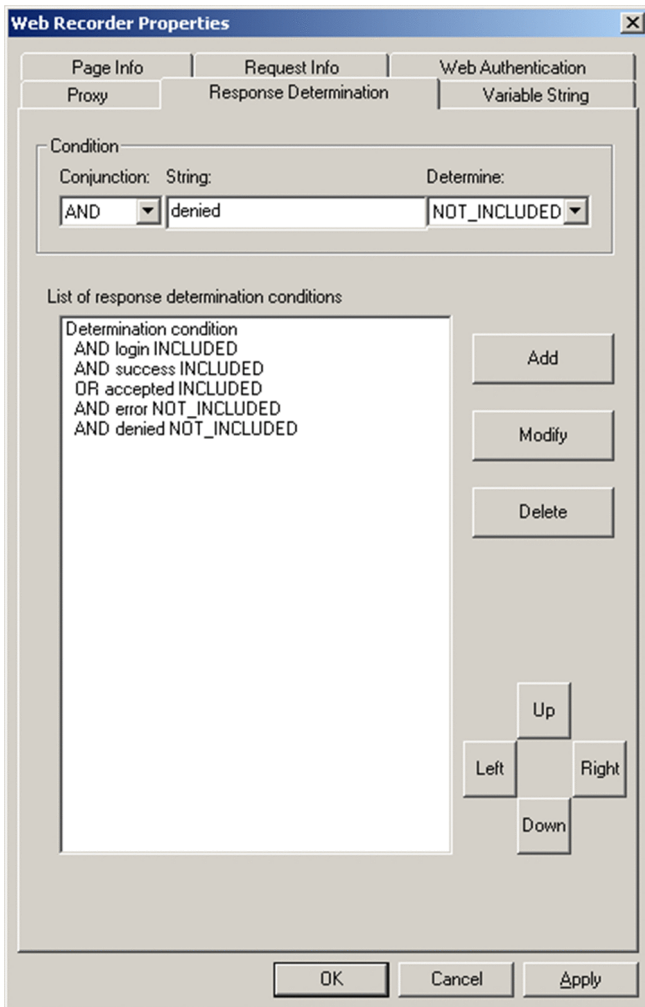
Note:

The password specified in **Proxy password** is stored as text in the Web transaction file, so it is recommended that you use the password utility.

(5) Response Determination page

The **Response Determination** page is used to specify conditions for determining whether or not a response is valid during Web transaction monitoring. Because the settings on this page are not recorded automatically even in the IE mode, you must directly enter any necessary settings on this page. Note that this response determination is applicable only to HTML texts.

Figure 7–16: Properties window (Response Determination page)



The following describes the displayed items.

Condition:

Specifies a condition for response determination.

Conjunction:

Select from the drop-down list the logical connector for this condition. Select **AND** or **OR**.

String:

Specifies a character string to be set as the condition. This character string cannot contain curly brackets ({}).

Determine:

Select **INCLUDED** or **NOT_INCLUDED** to specify whether or not to include the character string specified in **String**.

List of response determination conditions:

Lists in tree format the response determination conditions that have been specified. The top line on the list is always **Determination condition**. To add a condition at the beginning of the list, select **Determination condition** and then click the **Add** button.

Add button:

Adds the condition specified in **Condition** to the **List of response determination conditions**. The condition is added at the end of the hierarchical level that includes the condition selected in **List of response determination conditions**.

Modify button:

Changes the condition selected in **List of response determination conditions** to the values specified in **Condition**.

Delete button:

Deletes the condition selected in **List of response determination conditions**.

Move buttons (Up, Down, Right, and Left buttons):

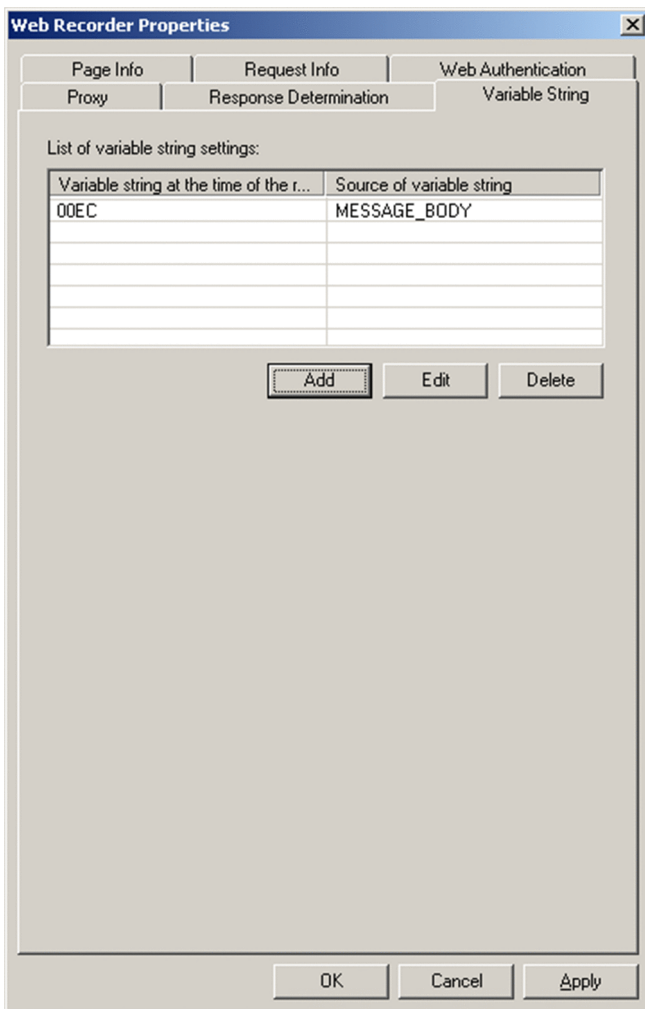
Enable you to modify the hierarchical structure of the conditions set in **List of response determination conditions**. You must select a condition in **List of response determination conditions** in order to use a move button.

- **Left button**
Shifts the selected condition and all those below it to the left by one tab, raising their level in the hierarchy.
- **Right button**
Shifts the selected condition and all those below it to the right by one tab, lowering their level in the hierarchy.
- **Up button**
Moves the selected condition and all those below it up in the hierarchy, so that they precede the immediately higher set of conditions at the same hierarchical level.
- **Down button**
Moves the selected condition and all those below it down in the hierarchy, so that they follow the immediately lower set of conditions at the same hierarchical level.

(6) Variable String page

The **Variable String** page is used to list the settings of the variable strings, which enable PFM - Agent for Service Response to support the dynamic session management.

Figure 7–17: Properties window (Variable String page)



The following describes the displayed items.

List of variable string settings:

The settings of the variable strings are listed. A combination of **Variable string at the time of the record** and **Source of variable string** is counted as one setting of a variable string and displayed in one line.

Note that when this page is displayed, none is selected.

Add button:

Add a new variable setting. When you click this button, the **Conditions of Variable String** window appears.

Edit button:

Edit the variable string setting selected in the **List of variable string settings**. When you click this button, the **Conditions of Variable String** window appears. If none is selected in the **List of variable string settings**, displays an error message.

Delete button:

Delete the variable string setting selected in the **List of variable string settings**. If none is selected in the **List of variable string settings**, displays an error message.

7.2.8 Conditions of Variable String window

The Conditions of Variable String window is used to set variable strings and substitute strings, which enable PFM - Agent for Service Response to support the dynamic session management. In the **Variable String** page in the Properties window, click the **Add** or **Edit** button this window appears. This window consists of tabs for two pages:

- **Variable String** page
- **Substitute String** page

In this window, the following button is displayed:

Import button

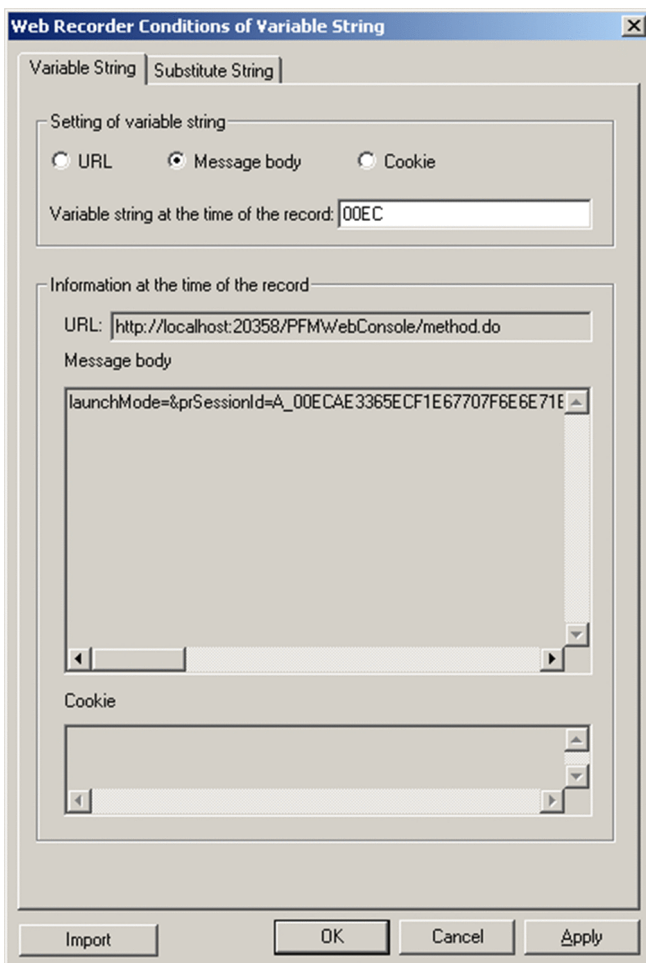
Imports the settings of the variable string and substitute string. You can import the settings of the variable strings and substitute strings defined in another step. When you click this button, the **Select Source of Variable String Settings** window appears. When you import the variable string settings, the corresponding substitute string settings are also imported.

The following subsections describe the items displayed on each page.

(1) Variable String page

The **Variable string** page is used to specify which part of the recorded URL, message body, or Cookie is the variable string.

Figure 7–18: Conditions of Variable String window (Variable String page)



The following describes the displayed items.

Setting of variable string:

Specifies the location containing a variable string and the variable string at the time of the record.

Location containing variable string

Select the location containing variable string from **URL**, **Message body**, or **Cookie**. **URL** is selected by default.

Variable string at the time of the record:

Specifies the variable string within the range from 1 to 4,095 bytes when recording. This is a required setting.

If there are multiple matched strings with the string specified in the **Variable string at the time of the record** in the URL, message body, or Cookie, the setting is applied to the first matching string from the beginning. If you substitute the other matched strings in the same way, it is recommended that you should replace the variable string part of the recorded URL, message body, or Cookie with \$VAR1\$, \$VAR2\$, or so. Modify the variable string part of the URL, message body, or Cookie in the Properties window of the modify target step.

Information at the time of the record:

Displays the information when recording.

Displays the URL, message body, or Cookie when recording on each section. You cannot edit this information.

(2) Substitute String page

The **Substitute String** page is used to specify the substitute string to substitute the variable string specified in the **Variable String** page.

Figure 7–19: Conditions of Variable String window (Substitute String page)

Web Recorder Conditions of Variable String

Variable String | Substitute String

From HTML or HTTP header

List of substitute string settings:

Step ID	Source of substit...	Element name or h...

Add Edit Delete

From Command

Command:

List of substitute string settings:

Step ID	Source of substit...	Element name or h...
STEP_ID_00001	HTML	INPUT
STEP_ID_00002	HTTP hrader	Set-Cookie

Add Edit Delete

URL encode at time of substitution.

Import OK Cancel Apply

The following describes the displayed items.

From HTML or HTTP header:

Select this to acquire the substitute string from the HTML file or HTTP header acquired earlier than this step.

List of substitute string settings:

Lists the settings of the substitute strings. When the **Substitute string** page appears, none is selected.

Note that when you specify the **From Command**, each substitute string setting is given as arguments to the command specified in the **Command** from top to bottom.

Add button

Add another substitute string. When you click this button, the Conditions of Substitute String window appears.

Note that when you specify the **From HTML or HTTP header** and already set the substitute strings, this button is deactivated.

Edit button

Edit the selected substitute string setting in the **List of substitute string settings**. When you click this button, the Conditions of Substitute String window appears. If you do not select the substitute string setting, displays an error message.

Delete button

Delete the selected substitute string setting in the **List of substitute string settings**. If you do not select the substitute string setting, displays an error message.

From Command:

Select this to acquire the substitute string from the command.

Command:

Specifies the absolute path name of the command and fixed arguments within the range from 1 to 4,095 bytes. When you specify the **From Command**, this is a required item. Note that any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted

Note:

It is recommended that you specify the path name of the command enclosed by double-quotation mark (").

The command may be able to be executed incorrectly if the path name of the command is not enclosed by double-quotation mark and the path name contains space characters.

List of substitute string settings:

Displays the list of substitute string settings. When the **Substitute String** page appears, none is selected.

Note that when you specify the **From Command**, each substitute string setting is given as arguments to the command specified in the **Command** from top to bottom.

Add button

Add another substitute string setting. When you click this button, the Conditions of Substitute String window appears.

Note that when you specify the **From HTML or HTTP header** and set substitute string settings, this button is deactivated.

Edit button

Edit the selected substitute string setting in the **List of substitute string settings**. When you click this button, the Conditions of Substitute String window appears. If you do not select a substitute string setting, displays an error message.

Delete button

Delete the selected substitute string setting in the **List of substitute string settings**. If you do not select the substitute string setting, displays an error message.

URL encode at time of substitution. check box

Select this check box if you URL-encode all the strings when substituting the substitute string for the variable string. If this check box is not selected, PFM - Agent for Service Response does not URL-encode. This check box is not selected by default.

The following shows that PFM - Agent for Service Response URL-encodes:

Substitute string	Encoding procedure
Alphanumeric characters	Not encoded
Following characters: * - . @ _	Not encoded
Space characters	Encoded into +
Characters not listed above	Encoded into three-character string in the format of %xy for each byte (x and y are the hex numbers with each one representing 4-bits)

Note:

When you specify the **From HTML or HTTP header**, you can set only one substitute string. When you specify the **Command**, you can set multiple substitute strings.

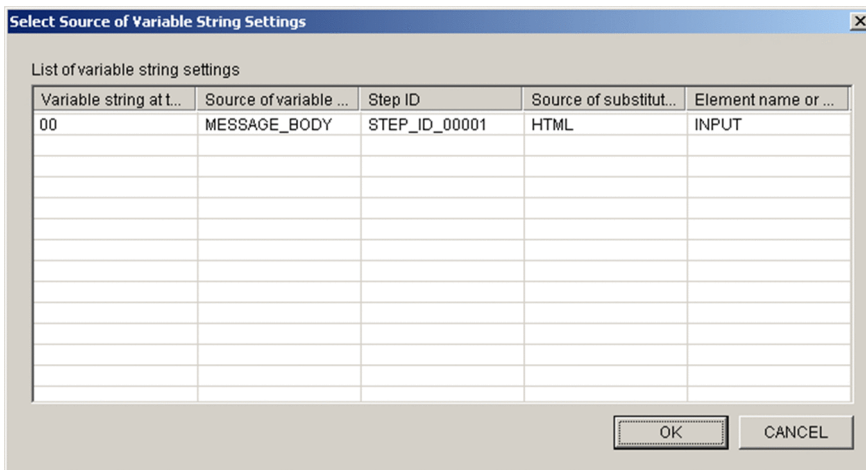
Reference note:

From HTML or HTTP header is selected by default.

7.2.9 Select Source of Variable String Settings window

The Select Source of Variable String Settings window is used to select the source of the variable string settings. This window appears when you click **Import** button in the **Conditions of Variable String** window.

Figure 7–20: Select Source of Variable String Settings window



The following describes the displayed items.

List of variable string settings:

Lists the variable string settings and their corresponding substitute string settings. The settings defined in another steps are also listed. When this window appears, none is selected.

When you select a variable string setting and click the **OK** button, the selected settings are imported and the settings in the **Conditions of Variable String** window are updated.

7.2.10 Conditions of Substitute String window

The Conditions of Substitute String window is used to identify the substitute strings. This window appears when you click **Add** button or **Edit** button in the **Substitute String** page in the Conditions of Variable String window.

Figure 7–21: Conditions of Substitute String window

Web Recorder Conditions of Substitute String

Step ID: STEP_ID_00001

Source of substitute string

From HTML

HTML element including substitute string

Element name: INPUT

Filtering conditions

List of filtering conditions

Type of element	Value of attribute or...	
Attribute	type="hidden"	Add
Attribute	name="session_id"	Edit
		Delete

When there are multiple matched elements, Use 1 th match.

Where to include substitute string

Content Attribute Attribute name: value

From HTTP header

Header name: Value of header:

String to exclude from substitute string

String just before: abc String just after:

Import OK Cancel

The following describes the displayed items.

Step ID:

Select the step ID. In the pull-down list, the step IDs of the recorded steps are listed. None is selected by default. You are required to select this item.

Source of substitute string:

Select the source of substitute string.

To acquire the substitute string from HTML:

Specify the **From HTML**. For details about the settings, see *(1) Settings to acquire the substitute string from HTML*.

To acquire the substitute string from HTTP header:

Specify the **From HTTP header**. For details about the settings, see *(2) Settings to acquire the substitute string from HTTP header*.

The **From HTML** is specified by default.

String to exclude from substitute string check box:

Select this check box when there is a string to exclude from the acquired substitute string. This check box is not selected by default.

When you select this check box, specify either or both **String just before** and/or **String just after**.

String just before:

Specify the **String just before** when there is a string to exclude before the acquired string. If there are multiple matched strings, first match from the top is excluded. Specify this item within the range from 1 to 255 bytes. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

If you specify the **Attribute** in the **Where to include substitute string**, you cannot specify double or single quotation marks (", '), because double or single quotation marks are the separators for attribute values.

String just after:

Specify the **String just after** when there is a string to exclude before the acquired string. If there are multiple matched strings, first match from the bottom is excluded. Specify this item within the range from 1 to 255 bytes. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

If you specify the **Attribute** in the **Where to include substitute string**, you cannot specify double or single quotation marks (", '), because double or single quotation marks are the separators for attribute values.

Import button:

Import the substitute string settings. You can import the substitute string setting of another step. When you click this button, the Select Source of Substitute String Settings window appears.

(1) Settings to acquire the substitute string from HTML

This subsection describes the settings when you specify the **From HTML** in the **Source of substitute string**.

From HTML:

Specify this button when you acquire the substitute string from HTML. You specify an element name to contain the substitute string, a filtering condition, a condition to choose one from multiple matched elements.

Element name:

Specify the element name to contain the substitute string within the range from 1 to 1,023 bytes. If you specify the **From HTML**, this is a required setting. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

Filtering conditions:

Specify the condition to filter the matched elements if there are multiple matched elements. Specify the necessary conditions using the **Add**, **Edit**, and **Delete** button. The **List of filtering conditions** displays the filtering conditions.

- **Add** button
Add a filtering condition to filter matched elements. When you click this button, the Filtering Conditions window appears.
- **Edit** button
- Edit the selected filtering condition in the **List of filtering conditions**. When you click this button, the Filtering Conditions window appears. If you do not select a filtering condition, displays an error message.
- **Delete** button
Delete the selected filtering condition in the **List of filtering conditions**. If you do not select a filtering condition, displays an error message.

When there are multiple matched elements, Use *n* th match.

Specify the *n* th match to contain the substitute string counting from the top within the range from 1 to 1,023 when there are multiple matched elements that match the **Element name** and **Filtering conditions**. The default value is 1. If you do not specify, the substitute string is acquired from the first match from the top.

Where to include substitute string:

Specify the source of the substitute string from the **Content** or **Attribute**. The **Attribute** is selected by default.

Content:

Specify this button when the content of the element contains the substitute string.

Attribute:

Specify this button when the attribute value of the element contains the substitute string. When you specify this button, you are required to specify the **Attribute name**.

In the **Attribute name**, you specify the *attribute name* within the range from 1 to 1,023 bytes.

You cannot use = to specify the *attribute name*. The **Attribute name** is not case sensitive. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

(2) Settings to acquire the substitute string from HTTP header

This subsection describes the settings when you specify the **From HTTP header** in the **Source of substitute string**.

Header name:

Specify the header name of the HTTP header within the range from 1 to 1,023 bytes.

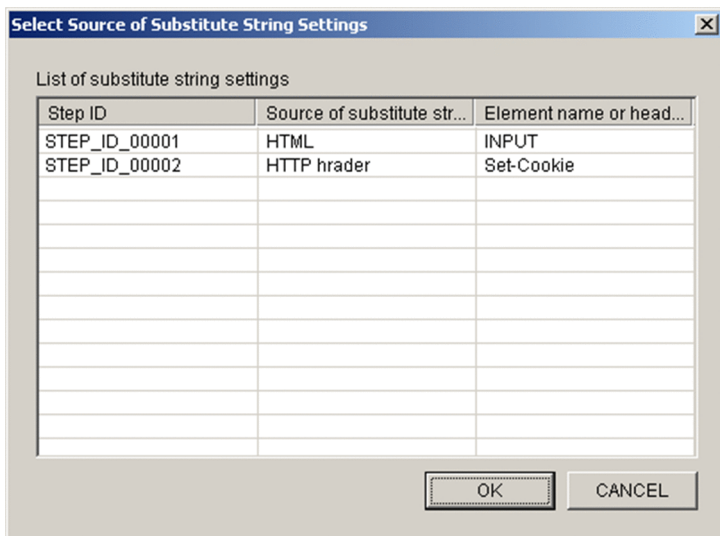
Value of header:

Specify the value of the HTTP header within the range from 1 to 4,095 bytes.

7.2.11 Select Source of Substitute String Settings window

The Select Source of Substitute String Settings window is used to select the source to import the substitute settings. This window appears when you click **Import** button in the **Conditions of Substitute String** window.

Figure 7–22: Select Source of Substitute String Settings window



The following describes the displayed items.

List of substitute string settings

Displays the list of the substitute string settings. The substitute string settings of other steps are displayed.

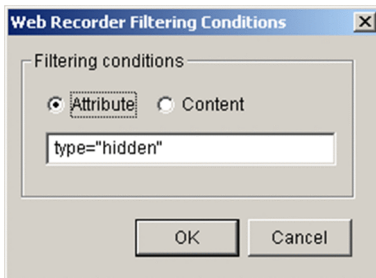
When this window appears, none is selected.

When you select a substitute string setting and click the **OK** button, the selected settings are imported and the settings in the Conditions of Substitute String window are updated.

7.2.12 Filtering Conditions window

The Filtering Conditions window is used to specify the condition to filter the matched elements. This window appears when you click the **Add** or **Edit** button in the **Filtering conditions** in the **Conditions of Substitute String** window.

Figure 7–23: Filtering Conditions window



The following describes the displayed items.

Filtering conditions:

Specify the condition to filter the matched elements from the **Attribute** or **Content**.

When you specify the **Attribute**:

Specify the element attribute of the element to contain the substitute string within the range from 1 to 1,023 bytes in the following format: *attribute name=attribute value*.

The *attribute name* part is not case sensitive. The *attribute value* part is case sensitive.

Do not specify the attributes to change dynamically. Note that PFM - Agent for Service Response do not verify the validity of the *attribute name* and *attribute value*. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

When you specify the **Content**:

Specify the string to be included by the content of the element containing the substitute string within the range from 1 to 1,203 bytes. Any spaces, tabs, or linefeed characters preceding or following the entered character string are deleted.

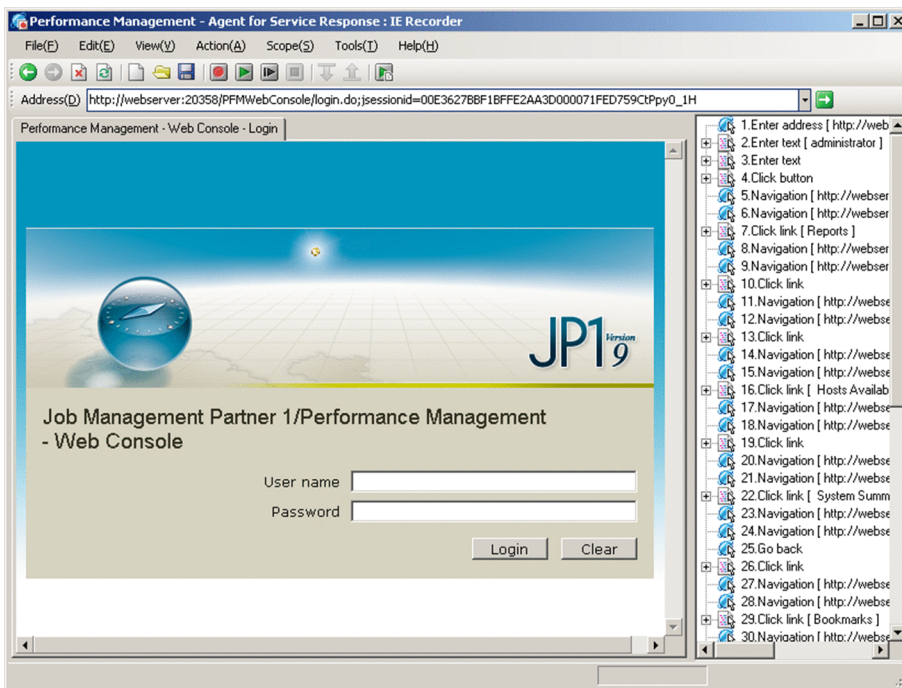
7.3 IE Recorder windows

IE Recorder provides windows for defining as IE scenarios a series of Web access operations using Internet Explorer, as well as windows for defining necessary informations. This section describes each IE Recorder window.

7.3.1 IE Recorder (main) window

The IE Recorder (main) window is used to define an IE scenario. This window is provided in three modes: the record mode, edit mode, and replay mode. The record mode is used to define a series of Internet Explorer operations on the screen as an IE scenario. The edit mode is used to edit an IE scenario. The replay mode is used to replay an IE scenario and measure the response time.

Figure 7–24: IE Recorder (main) window



The following describes the displayed items.

Titlebar:

Displays the title of the IE Recorder and the filename of the IE scenario displayed on the IE Recorder (main) window.

Toolbar:

Frequently used functions on the IE Recorder (main) window are placed as buttons.

Go Back button

Displays the previously-viewed URL in the browser history in the IE window section.

Go Forward button

Displays the subsequently-viewed URL in the browser history in the IE window section.

Stop button

Stops rendering the page in the IE window section.

 **Refresh** button

Refreshes the page in the IE window section.

 **New** button

Creates a new IE scenario.

 **Open** button

Opens an existing IE scenario file and displays the IE scenario.

 **Save** button

Saves the recorded or edited IE scenario.

 **Record** button

Records the IE scenario.

 **Replay** button

Replays the IE scenario.

 **Replay by Step** button

Replays the IE scenario by step.

 **Stop Recording/Relaying** button

Stops recording or replaying the IE scenario.

 **Set Start Scope** button

Displays the Start Scope Settings window for selecting the scope as a start point. The start-point scope is added in front of the selected operation in the Operation list.

 **Set End Scope** button


Displays the End Scope Settings window for selecting the scope as an end point. The end-point scope is added behind the selected operation in the Operation list.

 **Measurement Test** button

Replays the recorded IE scenario and conducts the measurement test.

Addressbar:

Displays the content of the navigation in the IE window section (i.e. URL). This addressbar does not hold the browser history. The drop-down list shows the URLs defined in the IE Recorder action condition definition file.

When you enter a URL and then click the  button or press the **Enter** key, the page whose URL you have entered is displayed in the IE window section.

 **Go** button

Displays the URL page you entered in the **Address** the IE window section.

To use an IP address to specify a host name, use an IPv4 dotted-decimal address (for example: `http://172.16.233.12/example.html`) or an IPv6 hexadecimal address enclosed in square brackets, using colons as separators (for example: `http://[ACE6:45:75:91::1]/example.html`).

IE window section:

Displays the URL page you entered in the **Address**. In the IE window section, you can operate in the same way you operate the Internet Explorer. Note that if you use the keyboard operation an IE scenario can be recorded improperly. It is recommended that you use the mouse operation in the IE window section. On the tabs, the page title is displayed. When a new window is displayed while you operate in the IE window section, a tab to display that window is automatically added. If you use the script to close the window, the tab is closed. However, when there is only one tab, you cannot close the tab.

The following table shows the result of the operations in relation to the number of tabs:

Table 7–2: Result of operations in relation to number of tabs

No.	Number of tabs in the IE window section	Operation	Result of operation
1	1 #1	Open window #2	Add a new tab to render the content of the new window.
2		Close window	Immediately after close the tab, add a new tab displaying a blank page.
3	More than 1	Open window #2	Add a new tab to render the content of the new window.
4		Close window	Close a tab. Which tab to close depends on the script.
5		Close tab	Close the tab. When you click View menu and then Close Tab, close the active tab. When you close tab from the context menu, close the tab which you have clicked.

Notes:

- These operations do not change the mode of the IE Recorder window.
- You cannot add a new tab from the menu.

#1:

When there is only one tab, you cannot close the tab.

#2:

To `open window` in the IE window section means:

- Click the link with the **Shift** key down.
- Click the link whose value of the `target` attribute is `_blank`.
- Open window by using scripts.

#3:

To `close window` in the IE window section means:

- Close window by using scripts.

Note:

You should note the following when you define IE scenarios:

- Your navigations operations in the IE window section depend on the Internet Explorer settings on the machine where PFM - Agent for Service Response is installed. This means that if an application that affects Internet Explorer operations is running when you define IE scenarios that application may affect the IE Recorder also picks up and records these effects.
- On the page displayed in the IE window, a script that controls the window itself (for instance, to resize it) may not function normally. However, a script that opens a new window to display a page can be executed.

Operation list:

Lists in the tree format the recorded operational information, the start scopes, and the end scopes.

The display format of the operation list is as follows:

```

Operation List
+--Tag info
|   +--Tag name:tag-name
|   +--Attributes
|   |   +-- attribute-name=attribute-value
|   |   ...

```



```

|      +--Inner text:contents-of-inner-text
|      +--Tag position
|      |      +--Within the same tag:nth-occurrence-within-the-same-tag
|      |      +--Within the same inner text:nth-occurrence-within-the-same-
inner-text
|      +--Same tag count:number-of-the-same-tags
|      +--Same inner text count:number-of-the-same-inner-text
|      +--Page transition:Occurred or Not occurred

```

Scope information is displayed on the operation list. The display format of the scope information is as follows:

```

+operations-information-1
+start-scope-information
+operations-information-2
+end-scope-information
+operations-information-3

```

Operational Information

Information of each operation is displayed in the below format:

```










operation-icon operation-number operation-name value










```

Operation number is the number assigned among the operations within the operation list. Operation number starts from 1 and are assigned to each operation from the top operation. If you delete an operation, operation numbers are re-assigned automatically from the top operation. Note that operation numbers are not assigned to scopes.

Among the operational information displayed in the Operation list, the following table lists shows the operation icons, operation names, and its values:

Table 7–3: Operation information in the Operation list

Operation icon	Operation name	Value	Description
	Click link	The value of the inner text	Clicking links on the page in the IE window.
	Enter text	The value of the entered text in the text box (the password is not displayed)	Entering texts in the text box on the page in the IE window.
	Select check box	The value of the inner text	Selecting check boxes or radio buttons on the page in the IE window.
	Select value	The value of the inner text	Selecting drop-down list on the page in the IE window.
	Click button	The value of the inner text	Clicking buttons on the page in the IE window.
	Enter address	The entered URL	Entering URL on the addressbar in the IE window, and then clicking  button or pressing the Enter key.
	Go forward	--	From the menu in the IE window selecting Go forward , or clicking  button.

Operation icon	Operation name	Value	Description
	Go back	--	From the menu in the IE window selecting Go back , or clicking  button.
	Refresh	--	From the menu in the IE window selecting Refresh , or clicking  button.
	Navigation	The URL of the accessed page	Operations representing the URL access. Note that the Navigation operations are not Click link operations. Rather, the Navigation operations are the URL access operations without entering the URLs in the addressbar or so.
	Close tab	The page title on the tab	Closing the tab in the IE window.
	Popup dialog box	--	Operations in the pop-up dialog box when you operate in the IE window.
	<i>Tag-name tag</i>	--	Operations of the tags which the IE Recorder can record by default but are not listed above (except, for instance, Click link or Enter text).
	<i>user-defined-operation-name</i>	--	Operations which users defined. You can define the user-defined operation names by registering in the IE Recorder action condition definition file (jpcvierec.conf).

Legend:

--: None

Tag info:

Tag info displays the information when recording is done. The following table shows the contents of the Tag info in the Operation list:

Table 7–4: Tag info displayed in Operation list

Displayed information		Description
Tag name		Tag name when recording is done.
Attributes		Attributes of the tag. If the tag has multiple attributes, displays all the attributes. Attributes with the default values are displayed although not defined in the HTML file.
Inner text		Displays the inner text (the string between the start tag and the end tag).
Tag position	Within the same tag	Displays the <i>n</i> th occurrence among the same tag in the HTML file.
	Within the same inner text	Displays the <i>n</i> th occurrence among the tags with the same inner text.
Same tag count		Displays the number of the same tags in displayed in the Tag name of the HTML file. This count includes the operation-target tag itself.
Same inner text count		Displays the number of the tags with the same inner text. This count includes the operation-target tag itself.
Page transition		Displays whether the page transition occurred. If occurred, <code>Occurred</code> is displayed. If not, <code>Not occurred</code> is displayed. ^{#1}

#1

Always display Not occurred.

Statusbar:

Displays the operation status, the page processing status, and the mode of the IE Recorder.

Operation status:

Displays the same information when you operate Internet Explorer. For example, displays Done when the page rendering is completed, and displays the linked URL when the mouse is over the link.

Page processing status:

Display the page processing status of the page in the IE window in a progressbar.

Mode of the IE Recorder:

The displayed information depends on the mode:

- Edit Mode
Displays none.
- Record Mode
Displays Recording Mode.
- Replay Mode
Displays Replay Mode.

The following table lists the shows the menu items in the IE Recorder (main) window:

Table 7–5: Menu items in the IE Recorder (main) window

Menu bar	Menu command	Function	
File	New	Creates a new IE scenario.	
	Open	Opens the existing IE scenario file and display the IE scenario.	
	Save	Saves the recorded or edited IE scenario.	
	Save As	Saves the recorded or edited IE scenario under a different storage file name.	
	Exit	Exits the IE Recorder (main) window.	
Edit	Delete	Delete one operation selected in the Operation list.	
	Delete All Operations after the Selected Operation	Deletes all operations after the selected operation in the Operation list.	
	Operation Settings	Displays the Operation Settings window where you can see and edit the settings. Edit the settings when the target HTML file is modified after recording or when the IE scenario cannot be replayed properly.	
	Change Password	Displays the Change Password window where you can change the password when the IE scenario is recorded. For details about the kind of passwords you can change, see <i>7.3.3 Change Password window</i> .	
	IE Recorder Settings	Displays the IE Recorder Settings window where you can change the settings about recording and replaying the IE scenario.	
View	Go To	Back	Displays the previously-viewed URL in the browser history in the IE window section.
		Forward	Displays the subsequently-viewed URL in the browser history in the IE window section.
		Home Page	Displays the home page in the IE window section.

Menu bar	Menu command	Function
View	Stop	Stops rendering the page in the IE window section.
	Refresh	Refresh the page in the IE window section.
	Source	Displays the HTML source code of the currently viewed page. If the currently viewed page does not contain HTML source code, displays none. You can display the source code even if the page forbids displaying the source code.
	Close Tab	Closes the tab in the IE window section.
Action	Record	Records the IE scenario. If you already recorded one or more operations, adds operations to the existing record.
	Replay	Replays the IE scenario. Use this when you check whether the IE scenario is properly replayed.
	Replay by Step	Replays the IE scenario by step. As you watch the IE scenario step by step, you can check the replayed page and the next operation-target link.
	Stop	Stops recording or replaying the IE scenario.
	Set Breakpoint	Sets breakpoint in the selected operation. You can set multiple breakpoints. Use breakpoints when you stop the IE scenario on the way to check the IE scenario.
	Delete Breakpoint	Deletes breakpoint. Note that you cannot resume replaying when you delete breakpoint of the operation which you paused while you replayed IE scenario.
	Measurement Test	Replays the recorded IE scenario and starts measurement. Use this test when you check the guideline threshold value, the timeout value, the factors of replay failure.
Scope	Set Start Scope	Displays the Start Scope Settings window to set the start scope. Add the selected start scope in front of the selected operation in the Operation list.
	Set End Scope	Displays the End Scope Settings window to set the end scope. Add the selected end scope behind the selected operation in the Operation list.
	Delete Scope	Deletes the selected scope in the IE scenario.
	Rename Scope	Renames the name of the selected scope.
	Scope List	Displays the list of scopes.
Tools	Simplified Registration	Registers the measurement conditions to the measurement condition registration file, based on the information of the currently displaying IE scenario. Before you register the measurement conditions, make sure that you stop PFM - Agent for Service Response in advance. If the IE scenario file exists, the following measurement condition is added to the measurement condition registration file: TASKID: the lowest and unused task ID is given. TASKLABEL: IE_Scenario-Task-ID (Task-ID is replaced by the value of TASKID) INTERVAL: 180 TIMEOUT: 30 IESCENA_FILE: IE-scenario-file-name
	Edit esptask.xml	Opens and edits the measurement condition registration file by the text editor. When you edit the measurement condition registration file, make sure that you stop PFM - Agent for Service Response.
	Internet Options	Displays the Internet Properties dialog box in the IE windows.
Help	About	Displays the version information for the PFM - Agent for Service Response.

Note:

If you edit the measurement condition registration file on the PFM - Web Console, you do not need to stop PFM - Agent for Service Response in advance. Therefore, it is recommended that you edit the measurement condition registration file on the PFM - Web Console.

Behavior when replaying IE scenarios

The replaying operation is highlighted when you replay IE scenarios.

- **Replay**
The next operation is highlighted when each recorded operation is replayed.
- **Replay by step**
The next operation is highlighted and stops replaying each time you replay by step.
- **Replay until breakpoint**
The operation after the breakpoint is highlighted when replaying stops.
- **While replaying, you change the filtering condition or tag position on the Operation Target page on the **Operation Settings** window.**
Change the highlighted operation. If the target operation does not exist after the change, turn highlight off.

Accelerator keys for IE Recorder cannot be used when the Internet Explorer window is active

In some cases, you cannot use some accelerator keys for IE Recorder menubar while the Internet Explorer window is active. This is because the setting of turning shortcuts off takes precedence when an Internet Explorer window is active.

The following table lists the accelerator keys turned off when the Internet Explorer setting takes precedence. For details about the shortcut keys in Internet Explorer, see Internet Explorer help.

Table 7–6: Accelerator keys turned off due to the Internet Explorer setting

Accelerator keys turned off	IE Recorder operation in Internet Explorer 8 to 11
<u>F</u> ile	Y
<u>E</u> dit	Y
<u>V</u> iew	N
<u>A</u> ction	Y
<u>S</u> cope	N
<u>T</u> ools	N
<u>H</u> elp	Y

Legend:

- Y: Available
- N: Unavailable
- <ALT key + [Key]>: Shortcut [Key] for IE

Note:

The availability of the accelerator keys might vary due to:

- The Service Pack for Internet Explorer, Service Release for Internet Explorer, Windows Update, or so.
- The HTML documents or the scripts.
- The Add-ons (ActiveX components, BHO (Browser Helper Object), or so) or so.

7.3.2 Operation Settings window

The Operation Settings window is used to set configurations for the recorded operations. The window title and the currently edited operation name are displayed on the titlebar. To display this window, in the IE Recorder (main) window, from the **Edit** menu, choose **Operation Settings**. This window consists of tabs for three pages:

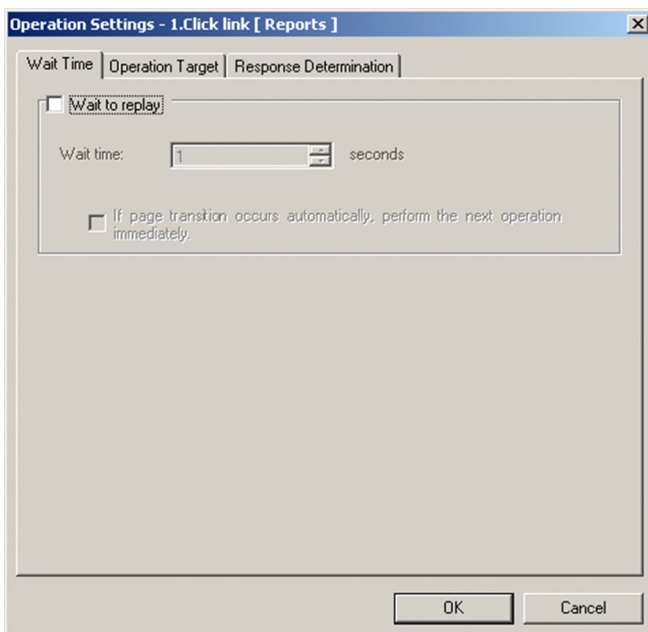
- **Wait Time** page
- **Operation Target** page
- **Response Determination** page

The following subsections describe the items displayed on each page.

(1) Wait Time page

The **Wait Time** page is used to set the wait time to replay the operations.

Figure 7–25: Operation Settings window (Wait Time page)



The following describes the displayed items.

Wait to replay check box

Specify this check box when you set the wait time to replay the operations. This check box is not selected by default.

Wait time:

Specify the wait time within the range from 1 to 600 seconds.

If **Wait to replay** check box is not selected, the wait time is set to 0. If you specify the decimal fraction, truncate the value at the decimal point. If none is specified, the wait time is reset to the previous value.

Specify the **Wait time** when you specify the wait time to replay the next operation. For browser navigation operations, the specified time is the time to wait for the completion of moving to the URL page that is recorded. For other operations, the specified time is the time to wait until operation execution starts. This wait time can enable you to monitor the Web pages that do not complete these page transition or the Web pages whose page transitions are not detected.

For example, the next operations are carried out immediately after the pages are displayed on the IE Recorder's measurement tests or replaying by IE probe. Yet, since there must be time lags, in reality, when you carry out

the next operation after the page is displayed there is a great difference between the time you record the IE scenario and the time takes IE Recorder's measurement tests or replaying by IE probe. In this case, measurement tests or replaying by IE probe become similar to real situations if you specify **Wait time** to, for example, the Click Link operation. Note that no notification window or message is displayed even if the specified wait time is exceeded.

The following table lists the default status of items on the **Wait time** page:

Table 7–7: Default status of items on Wait time page

No.	Operation		Item	Status
1	HTML operation		Waits to replay	--
			Wait time [#]	T1
			If page transition occurs, automatically performs the next operation immediately.	--
2	Browser operation	Enter address	Waits to replay	--
3			Wait time [#]	T1
4			If page transition occurs, automatically performs the next operation immediately.	--
5		Go forward/ Go back	Waits to replay	--
6			Wait time [#]	T1
7			If page transition occurs, automatically performs the next operation immediately.	--
8		Refresh	Waits to replay	--
9			Wait time [#]	T1
10			If page transition occurs, automatically performs the next operation immediately.	--
11		Navigation	Waits to replay	Y
12			Wait time [#]	T1+10
13			If page transition occurs, automatically performs the next operation immediately.	Y
14		Close tab	Waits to replay	--
15			Wait time [#]	T1
16			If page transition occurs, automatically performs the next operation immediately.	--
17		Dialog operation	Popup dialog box	Waits to replay
18	Wait time [#]			Deactivated
19	If page transition occurs, automatically performs the next operation immediately.			Deactivated

Legend:

Y: Selected by default

--: Not selected by default

T1: The execution time when you record the operation

#

The initial status of the item when **Wait to replay** is activated. If **Wait to replay** is deactivated, the initial status is ineffective.

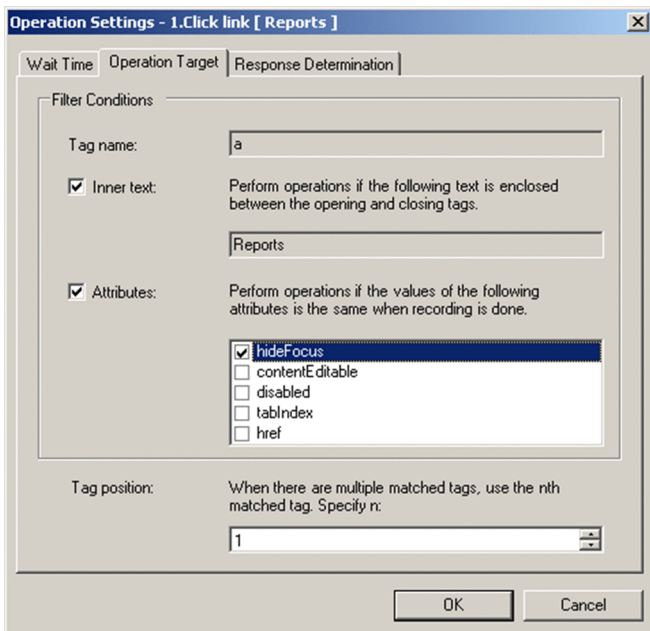
If page transition occurs, automatically perform the next operation immediately. check box

Select this check box when you carry out the next operation immediately if page transitions occur during the wait time. This check box is activated only for the navigation operations.

(2) Operation Target page

The **Operation Target** page is used to set how to identify the operation target tags. After the IE scenario is recorded, the attributes or the positions of the tags are changed due to the layout change of the monitoring target site. In this case, you can cope with the layout change without re-recording the IE scenario. Also use this page when the IE scenario is not replayed as you intend because the default identification method does not identify the tag. Each item on this page is activated only for HTML operations.

Figure 7–26: Operation Settings window (Operation Target page)



The following describes the displayed items.

Filter Conditions:

Specify the filter conditions to identify the operation target tag when you replay the recorded operations. If you specify either **Inner text** or **Attributes** check box, replay the operations that match the condition. If you specify both **Inner text** and **Attributes** check box, replay the operations that match the both conditions.

Tag name:

Display the tag name for the selected operation. This item cannot be edited.

Inner text check box

Select this check box when you set the tag with the same inner text as the operation target. If the tag name is a, Inner text check box is selected by default.

Attributes check box

Select this check box when you identify the attributes of the operation target tag. This check box is not selected by default. The list view shows the attributes of the tags when the operation is recorded. The tag with the same attribute value is selected as the operation target. If you select multiple attributes, the tag with the same attribute values is selected. Note that the list view may list the attributes that are not defined in the HTML file but has default values.

Tag position:

Specify the tag position within the range from 1 to 2,147,483,647. The tag that occurs in the specified position is selected as the operation target. The default value is the tag position when you record the operations. If you specify more than the maximum value, 2,147,483,647 is set as Tag position. If you specify less than the minimum value, 1 is set as Tag position. If you set a decimal fraction, truncate the value at the decimal point. If none is specified, Tag position is reset to the previous value.

The following shows that the default value for Tag position varies depending on the tag name.

- When the tag name is a:

The tag position of the operated tag among the same tags with the same inner-text, counting from the beginning of the HTML file.

- When the tag name is other than a:

The tag position of the operated tag among the same tags, counting from the beginning of the HTML file.

The following shows that the operation target tag varies depending on the Filter Conditions.

- **Filter Conditions** is not selected:

Among the tags displayed in the Tag name, the tag in the Tag position is selected as the operation target.

- **Inner text** is selected:

Among the tags displayed in the Tag name with the same inner-text, the tag in the Tag position is selected as the operation target.

- **Attributes** is selected:

Among the tags displayed in the Tag name with the same attribute values, the tag in the Tag position is selected as the operation target.

- Both **Inner text** and **Attributes** are selected:

Among the tags displayed in the Tag name with the same inner-text and attribute values, the tag in the Tag position is selected as the operation target.

The following table list shows how the combination of options affects the behavior:

Table 7–8: How the combination of options affects the behavior

Specifiable combination			Behavior	Applicable case
Inner text	Attribute value	Tag position		
Y	Y	Y	The <i>Tag-position</i> th tag with the same inner-text and attribute value is selected as the operation target.	Use this combination when the operation target is not identified using the combinations listed below.
N	Y	Y	The <i>Tag-position</i> th tag with the same attribute value is selected as the operation target.	Use this combination when the operation target has no inner-text but has a unique attribute value. Do not use this combination when there are many tags with the same attribute value and the number of those tags in the page changes.
Y	N	Y	The <i>Tag-position</i> th tag with the same inner-text is selected as the operation target.	This combination is a default setting for the <A> tag. Use this combination when the operation target has a unique inner-text. Do not use this combination when there are many tags with the same inner-text and the number of those tags in the page changes.
N	N	Y	The <i>Tag-position</i> th tag is selected as the operation target.	This combination is a default setting for tags other than the <A> tag. Use this combination when the content of the page does not change.

Specifiable combination			Behavior	Applicable case
Inner text	Attribute value	Tag position		
N	N	Y	The <i>Tag-position</i> th tag is selected as the operation target.	Do not use this combination when the number of the same tag in the page changes.

Legend:

Y : Selected

N : Not selected

Tag position is always selected.

Note that the tag position is a relative position, counting among the tags identified by the inner-text and attributes. Therefore, if you change the combination of options, the number of the tags identified by the inner-text and attributes also changes so that you reconsider the tag position.

The following shows the examples:

Figure 7–27: The page when recording

<Browser display>	<HTML source code>
<pre> : Products Information is Here Maintenance Information Updates is Here : </pre>	<pre> : Products Information is Here Maintenance Information Updates is Here : </pre>

As shown in the Figure 7-27, when you click the `Here` link of the `Maintenance Information Updates` in the page where the same inter-text exists, the following information is recorded:

Figure 7–28: Recorded Information

<pre> Tag: A Inner text: Here Tag position : 2 </pre>

Yet, when this page changes as in the following figure, the tag position of the `Maintenance Information Updates is Here` link becomes 3rd. Thus, replaying fails.

Figure 7–29: The page when replaying

<Browser display>	<HTML source code>
<pre> : Products Information is Here Support Information Updates is Here Maintenance Information Updates is Here : </pre>	<pre> : Products Information is Here Support Information Updates is Here Maintenance Information Updates is Here : </pre>

In this case, you cope with this change in the following 3 ways. Note that if you cope in the (ii) or (iii) way you modify the recorded operation information so that you have the knowledge enough to analyse the HTML source. If you cannot analyse the HTML source, either you re-record the IE scenario or acquire the necessary information from the administrator of the monitoring target site (or page).

(i) *Re-record the IE scenario*

Re-record the IE scenario in the changed page. If you cope in this way, you do not have to care about the page change.

(ii) *Change the tag position*

Since the tag and inner-text of the operation target does not change, you can cope with the page change by changing the tag position.

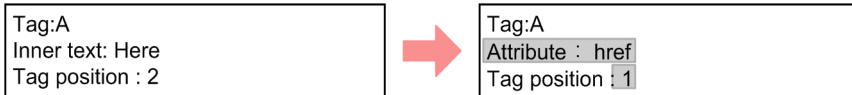
Figure 7–30: Modification by changing the tag position



(iii) Change the identification method and the tag position

Change the identification method for the recorded operation from the inner-text to the attributes. In the example shown in the Figure 7-27 and 7-29, the value of the `href` attribute does not change before and after the page change. Thus, you can identify the tag by using the attribute information. This method is effective, especially when you expect the tags with the same inner-text and each unique `href` attribute value (URL) to increase in the page. If you take this method, you are required to change the tag position because you change the identification condition for calculating the tag position.

Figure 7–31: Modification by changing the specification method and tag position



How to identify the operation:

You can check the operation target when you change the filter condition in the following procedure:

1. Set break point in the operation to check the filter condition.
2. Replay by step until the operation to check the filter condition.
The next operation target turns light red.
3. Select the next operation and open the Operation Settings window and then the Operation Target page.
4. Change the Filter Conditions and/or the Tag position.
5. Click the **OK** button after you change the settings.

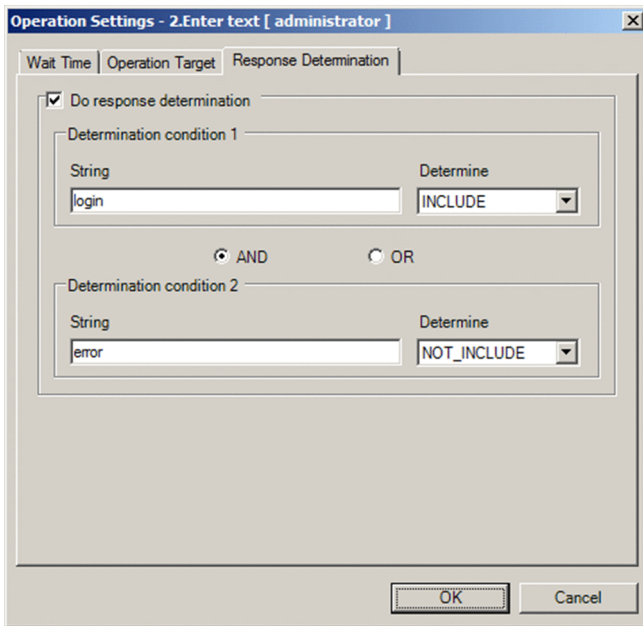
The changed filter condition is evaluated and the next operation target turns red.

In this way, you can check the operation target when you change the filter conditions.

(3) Response Determination page

The **Response Determination** page is used to specify conditions to check whether the HTTP response is proper. Define the condition to judge for each operation. All the received pages for each operation are determined. Note that this response determination is applicable only to HTML texts.

Figure 7–32: Operation Settings window (Response Determination page)



The following describes the displayed items.

Do response determination check box

Select this check box when you check HTTP response. This check box is not selected by default. You can define two conditions.

AND

Select this check box if you determine the response to be proper when both the **Determination condition 1** and **Determination condition 2** are matched. If either the **Determination condition 1** and **Determination condition 2** is matched, measurement ends.

OR

Select this check box if you judge the response to be proper when either the **Determination condition 1** or **Determination condition 2** is matched. If neither the **Determination condition 1** nor **Determination condition 2** is matched, measurement ends.

String

Specify the string up to 1024 characters to check. Any characters are specifiable. If none is specified, HTTP response is not checked.

Determine

Specify whether **Character string** is **INCLUDED** or **NOT_INCLUDED** in the HTTP response. **INCLUDED** is selected by default.

! Important

Even if you specify response determination for the navigation in the **Operation list** for IE scenarios, the HTTP response will not be checked. Specify response determination for the operation preceding a navigation operation.

7.3.3 Change Password window

The Change Password window is used to change the user IDs and passwords specified when recording the IE scenarios. To display this window, in the Web Recorder (main) window, from the **Edit** menu, choose **Change Password**. You can change passwords for the pop-up dialog operation with the Windows standard password input field and the enter text operation to the `<INPUT TYPE=PASSWORD>` tag in the HTML document.

Figure 7–33: Change Password window



The following describes the displayed items.

User ID:

Display the user ID when recording. If the user ID was not entered, none is displayed. Specify the user ID up to 1024 characters. This item cannot be changed by default.

None is displayed for the enter text operation to the `<INPUT TYPE=PASSWORD>` tag in the HTML document.

Change user ID check box

Select this check box when you change the user ID. After you select this check box, you can change the user ID. The default is that this check box is not selected. This check box cannot be selected for the enter text operation to the `<INPUT TYPE=PASSWORD>` tag in the HTML document (not activated).

New password:

Specify the new password up to 1024 characters.

Confirm new password:

Re-enter the password you specify in the **New password**. If you enter a different password, an error message is displayed.

Change password for same IDs check box

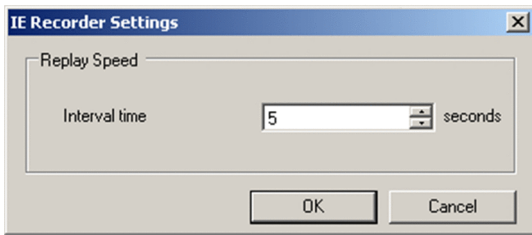
Change password for all the operations in the IE scenario file with the same ID as the current one entered. This check box is not selected by default.

This check box cannot be selected for the enter text operation to the `<INPUT TYPE=PASSWORD>` tag in the HTML document (not activated).

7.3.4 IE Recorder Settings window

The IE Recorder Settings window is used to change the IE Recorder settings. To display this window, in the IE Recorder (main) window, from the **Edit** menu, choose **IE Recorder Settings**. The changes made in this window are not reflected in the IE Recorder action condition definition file (jpcvierec.conf).

Figure 7–34: IE Recorder Settings window



The following describes the displayed items.

Replay Speed

Specify the replay speed of the IE scenario. If you change this item, the interval (the number of seconds you specified) is inserted for each operation so that you can easily check the transition status.

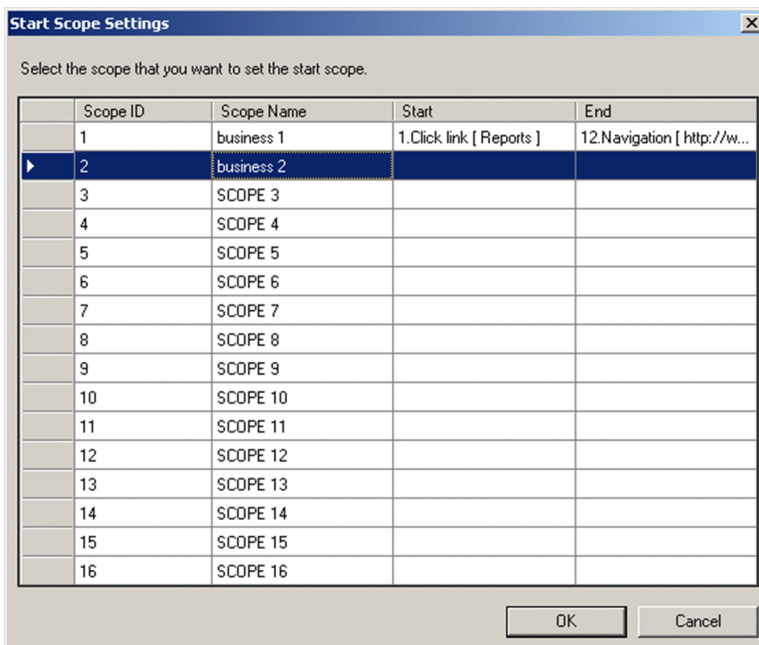
Interval time:

Specify the interval time from 0 to 99 seconds. 1 second is set by default. The Interval time means the inserted wait time immediately after each operation (in other words, the next operation target is marked). The specified value is applied only when replaying in the IE recorder. If you specify the decimal fraction, truncate the value at the decimal point. If none is specified, the wait time is reset to the previous value. Note that this value is ignored when you replay by step, conducts the measurement test, or measure by the IE Probe so that play time does not include this value.

7.3.5 Start Scope Settings window

The Start Scope Settings window is used to set the start scope when you define a scope in any range of operations. To display this window, in the IE Recorder (main) window, from the **Scope** menu, choose **Set Start Scope**.

Figure 7–35: Start Scope Settings window



The following describes the displayed items.

Scope ID

The scope IDs are listed in ascending order. The scope ID is not editable.

Scope Name

Specify the names for scopes up to 127 bytes. The default value for each scope is `SCOPE scope ID`. When you double-click cells, you can edit scope names.

The comma (,) and double-quotation mark (") cannot be used in a scope name. This item cannot be specified as all blanks.

Start

Display the operation which starts the scope. None is displayed when you do not set the start scope. You cannot edit the Start.

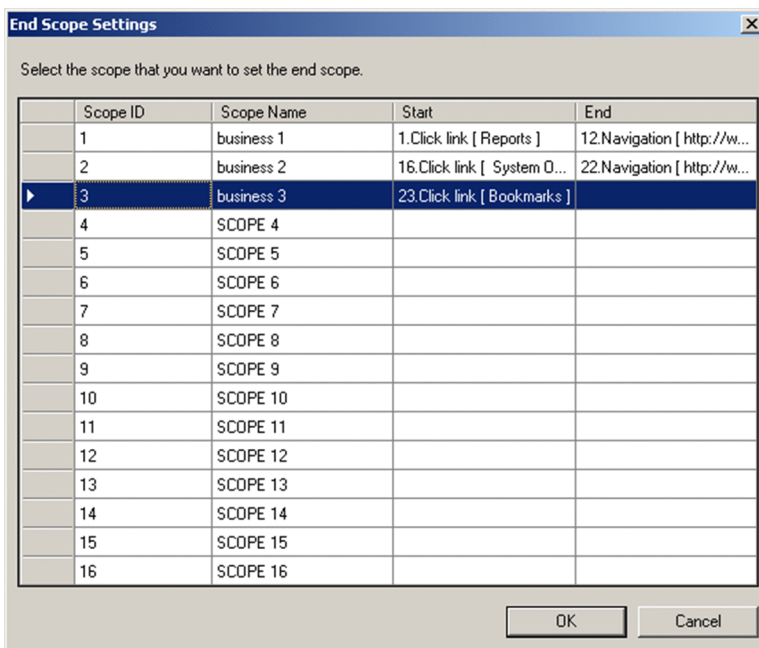
End

Display the operation which ends the scope. None is displayed when you do not set the start scope. You cannot edit the End.

7.3.6 End Scope Settings window

The End Scope Settings window is used to set the end scope when you define a scope in any range of operations. To display this window, in the IE Recorder (main) window, from the **Scope** menu, choose **Set End Scope**.

Figure 7–36: End Scope Settings window

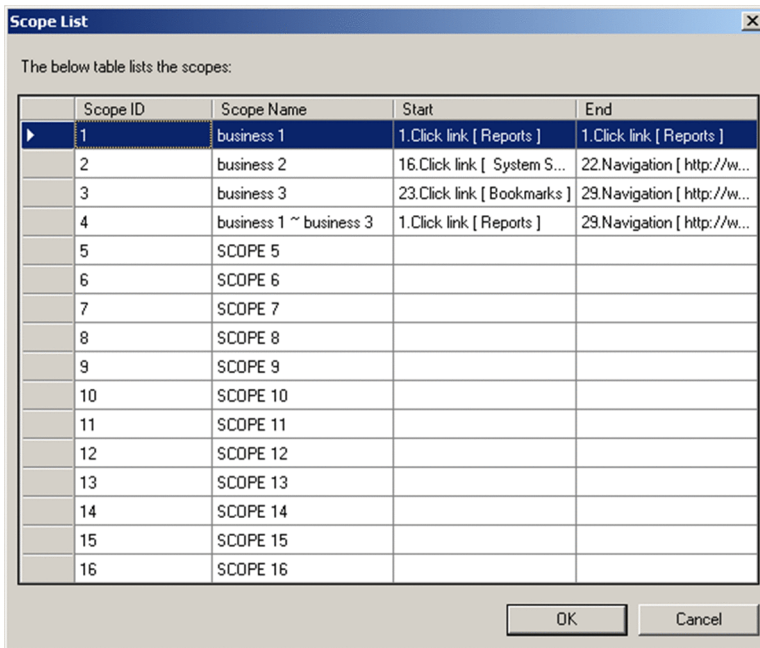


For details about the displayed items, see [7.3.5 Start Scope Settings window](#)

7.3.7 Scope List window

The Scope List window is used to check the scope list. To display this window, in the IE Recorder (main) window, from the **Scope** menu, choose **Scope List**.

Figure 7–37: Scope List window

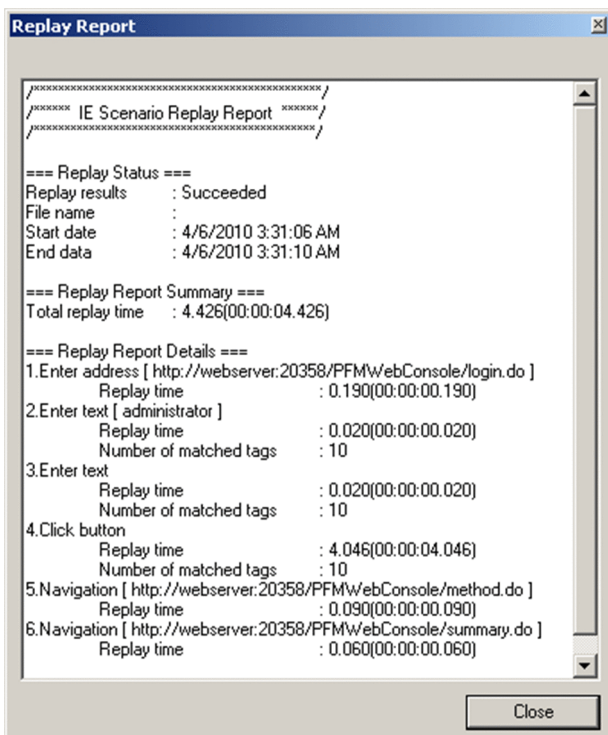


For details about the displayed items, see [7.3.5 Start Scope Settings window](#)

7.3.8 Replay Report window

The Replay Report window is used to show the replay report of the IE scenario by the **Measurement Test**. This window appears when the replaying IE scenario is completed.

Figure 7–38: Replay Report window



The following describes the displayed items.

Replay results of operations

The following shows the information about the result of the replaying an IE scenario.

- *Replay Status*
Displays the *Replay Status* (Succeeded or Failed), *File name*, *Start date*, and *End data*.
 - *Replay Report Summary*
Displays the *Total replay time*. The Total replay time is displayed to three places of decimals.
 - *Scope Summary*
Displays the replayed scopes (scope IDs and scope names) and the *Total replay time* of the scope.
 - *Replay Report Details*
Displays the replayed operations (operation number and operation name), *Replay time* of the scope^{#1}, *Start Scope* (*scope IDs* and *scope names*^{#2}), *End Scope* (*scope IDs* and *scope names*^{#2}), and the number of the tags that match the Filter Conditions. Note that the number of the tags that match the Filter Conditions is displayed only for the HTML operations.
- #1
The Replay time is displayed to three places of decimals.
- #2
If multiple scopes are specified in one operation, only scope name is displayed.
- *Message Information*
Displays the operations where errors occur (operation number and operation name) and the error message information.

8

Definition Files

This chapter describes the definition files used with PFM - Agent for Service Response.

8.1 List of definition files

The following table lists and describes the files that are used to set up an environment for PFM - Agent for Service Response and for registration of measurement conditions.

Table 8–1: Definition files used for environment setup

Definition file	File name	Description	See
Probe action condition definition file	<i>installation-folder</i> \agtv\probe\conf\esp.conf	Sets the Probe Daemon and the IE Probe Daemon's start options.	8.2
Measurement condition registration file	<i>installation-folder</i> \agtv\probe\task\esp\esptask.xml	Defines measurement conditions for each Internet service. The measurement conditions consist of a section for common conditions, and sections for service-specific conditions.	8.3
		Common section	8.3.2
		Service-specific condition sections	8.3.3
		for HTTP	8.3.3(1)
		for HTTPS	8.3.3(2)
		for SMTP	8.3.3(3)
		for POP3	8.3.3(4)
		for IMAP4	8.3.3(5)
		for DNS	8.3.3(6)
		for DHCP	8.3.3(7)
		for FTP	8.3.3(8)
		for TCP	8.3.3(9)
		for WEBTRANS	8.3.3(10)
for IESCENA	8.3.3(11)		
for USERSERV	8.3.3(12)		
Web Recorder action condition definition file	<i>installation-folder</i> \agtv\probe\conf\wr.conf	Defines the Web Recorder's action conditions.	8.4
Web transaction files	Any file name with the extension xml under <i>installation-folder</i> \agtv\probe\webtrans\	Each defines a series of Web access operations as a single Web transaction.	8.5
Command registration file	<i>installation-folder</i> \agtv\probe\conf\espccommand.xml	Registers user-defined commands.	8.6
Measurement condition label definition file	<i>installation-folder</i> \agtv\probe\conf\esptasklabel.conf	Defines labels for measurement conditions.	8.7
IE Recorder action condition definition file	<i>installation-folder</i> \agtv\probe\conf\jpcvierec.conf	Defines the IE Recorder's action conditions.	8.8
IE scenario files	Any file name with the extension xml under <i>installation-folder</i> \agtv\probe\iescena\	Defines a series of operations as an IE scenario.	8.9

8.1.1 About specification in XML format

The measurement condition registration file, command registration file, and Web transaction files are created in XML format. The following points must be noted when you create definition files in XML format.

Start and end tags

XML tags must always be paired (start tag and end tag). If the end tag is missing for a specified start tag, or vice versa, an error results. Within a tag enclosed by angle brackets (< and >), you cannot specify any codes other than the tag name (such as spaces, tabs, or linefeed characters).

Element

The coding enclosed by a start tag and an end tag constitutes an *element*.

```
<SAMPLE_TAG>..element..</SAMPLE_TAG>
```

The start tag must have a corresponding end tag. In the example above, if <SAMPLE_TAG> were not accompanied by the corresponding </SAMPLE_TAG>, an error would result.

If there is no element, the start and end tags can be combined as follows:

```
<SAMPLE_TAG/>
```

Case

XML coding is case sensitive. You must enter all information exactly as shown in the definition file format.

Deletion of space, tab, and linefeed characters

Space, tab, and linefeed characters that were entered before or after an element are deleted; they are not treated as part of the element.

Characters requiring replacement

The characters listed below are reserved characters in the XML syntax. To use these characters as part of an element, they must be replaced with the indicated character strings.

Table 8–2: Characters requiring replacement

Character	Replacement character string
&	&
<	<
>	>
"	"
'	'

Specification of a comment

You can specify a comment in following format:

```
<!--comment-->
```

A comment text cannot contain two hyphens in succession (--).

Linefeed code

A linefeed code in a text is treated as LF (0x0a). To treat it as CRLF (0x0d0a), use 
 instead of the linefeed code.

8.1.2 Editing the definition files after an upgrade installation to the multi-language edition

When performing an upgrade installation of Performance Management from the overseas edition of version 9 or earlier to the multi-language edition of version 10, note that the contents of the definition files below are not changed.

If you do not need to add or change any information in the definition files, there is no need to edit them.

However, if you add or change any information in the definition file by using a character encoding other than that declared on the first line of the file, you must change the character encoding in that file.

The following definition files need to have the character encoding changed before editing:

- Measurement condition registration file (`esptask.xml`)
- Web transaction file
- Command registration file (`espcommand.xml`)

For example, assume that the character encoding specified in the measurement condition registration file (`esptask.xml`) is Shift JIS. If you attempt to update the contents of the file by entering characters not supported by Shift JIS from PFM - Web Console, you might get the following message, and the attempt to update the contents of the file might fail.

```
KAVJS2604-E (PFM0446)
The service properties could not be updated.
An error occurred while updating service properties.
Use the jpcctrl list command to confirm that the service has started. If the service has stopped, execute the jpcstart command.
```

In such a case, change the character encoding specified in the measurement condition registration file (`esptask.xml`) before updating the contents of the file. You can use any editor to change the character encoding. Note that the character encoding in the definition file cannot be changed from PFM - Web Console.

8.2 Probe action condition definition file (esp.conf)

The Probe action condition definition file is used to set the Probe Daemon's start options and the IE Probe Daemon's start options. It is read when the Probe Daemon starts and the IE Probe Daemon starts.

To apply the definitions specified in the Probe action condition definition file, you must restart PFM - Agent for Service Response.

8.2.1 Format

```
[General]
mode=ESP
number_of_probes=maximum-number-of-measurement-conditions-for-probe
max_reportfile_size=maximum-size-of-report-file
ie_number_of_probes=maximum-number-of-measurement-conditions-for-IE-probe
ie_max_reportfile_size=maximum-size-of-IE-probe-report-file
ie_service_flag={Y|N}
disable_ssl_protocol={NONE|TLSV11|TLSV12}
html_script_skip_flag={Y|N}

[System Log]
printlog_flag={Y|N}

[Cluster]
cluster_flag={Y|N}
shared_directory=folder-name-on-shared-disk-used-for-cluster-operation

[WEBTRANS Probe]
max_keep_alive_session=maximum-sessions-count-in-keep-alive-mode
skip_emb_rsc_error={Y|N}
post_redirect_method={GET|POST}

[FTP Probe]
ignore_quit_resp_recv_error={Y|N}

[IE Probe]
html_log_flag={Y|N}
max_number_of_html_log=maximum-number-of-storing-HTML-file-acquired-when-measuring-IE-scenario
ie_probe_browser_mode=Internet-Explorer-version-for-using-IE-probe
```

Note:

The following notes apply to specifying the Probe action condition definition file:

- Each key name and its value must be connected by an equal sign (=).
- Each key name and its value must be specified on a single line.
- The specification must begin in column 1.

A line beginning with a hash mark (#) is treated as a comment line.

8.2.2 Definition

This subsection describes the definitions. You can omit any unneeded optional key name (or optional section).

General section:

Specifies the maximum number of measurement conditions for the probe and IE probe of PFM - Agent for Service Response and the maximum size of a report file.

Table 8–3: Definition in the General section

Key name	Mandatory	Value to be specified
Mode	Y#	Always ESP. When the probe is used, this item takes effect.
number_of_probes ((1 to 100))<<10>>	--	Specifies the maximum number of measurement conditions for a probe. When the probe is used, this item takes effect.
max_reportfile_size ((1 to 32))(MB)<<4>>	--	Specifies the maximum size of a report file. When the probe is used, this item takes effect.
ie_number_of_probes ((1 to 20))<<5>>	--	Specifies the maximum number of measurement conditions for an IE probe. When the IE probe is used, this item takes effect.
ie_max_reportfile_size ((1 to 32))(MB)<<1>> or, ((128K to 32768K))(KB)	--	Specifies the maximum size of an IE report file. When the IE probe is used, this item takes effect.
ie_service_flag ((Y or N))<<N>>	--	Specifies whether you use Windows services to start and stop the IE probe. If you use, specify Y. If you do not use, specify N. If you manually start and stop the IE probe from the Windows start menu, specify N. If you operate PFM - Agent for Service Response in a cluster system, specify Y. If you do not use IE scenarios in a cluster environment, specify N.
disable_ssl_protocol ((NONE, TLSV11, or TLSV12))<<NONE>>	--	Specifies which of the SSL protocols used for communication between a probe and Web server will be disabled for monitoring of HTTPS (including monitoring of Web transactions that use HTTPS). PFM - Agent for Service Response supports the following SSL protocols: <ul style="list-style-type: none"> • TLSv1 • TLSv1.1 • TLSv1.2 If you monitor a Web server that does not support TLSv1.1, TLSv1.2 or later, the Result Code (RESULT_CODE) field of the record collected by monitoring might be set to 3, causing a measurement error. You might be able to prevent this error by specifying TLSV11 or TLSV12 for this option. If you want to use all protocols, specify NONE. If you want to disable a specific protocol, specify either of the following value: <ul style="list-style-type: none"> • TLSV11: Disables TLSv1.1 or later. • TLSV12: Disables TLSv1.2 or later.
html_script_skip_flag ((Y or N))<<N>>	--	Specifies whether the contents of script tags will be ignored when embedded resources are searched during monitoring of HTTP, HTTPS, or Web transactions. Specify Y to ignore the contents of script tags during a search. Specify No to search for the contents of script tags. Specifying Y might be able to prevent the KAVK08261-E message from being output to a log during HTTP or HTTPS measurement or the KAVK08261-E and KAVK08311-W messages from being output to a log during Web transaction measurement.
enable_low_level_ssl_protocol ((SSL))	--	Specifies which of the SSL protocols used for communication between a probe and a Web server will be lower protocols for monitoring of HTTPS(including monitoring

Key name	Mandatory	Value to be specified
enable_low_level_ssl_protocol ((SSL))	--	of Web transactions that use HTTPS). PFM - Agent for Service Response supports the following SSL protocols: <ul style="list-style-type: none"> • TLSv1 • TLSv1.1 • TLSv1.2 SSLv2.0 and SSLv3.0 become effective in addition to the protocol mentioned above when you specify "SSL" to this key. But, it is not recommended that you validate SSLv2.0 and SSLv3.0, which are lower protocols.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the key.

<<>>: Default value

#

When you use the probe, this item is mandatory.

System Log section:

Specifies a setting related to log output.

Table 8–4: Definition in the System Log section

Key name	Mandatory	Value to be specified
printlog_flag ((Y or N))<<N>>	--	Specifies whether or not the Probe Daemon's event log and the IE Probe Daemon's event log are to be output. To output the event log, specify Y; otherwise, specify N.

Legend:

--: Optional item

(()): Specifiable value range of the key.

<<>>: Default value

Cluster section:

Specifies settings related to cluster operation.

Table 8–5: Definition in the Cluster section

Key name	Mandatory	Value to be specified
cluster_flag ((Y or N))<<N>>	--	Specifies Y to use PFM - Agent for Service Response in a cluster environment; otherwise, specifies N.
shared_directory ((up to 255 bytes))	--#	When PFM - Agent for Service Response is to be used in a cluster environment, this item specifies the name of the directory on the shared disk to which report files are to be output. If you specify Y in cluster_flag, you must specify this item. If you specify N in cluster_flag, this item is ignored, if specified. Do not enclose the value in double quotation marks (") even when the specified path contains a space.

Legend:

--: Optional item

(()): Specifiable value range of the key.

<<>>: Default value

#

When Y is specified in cluster_flag, this item is mandatory.

WEBTRANS Probe section:

Specifies settings related to Web transaction measurement. These settings take effect when you use the probe.

Table 8–6: Definition in the WEBTRANS Probe section

Key name	Mandatory	Value to be specified
max_keep_alive_session ((1 to 20))<<10>>	--	When the keep alive mode is used for Web transaction measurement, this item specifies the maximum number of sessions that can be kept alive. This becomes the maximum number of sessions per Web transaction measurement.
skip_emb_rsc_error ((Y or N))<<Y>>	--	Specifies whether or not measurement is to continue when acquisition of an embedded resource results in an error during Web transaction measurement. To continue measurement, specify Y; otherwise, specify N.
post_redirect_method ((GET or POST))<<GET>>	--	Specifies the method to be used for redirecting a POST request during Web transaction measurement. To use a GET method, specify GET; to use a POST method, specify POST. Normally, do not change this value.

Legend:

- : Optional item
- (()): Specifiable value range of the key.
- << >>: Default value

FTP Probe section:

Specifies a setting related to FTP measurement.

Table 8–7: Definition in the FTP Probe section

Key name	Mandatory	Value to be specified
ignore_quit_resp_rcv_err or ((Y or N))<<N>>	--	Specifies whether or not monitoring is to continue when a reception error occurs in the response message from the FTP server for a logout request (entry of the QUIT command) during FTP measurement. To continue measurement, specify Y; otherwise, specify N. When FTP monitoring is performed in an environment where a Windows firewall is used, specify Y in this item.

Legend:

- : Optional item
- (()): Specifiable value range of the key.
- << >>: Default value

IE Probe section:

Specifies a setting related to IE Probe measurement. These settings take effect when you use the probe.

Table 8–8: Definition in the IE Probe section

Key name	Mandatory	Value to be specified
html_log_flag ((Y or N))<<Y>>	--	<p>Specifies whether the Web pages acquired while measuring IE scenarios are output to the HTML files. Specify Y to check the contents of the HTML files when detecting problems during measurements. The output files when replaying an IE scenario are stored in a folder. The character code of the output file is UTF-8. The following shows the output destination of the HTML files and their names:</p> <p>The output destination of the HTML files:</p> <p style="margin-left: 40px;"><i>installation-folder\agtv\probe\probedata\iescena\ieprobed_measurement-condition-ID\measurement-start-time-for-IE-scenario</i>^{#1}</p> <p>The output file name:</p> <p style="margin-left: 40px;"><i>output-number_sequence-number_frame-number.html</i>^{#2}</p>

Key name	Mandatory	Value to be specified
max_number_of_html_log ((1 to 500))<<20>>	--	Specifies the maximum case number of storing the HTML files acquired while measuring IE scenarios. Counts all the HTML files acquired when measuring an IE scenario as 1 case. The IE probe stores the HTML files the <i>max_number_of_html_log</i> times for each measurement condition. If the store case number exceeds the <i>max_number_of_html_log</i> , the files of the oldest case are deleted. If you specify N as the value of <i>html_log_flag</i> , the value you specified is ignored.
ie_probe_browser_mode ((IE7, IE8, IE9, IE10 or IE11)) ^{#3}	--	Specifies the Internet Explorer version for using the IE probe. Before specifying this item, check the Internet Explorer version supported by the monitoring target and the version of Internet Explorer installed in an environment in which PFM - Agent for Service Response is installed. Internet Explorer 7 is the default version. <ul style="list-style-type: none"> • IE7 Specify this when the monitoring target supports Internet Explorer 7. • IE8 Specify this when the monitoring target supports Internet Explorer 8. • IE9 Specify this when the monitoring target supports Internet Explorer 9. You can specify this option when Internet Explorer 9 or a later version is installed in an environment in which PFM - Agent for Service Response is installed. • IE10 Specify this when the monitoring target supports Internet Explorer 10. You can specify this option when Internet Explorer 10 or a later version is installed in an environment in which PFM - Agent for Service Response is installed. • IE11 Specify this when the monitoring target supports Internet Explorer 11. You can specify this option when Internet Explorer 11 or a later version is installed in an environment in which PFM - Agent for Service Response is installed. You must specify the Internet Explorer version that was specified when IE scenarios were created. This value must also be specified for <i>ie_rec_browser_mode</i> in the IE Recorder action condition definition file. If a value is not specified or if an invalid value is specified, the default version (Internet Explorer 7) is used.

Legend:

--: Optional item

(()): Specifiable value range of the key.

<< >>: Default value

#1

The measurement start time for IE scenario is displayed in the following format: YYYYMMDD_hhmmss format (YYYY:Year, MM:Month, DD:Day, hh:Hour, mm:Minute, ss:second).

#2

The output number begins with 1. For details about the *sequence number*, see [7.3.1 IE Recorder \(main\) window](#).

#3

Do not specify version of Internet Explorer that PFM - Agent for Service Response does not support.

8.2.3 Example

The following is an example of a Probe action condition definition file:

```
[General]
mode= ESP
number_of_probes= 10
max_reportfile_size= 1
```

```
ie_number_of_probes= 5
ie_max_reportfile_size= 128K
ie_service_flag= N
disable_ssl_protocol=NONE
html_script_skip_flag=N

[System Log]
printlog_flag=Y

[Cluster]
cluster_flag= N
shared_directory=folder-name-on-shared-disk-used-for-cluster-operation

[WEBTRANS Probe]
max_keep_alive_session= 10
skip_emb_rsc_error= Y
post_redirect_method= GET

[FTP Probe]
ignore_quit_resp_recv_error= N

[IE Probe]
html_log_flag= Y
max_number_of_html_log= 10
ie_probe_browser_mode=
```

8.3 Measurement condition registration file (esptask.xml)

The measurement condition registration file is used to register measurement conditions for the IE scenario or each Internet service. This file is read when the Agent Collector, the Probe Daemon, or the IE Probe Daemon starts. This file is specified in XML format.

You can use PFM - Web Console to define the settings of the measurement condition registration file. If you use PFM - Web Console to define the settings, you do not need to restart PFM - Agent for Service Response. You can also use PFM - Web Console to apply these settings to the Probe Daemon and the IE Probe Daemon. For these reasons, usually use PFM - Web Console to define the measurement conditions.

When you define the measurement condition for IE scenarios, you can register the definitions to the measurement condition registration file and edit this file in the IE Recorder (main) window. Yet, if you edit this file in the IE Recorder (main) window, you must stop PFM - Agent for Service Response in advance. Hitachi recommends that you use PFM - Web Console to edit the measurement condition registration file.

If you do not use PFM - Web Console, you must restart PFM - Agent for Service Response to apply the definitions specified in the measurement condition registration file.

You cannot use PFM - Web Console to specify the <POST> tags under the <HTTP> tag or the <POST> tags under the <HTTPS> tag. Edit directly the measurement condition registration file to specify the <POST> tags.

Notes on editing directly the measurement condition registration file

- You must stop PFM - Agent for Service Response in advance before editing directly the measurement condition registration file.
- If you edit directly the measurement condition registration file, you can specify the multibyte characters as the values of the properties that are not allowed to contain the multibyte characters. In this case, when the measurement condition registration file is read, PFM - Web Console displays the values of the properties as they are and the `Valid` is displayed in the **Status**. Yet, if you click the OK button, PFM - Web Console outputs the error message that the multibyte characters are specified in the field allowed to contain only the single-byte characters (KAVJS2602-E).
- While editing directly the measurement condition registration file, you must not choose from the **Tools** menu **Simplified Registration** in the IE Recorder (main) window.

Notes on specifying tags for the measurement condition registration file

Multibyte characters (for example, Japanese) can be specified in the following tags only:

- <TASKLABEL> tags for all services
- <MESSAGE_BODY> tags for HTTP and HTTPS services
- <CLIENT_CERT_FILE> tags for HTTPS services
- <FILE_NAME> tags for FTP services
- <TRANSACTION_FILE> tags for WEBTRANS services
- <TRANSACTION_NAME> tags for WEBTRANS services
- <IESCENA_FILE> tags for IE scenarios

8.3.1 Format and definition of the measurement condition registration file

(1) Format

```
<?xml version="1.0" encoding="US-ASCII" standalone="no"?>
<!DOCTYPE TASKLIST SYSTEM "esptask.dtd">
<TASKLIST>
  <TASK>
    <GEN_PARAM>
      <!--GEN_PARAM -->
    </GEN_PARAM>
    <SERV_PARAM>
      <!--SERV_PARAM is specific to service type-->
    </SERV_PARAM>
  </TASK>
  ...
</TASKLIST>
```

(2) Definition

(a) XML declaration and document type declaration

Specify the XML declaration on the first line and the document type declaration on the second and third lines. Specify exactly as shown below:

```
<?xml version="1.0" encoding="encoding-type" standalone="no"?>
<!DOCTYPE TASKLIST SYSTEM "esptask.dtd" [
]>
```

The document type declaration on the second and third lines can be specified as shown below:

```
<!DOCTYPE TASKLIST SYSTEM "esptask.dtd">
```

Specify one of the following encoding types. In operating on the PFM - Web Console, the encode type when this file is read is saved.

- Shift_JIS
- US-ASCII
- GB18030#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

(b) XML definition

Table 8–9: XML definition

XML tag	Mandatory	Role of tag and value to be specified
<TASKLIST>...</TASKLIST>	Y	Indicates a list of measurement conditions. This tag contains one or more <TASK> tags. A new <TASK> tag can start immediately after a </TASK> tag.

XML tag	Mandatory	Role of tag and value to be specified
<TASK>...</TASK>	Y	Indicates a single measurement condition. This tag contains one set consisting of a <GEN_PARAM> tag and a <SERV_PARAM> tag.
<GEN_PARAM>...</GEN_PARAM>	Y	Contains the <TASKID>, <INTERVAL>, and <TIMEOUT> measurement condition tags, which contain parameters that do not depend on the target service. For details, see 8.3.2 Format and definition of measurement conditions (common section) .
<SERV_PARAM>...</SERV_PARAM>	Y	Contains measurement condition parameters that depend on the target service. This tag contains one of the <HTTP>, <HTTPS>, <SMTP>, <POP3>, <IMAP4>, <DNS>, <DHCP>, <FTP>, <TCP>, <WEBTRANS>, <IESCENA >, or <USERSERV> tags. For details, see 8.3.3 Format and definition of measurement conditions (service-specific condition sections) .

Legend:

Y: Mandatory item

8.3.2 Format and definition of measurement conditions (common section)

This subsection describes the format and definition of the common section of the measurement conditions.

(1) Format

```
<GEN_PARAM>
  <TASKID>measurement-condition-ID</TASKID>
  <TASKLABEL>measurement-condition-label</TASKLABEL>
  <INTERVAL>measurement-interval</INTERVAL>
  <TIMEOUT>timeout-value</TIMEOUT>
</GEN_PARAM>
```

(2) Definition of <GEN_PARAM>

Table 8–10: Definition of <GEN_PARAM>

XML tag	Mandatory	Role of tag and value to be specified
<TASKID>...</TASKID> ((1 to 65535))	Y	Specifies the ID that identifies a measurement condition.
<TASKLABEL>...</TASKLABEL> ((character string of up to 63 bytes))	--	Specify this item if you give any label name to the task. Hitachi recommends that the name is unique among the other task labels in the other measurement conditions. You can also specify the task labels in the measurement condition label definition file (esptasklabel.conf). The settings in the measurement condition registration file take precedence over the settings in the measurement condition label definition file. You cannot specify the comma (,) and double-quotation mark (") in a label name. Yet, you can specify the equal sign (=).
<INTERVAL>...</INTERVAL> ((60 to 86400))(seconds)	Y	Specifies the measurement interval when the specified measurement is to be taken repetitively. This value must be greater than the value specified in the <TIMEOUT> tag (timeout value).

XML tag	Mandatory	Role of tag and value to be specified
<TIMEOUT>...</TIMEOUT> ((1 to 3600))(seconds)<<30>>	--	Specifies the maximum amount of time within which a single measurement must be completed. This value must be smaller than the value specified in the <INTERVAL> tag (measurement interval).

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the key.

<<>>: Default value

8.3.3 Format and definition of measurement conditions (service-specific condition sections)

This subsection describes the format and definition of measurement conditions for each target Internet service.

The 12 types of SERVICE_IDs are described below.

(1) HTTP

This subsection describes the tags for the settings specific to the HTTP service.

(a) Format

```
<SERV_PARAM>
  <HTTP>
    <URL>URL</URL>
    <POST>
      <MESSAGE_BODY>message-body</MESSAGE_BODY>
    </POST>
    <DEPTH>depth</DEPTH>
    <WEB_AUTH>
      <WEB_USERNAME>Web-authentication-user-name</WEB_USERNAME>
    </WEB_AUTH>
    <PROXY>
      <PROXY_HOSTNAME>proxy-host-name-or-IP-address</PROXY_HOSTNAME>
      <PROXY_PORT>proxy-port-number</PROXY_PORT>
      <PROXY_USERNAME>proxy-user-name</PROXY_USERNAME>
    </PROXY>
  </HTTP>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (HTTP)

Table 8–11: Definition of <SERV_PARAM> (HTTP)

XML tag	Mandatory	Role of tag and value to be specified
<HTTP>...</HTTP>	Y	Contains the parameters specific to the HTTP service.
<URL>...</URL> ((character string of up to 255 bytes)) ^{#1}	Y	Specifies the URL of the Web page to be subject to measurement. The protocol identifier (http://) is not included. The port

XML tag	Mandatory	Role of tag and value to be specified
<URL> . . . </URL> ((character string of up to 255 bytes)) ^{#1}	Y	number can be omitted. If the port number is omitted, port number 80 is used.
<POST> . . . </POST>	--	Specifies that the POST method is to be measured. To set this tag, use the <MESSAGE_BODY> tag. To omit the specification, omit the <POST> tag and the tags contained in the <POST> tag. When this tag is omitted, the GET method is used.
<MESSAGE_BODY> . . . </MESSAGE_BODY> ((1 to 1,023 bytes of character string))	..#2	Specifies a character string that is to be sent as the message body for transmission by the POST method. When the POST method is used, this item cannot be omitted.
<DEPTH> . . . </DEPTH> ((1 to 100))<<2>>	--	Specifies the depth of embedded resources and frames to be acquired. This is the depth of the resources and frames in the Web page that are to be downloaded. The following shows examples: DEPTH=1 is specified: Only the Web page is downloaded. DEPTH=2 is specified: The Web page and the resources and frames embedded in the page are downloaded. 3 or a greater value is specified in DEPTH: The Web page, the resources and frames embedded in the page, and the information embedded in the acquired frames (such as the resources and frames embedded in the downloaded frames) are downloaded up to the specified depth. If nothing is embedded in an acquired frame, no more acquisition is performed. For details about embedded resources and frames, see HTTP in 10. Records .
<WEB_AUTH> . . . </WEB_AUTH>	--	Specifies that Web authentication is to be performed. Use the <WEB_USERNAME> tag to specify the settings related to Web authentication. To omit the specification, omit the <WEB_AUTH> tag and all the tags contained in it.
<WEB_USERNAME> . . . </WEB_USERNAME> ((character string of up to 64 bytes))	..#3	Specifies the user name to be used for Web authentication. This tag is applicable only when Web authentication is executed.
<PROXY> . . . </PROXY>	--	Specifies that a proxy is to be used. Use the <PROXY_HOSTNAME>, <PROXY_PORT>, and <PROXY_USERNAME> tags to specify the proxy-related settings. To omit the specification, omit the <PROXY> tag and all the tags contained in it.
<PROXY_HOSTNAME> . . . </PROXY_HOSTNAME> ((character of up to 255 bytes)) ^{#4}	..#5	Specifies the proxy server's host name or IP address. This tag is applicable only when a proxy is used.
<PROXY_PORT> . . . </PROXY_PORT> ((1 to 65535))	..#5	Specifies the proxy server's port number. This tag is applicable only when a proxy is used.
<PROXY_USERNAME> . . . </PROXY_USERNAME> ((character of up to 64 bytes))	..#6	Specifies the user name to be used for proxy authentication. If proxy authentication is not performed, omit this tag.

Legend:

- Y: Mandatory item
- : Optional item
- (()): Specifiable value range of the tag.
- <<>>: Default value

#1

To use an IP address to specify a host name, use an IPv4 dotted-decimal address (for example: 172.16.233.12/example.html) or an IPv6 hexadecimal address enclosed in square brackets, using colons as separators (for example: [ACE6:45:75:91::1]/example.html).

#2

This item is mandatory when the <POST> tag is specified.

#3

This item is mandatory when the <WEB_AUTH> tag is specified.

#4

To specify an IPv4 address for the host name, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: ACE6:45:75:91::1).

#5

This item is mandatory when the <PROXY> tag is specified.

#6

This item is mandatory when the <PROXY> tag is specified and proxy authentication is performed.

(2) HTTPS

This subsection describes the tags for the settings specific to the HTTPS service.

(a) Format

```

<SERV_PARAM>
  <HTTPS>
    <URL>URL</URL>
    <POST>
      <MESSAGE_BODY>message-body</MESSAGE_BODY>
    </POST>
    <DEPTH>depth</DEPTH>
    <WEB_AUTH>
      <WEB_USERNAME>Web-authentication-user-name</WEB_USERNAME>
    </WEB_AUTH>
    <PROXY>
      <PROXY_HOSTNAME>proxy-host-name-or-IP-address</PROXY_HOSTNAME>
      <PROXY_PORT>proxy-port-number</PROXY_PORT>
      <PROXY_USERNAME>proxy-user-name</PROXY_USERNAME>
    </PROXY>
    <SSL_AUTH_IGNORE></SSL_AUTH_IGNORE>
    <CLIENT_AUTH>
      <CLIENT_CERT_FILE>client-certificate-file-name</CLIENT_CERT_FILE>
    </CLIENT_AUTH>
  </HTTPS>
</SERV_PARAM>

```

(b) Definition of <SERV_PARAM> (HTTPS)

Table 8–12: Definition of <SERV_PARAM> (HTTPS)

XML tag	Mandatory	Role of tag and value to be specified
<HTTPS>...</HTTPS>	Y	Contains the parameters specific to the HTTPS service.
<URL>...</URL> (character string of up to 255 bytes) ^{#1}	Y	Specifies the URL of the Web page to be subject to measurement. The protocol identifier (https://) is not included. The port number can be omitted. If the port number is omitted, port number 443 is used.

XML tag	Mandatory	Role of tag and value to be specified
<POST>...</POST>	--	Specifies that the POST method is to be measured. To set this tag, use the <MESSAGE_BODY> tag. To omit the specification, omit the <POST> tag and the tags contained in the <POST> tag. When this tag is omitted, the GET method is used.
<MESSAGE_BODY>...</MESSAGE_BODY> ((1 to 1,023 bytes of character string))	..#2	Specifies a character string that is to be sent as the message body for transmission by the POST method.
<DEPTH>...</DEPTH> ((1 to 100))<<2>>	--	Specifies the depth of embedded resources and frames to be acquired. This is the depth of the resources and frames in the monitored Web page that are to be downloaded. The following shows examples: DEPTH=1 is specified: Only the Web page is downloaded. DEPTH=2 is specified: The Web page and the resources and frames embedded in the page are downloaded. 3 or a greater value is specified in DEPTH: The Web page, the resources and frames embedded in the page, and the information embedded in the acquired frames (such as the resources and frames embedded in the downloaded frames) are downloaded up to the specified depth. If nothing is embedded in an acquired frame, no more acquisition is performed. For details about embedded resources and frames, see HTTPS in 10. Records .
<WEB_AUTH>...</WEB_AUTH>	--	Specifies the settings related to Web authentication. Specify this tag to perform Web authentication. If you do not want to perform Web authentication, omit the <WEB_AUTH> tag and all the tags contained in it.
<WEB_USERNAME>...</WEB_USERNAME> ((character string of up to 64 bytes))	..#3	Specifies the user name to be used for Web authentication. This tag is applicable only when Web authentication is executed.
<PROXY>...</PROXY>	--	Specifies that a proxy is to be used. Use the <PROXY_HOSTNAME>, <PROXY_PORT>, and <PROXY_USERNAME> tags to specify the proxy-related settings. To omit the specification, omit the <PROXY> tag and all the tags contained in it.
<PROXY_HOSTNAME>...</PROXY_HOSTNAME> ((character of up to 255 bytes)) ^{#1}	..#4	Specifies the proxy server's host name or IP address. This tag is applicable only when a proxy is used.
<PROXY_PORT>...</PROXY_PORT> ((1 to 65535))	..#4	Specifies the proxy server's port number. This tag is applicable only when a proxy is used.
<PROXY_USERNAME>...</PROXY_USERNAME> ((character of up to 64 bytes))	..#5	Specifies the user name to be used for proxy authentication. If proxy authentication is not performed, omit this tag.
<SSL_AUTH_IGNORE> </SSL_AUTH_IGNORE>	--	Specifies that measurement is to continue when SSL server authentication fails. To terminate measurement if SSL server authentication fails, omit this tag.

XML tag	Mandatory	Role of tag and value to be specified
<CLIENT_AUTH>...</CLIENT_AUTH>	--	Specifies that client authentication is to be performed. Use the <CLIENT_CERT_FILE> tag to specify the settings related to client authentication. If you do not want to perform client authentication, omit the <CLIENT_AUTH> tag and all the tags contained in it.
<CLIENT_CERT_FILE>...</CLIENT_CERT_FILE> (character of up to 255 bytes)	--#6	Specifies the file in which the client certificate and private key are stored. Use a maximum of 255 bytes to specify the name of a file that is stored in <i>installation-folder\agt\probe\cert</i> . Do not include the path. The file must be converted to Base64-encoded X.509 format.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

#1

You cannot specify an IPv6 address for the host name.

#2

This item is mandatory when the <POST> tag is specified.

#3

This item is mandatory when the <WEB_AUTH> tag is specified.

#4

This item is mandatory when the <PROXY> tag is specified.

#5

This item is mandatory when the <PROXY> tag is specified and proxy authentication is performed.

#6

This item is mandatory when the <CLIENT_AUTH> tag is specified.

(3) SMTP

This subsection describes the tags for the settings specific to the SMTP service.

(a) Format

```

<SERV_PARAM>
  <SMTP>
    <HOSTNAME>host-name-or-IP-address</HOSTNAME>
    <PORT>port-number</PORT>
    <MSG_SIZE>message-size</MSG_SIZE>
    <DST_MAIL_ADDR>destination-email-address</DST_MAIL_ADDR>
    <SRC_MAIL_ADDR>source-email-address</SRC_MAIL_ADDR>
    <POP3_AUTH>
      <POP3_HOSTNAME>POP3-host-name-or-IP-address</POP3_HOSTNAME>
      <POP3_PORT>POP3-port-number</POP3_PORT>
      <POP3_USERNAME>POP3-user-name</POP3_USERNAME>
    </POP3_AUTH>
  </SMTP>
</SERV_PARAM>

```

(b) Definition of <SERV_PARAM> (SMTP)

Table 8–13: Definition of <SERV_PARAM> (SMTP)

XML tag	Mandatory	Role of tag and value to be specified
<SMTP>...</SMTP>	Y	Contains the parameters specific to the SMTP service.
<HOSTNAME>...</HOSTNAME> ((character string of up to 255 bytes))	Y	Specifies the SMTP server's host name or IP address.
<PORT>...</PORT> ((1 to 65535))<<25>>	--	Specifies the SMTP server's port number.
<MSG_SIZE>...</MSG_SIZE> ((0 to 10000))(bytes)	Y	Specifies the size of the text for a measurement email.
<DST_MAIL_ADDR>...</DST_MAIL_ADDR> ((character string of up to 256 bytes))	Y	Specifies exactly one email address to which a measurement email is to be sent.
<SRC_MAIL_ADDR>...</SRC_MAIL_ADDR> ((character string of up to 256 bytes))	--	Specifies the email address from which a measurement email is to be sent.
<POP3_AUTH>...</POP3_AUTH>	--	Specifies that POP3 (POP before SMTP) authentication is to be performed. Use the <POP3_HOSTNAME>, <POP3_PORT>, and <POP3_USERNAME> tags to specify the settings related to POP3 authentication. To omit the specification, omit the <POP3_AUTH> tag and all the tags contained in it.
<POP3_HOSTNAME>...</POP3_HOSTNAME> ((character string of up to 255 bytes))	--#	Specifies the POP3 server's host name or IP address. This tag is applicable only when POP3 authentication is executed.
<POP3_PORT>...</POP3_PORT> ((1 to 65535))<<110>>	--#	Specifies the POP3 server's port number. This tag is applicable only when POP3 authentication is executed.
<POP3_USERNAME>...</POP3_USERNAME> ((character string of up to 40 bytes))	--#	Specifies the user name to be used for POP3 authentication. This tag is applicable only when POP3 authentication is executed.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

#

This item is mandatory when the <POP3_AUTH> tag is specified.

(4) POP3

This subsection describes the tags for the settings specific to the POP3 service.

(a) Format

```
<SERV_PARAM>
  <POP3>
    <HOSTNAME>host-name-or-IP-address</HOSTNAME>
    <PORT>port-number</PORT>
    <USERNAME>user-name</USERNAME>
    <NON_DELETE_MAIL></NON_DELETE_MAIL>
```

```
</POP3>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (POP3)

Table 8–14: Definition of <SERV_PARAM> (POP3)

XML tag	Mandatory	Role of tag and value to be specified
<POP3> . . . </POP3>	Y	Contains the parameters specific to the POP3 service.
<HOSTNAME> . . . </HOSTNAME> ((character string of up to 255 bytes))	Y	Specifies the POP3 server's host name or IP address.
<PORT> . . . </PORT> ((1 to 65535))<<110>>	--	Specifies the POP3 server's port number.
<USERNAME> . . . </USERNAME> ((character string of up to 40 bytes))	Y	Specifies the user name to be used in the POP3 service.
<NON_DELETE_MAIL> </NON_DELETE_MAIL>	--	Specifies that read emails are not to be deleted. To delete read emails, omit this tag.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

(5) IMAP4

This subsection describes the tags for the settings specific to the IMAP4 service.

(a) Format

```
<SERV_PARAM>
  <IMAP4>
    <HOSTNAME>host-name-or-IP-address</HOSTNAME>
    <PORT>port-number</PORT>
    <USERNAME>user-name</USERNAME>
    <DELETE_MAIL></DELETE_MAIL>
  </IMAP4>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (IMAP4)

Table 8–15: Definition of <SERV_PARAM> (IMAP4)

XML tag	Mandatory	Role of tag and value to be specified
<IMAP4> . . . </IMAP4>	Y	Contains the parameters specific to the IMAP4 service.
<HOSTNAME> . . . </HOSTNAME> ((character string of up to 255 bytes))	Y	Specifies the IMAP4 server's host name or IP address.
<PORT> . . . </PORT> ((1 to 65535))<<143>>	--	Specifies the IMAP4 server's port number.
<USERNAME> . . . </USERNAME> ((character string of up to 64 bytes))	Y	Specifies the user name to be used in the IMAP4 service.

XML tag	Mandatory	Role of tag and value to be specified
<DELETE_MAIL> </DELETE_MAIL>	--	Specifies that read emails are to be deleted. If you do not want to delete read emails, omit this tag.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

(6) DNS

This subsection describes the tags for the settings specific to the DNS service.

(a) Format

```
<SERV_PARAM>
  <DNS>
    <IPADDRESS>IP-address</IPADDRESS>
    <PORT>port-number</PORT>
    <QUERY>name-of-host-to-be-searched</QUERY>
    <RETRY>retries-count</RETRY>
  </DNS>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (DNS)

Table 8–16: Definition of <SERV_PARAM> (DNS)

XML tag	Mandatory	Role of tag and value to be specified
<DNS>...</DNS>	Y	Contains the parameters specific to the DNS service.
<IPADDRESS>...</IPADDRESS>	Y	Specifies the DNS server's IP address. Only the IP address is accepted; the DNS name is not accepted.
<PORT>...</PORT> ((1 to 65535))<<53>>	--	Specifies the DNS server's port number.
<QUERY>...</QUERY> ((character string of up to 255 bytes))	Y	Specifies the name of the host to be searched for that is registered on the DNS server.
<RETRY>...</RETRY> ((1 to 5))<<1>>	--	Specifies the number of retries. From this value and the timeout value specified in the <TIME_OUT> tag contained in the <GEN_PARAM> tag, the retry timeout value is determined and set automatically. The formula is as follows: Retry timeout value = timeout value/(number of retries + 1)

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

(7) DHCP

This subsection describes the tags for the settings specific to the DHCP server.

(a) Format

```
<SERV_PARAM>
  <DHCP>
    <HOSTNAME>host-name-or-IP-address</HOSTNAME>
    <PORT>port-number</PORT>
    <PROBE_PORT>probe's-port-number</PROBE_PORT>
    <NON_ACCEPT_OFFER></NON_ACCEPT_OFFER>
  </DHCP>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (DHCP)

Table 8–17: Definition of <SERV_PARAM> (DHCP)

XML tag	Mandatory	Role of tag and value to be specified
<DHCP>...</DHCP>	Y	Contains the parameters specific to the DHCP service.
<HOSTNAME>...</HOSTNAME> (character string of up to 255 bytes)	Y	Specifies the DHCP server's host name or IP address.
<PORT>...</PORT> ((1 to 65535))<<67>>	--	Specifies the DHCP server's port number.
<PROBE_PORT>...</PROBE_PORT> ((1 to 65535))<<68>>	--	Specifies the port number of the probe that is used as the DHCP client in measuring the measurement condition.
<NON_ACCEPT_OFFER> </NON_ACCEPT_OFFER>	--	Specifies that the IP address assigned from the DNS server is not to be accepted. To accept it, omit this tag.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

(8) FTP

This subsection describes the tags for the settings specific to the FTP service.

(a) Format

```
<SERV_PARAM>
  <FTP>
    <HOSTNAME>host-name-or-IP-address</HOSTNAME>
    <PORT>port-number</PORT>
    <USERNAME>user-name</USERNAME>
    <TRANS_DIRECTION>transfer-direction</TRANS_DIRECTION>
    <FILE_NAME>name-of-transferred-file</FILE_NAME>
    <PASSIVE></PASSIVE>
  </FTP>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (FTP)

Table 8–18: Definition of <SERV_PARAM> (FTP)

XML tag	Mandatory	Role of tag and value to be specified
<FTP>...</FTP>	Y	Contains the parameters specific to the FTP service.
<HOSTNAME>...</HOSTNAME> ((character string of up to 255 bytes)) ^{#1}	Y	Specifies the FTP server's host name or IP address.
<PORT>...</PORT> ((1 to 65535))<<21>>	--	Specifies the FTP server's port number.
<USERNAME>...</USERNAME> ((character string of up to 64 bytes))	Y	Specifies the user name to be used in the FTP service.
<TRANS_DIRECTION>...</TRANS_DIRECTION> ((UPLOAD or DOWNLOAD))	Y	Specifies the file transfer method. ^{#2} To transfer a file to the server, specify <code>UPLOAD</code> ; to transfer a file from the server, specify <code>DOWNLOAD</code> .
<FILE_NAME>...</FILE_NAME> ((character string of up to 32 bytes))	Y	Specifies the name of the file to be transferred.
<PASSIVE></PASSIVE>	--	Specifies the connection mode. ^{#3} This tag is used to establish data connection in the <code>PASSIVE</code> mode. To omit the specification, omit this tag. When this tag is omitted, data transfer connection is established in the <code>ACTIVE</code> mode.

Legend:

- Y: Mandatory item
- : Optional item
- (()): Specifiable value range of the tag.
- <<>>: Default value

#1

To specify an IPv4 address for the host name, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: ACE6:45:75:91::1).

#2

A transfer file for measurement must already be stored in the following folder:

For `UPLOAD`: `installation-folder\agtv\probe\probedata\ftp`

For `DOWNLOAD`: Specified account's home directory

#3

The connection establishment method depends on the connection mode, as described below:

In the `ACTIVE` mode:

The connection request for file transfer is issued from the FTP server.

In the `PASSIVE` mode:

The connection request for file transfer is issued from the FTP probe.

(9) TCP

This subsection describes the tags for the settings specific to the TCP service.

(a) Format

```
<SERV_PARAM>
  <TCP>
    <HOSTNAME>host-name-or-IP-address</HOSTNAME>
    <PORT>port-number</PORT>
```



```
</TCP>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (TCP)

Table 8–19: Definition of <SERV_PARAM> (TCP)

XML tag	Mandatory	Role of tag and value to be specified
<TCP>...</TCP>	Y	Contains the parameters specific to the TCP service.
<HOSTNAME>...</HOSTNAME> ((character string of up to 255 bytes)) [#]	Y	Specifies the TCP server's host name or IP address.
<PORT>...</PORT> ((1 to 65535))	Y	Specifies the TCP server's port number.

Legend:

Y: Mandatory item

(()): Specifiable value range of the tag.

#

To specify an IPv4 address for the host name, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: ACE6:45:75:91::1).

(10) WEBTRANS

This subsection describes the tags for the settings specific to the WEBTRANS service.

(a) Format

```
<SERV_PARAM>
  <WEBTRANS>
    <TRANSACTION_FILE>Web-transaction-file-name</TRANSACTION_FILE>
    <TRANSACTION_NAME>Web-transaction-name</TRANSACTION_NAME>
  </WEBTRANS>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (WEBTRANS)

Table 8–20: Definition of <SERV_PARAM> (WEBTRANS)

XML tag	Mandatory	Role of tag and value to be specified
<WEBTRANS>...</WEBTRANS>	Y	Contains the parameters specific to the WEBTRANS service.
<TRANSACTION_FILE>...</TRANSACTION_FILE> ((character string of up to 255 bytes))	Y	Specifies the name of the Web transaction file. Specify a file with the extension .xml that is stored in <i>installation-folder\agtv\probe\webtrans</i> . <ul style="list-style-type: none"> Do not include the path. The specified name is not case sensitive.
<TRANSACTION_NAME>...</TRANSACTION_NAME> ((character string of up to 255 bytes))	Y	Specifies the name of the Web transaction. The vertical bar character () cannot be used.

Legend:

Y: Mandatory item

(()): Specifiable value range of the tag.

(11) IESCENA

This subsection describes the tags for the settings specific to the IE scenario.

(a) Format

```
<SERV_PARAM>
  <IESCENA>
    <IESCENA_FILE>IE-scenario-file-name</IESCENA_FILE>
  </IESCENA>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (IESCENA)

Table 8–21: Definition of <SERV_PARAM> (IESCENA)

XML tag	Mandatory	Role of tag and value to be specified
<IESCENA>...</IESCENA>	Y	The tag to contain the parameters specific to the IE scenario.
<IESCENA_FILE>...</IESCENA_FILE> (character string of up to 255 bytes)	Y	Specifies the name of the IE scenario file. Specify a file with the extension .xml that is stored in <i>installation-folder\agtv\probe\iescena</i> . <ul style="list-style-type: none"> Do not include the path. The specified name is not case sensitive.

Legend:

Y: Mandatory item

(()): Specifiable value range of the tag.

(12) USERSERV

This subsection describes the tags for the settings specific to a user-defined service.

(a) Format

```
<SERV_PARAM>
  <USERSERV>
    <USER_SERVICE_ID>user-defined-service-ID</USER_SERVICE_ID>
  </USERSERV>
</SERV_PARAM>
```

(b) Definition of <SERV_PARAM> (USERSERV)

Table 8–22: Definition of <SERV_PARAM> (USERSERV)

XML tag	Mandatory	Role of tag and value to be specified
<USERSERV>...</USERSERV>	Y	Contains the parameters specific to a user-defined service.
<USER_SERVICE_ID>...</USER_SERVICE_ID> ((1 to 100))	Y	Specifies a user-defined service ID that has been registered in the command registration file.

Legend:

Y: Mandatory item

(()): Specifiable value range of the tag.

8.3.4 Example

The following is an example of a measurement condition registration file:

```
<?xml version="1.0" encoding="US-ASCII" standalone="no"?>
<!DOCTYPE TASKLIST SYSTEM "esptask.dtd">
<TASKLIST>
  <TASK>
    <GEN_PARAM>
      <TASKID>100</TASKID>
      <TASKLABEL>Response time of the top page</TASKLABEL>
      <INTERVAL>120</INTERVAL>
      <TIMEOUT>30</TIMEOUT>
    </GEN_PARAM>
    <SERV_PARAM>
      <HTTP>
        <URL>www.hitachi.co.jp:80/index.htm</URL>
        <DEPTH>1</DEPTH>
      </HTTP>
    </SERV_PARAM>
  </TASK>
  <TASK>
    <GEN_PARAM>
      <TASKID>101</TASKID>
      <TASKLABEL>Response time of the email sending</TASKLABEL>
      <INTERVAL>120</INTERVAL>
      <TIMEOUT>30</TIMEOUT>
    </GEN_PARAM>
    <SERV_PARAM>
      <SMTP>
        <HOSTNAME>smtp.hitachi.co.jp</HOSTNAME>
        <MSG_SIZE>3000</MSG_SIZE>
        <DST_MAIL_ADDR>pfmuser</DST_MAIL_ADDR>
      </SMTP>
    </SERV_PARAM>
  </TASK>
  <TASK>
    <GEN_PARAM>
      <TASKID>102</TASKID>
      <TASKLABEL>Response time of the email receiving</TASKLABEL>
      <INTERVAL>120</INTERVAL>
      <TIMEOUT>30</TIMEOUT>
    </GEN_PARAM>
    <SERV_PARAM>
      <POP3>
        <HOSTNAME>pop3.hitachi.co.jp</HOSTNAME>
        <USERNAME>pfmuser</USERNAME>
      </POP3>
    </SERV_PARAM>
  </TASK>
  <TASK>
    <GEN_PARAM>
      <TASKID>103</TASKID>
      <TASKLABEL>Monitor of the portal site</TASKLABEL>
      <INTERVAL>120</INTERVAL>
      <TIMEOUT>30</TIMEOUT>
    </GEN_PARAM>
```

```
<SERV_PARAM>
  <WEBTRANS>
    <TRANSACTION_FILE>hitachi.xml</TRANSACTION_FILE>
    <TRANSACTION_NAME>portal</TRANSACTION_NAME>
  </WEBTRANS>
</SERV_PARAM>
</TASK>
<TASK>
  <GEN_PARAM>
    <TASKID>104</TASKID>
    <TASKLABEL>Monitor of the Internet Explorer site</TASKLABEL>
    <INTERVAL>120</INTERVAL>
    <TIMEOUT>30</TIMEOUT>
  </GEN_PARAM>
  <SERV_PARAM>
    <IESCENA>
      <IESCENA_FILE>iescenal.xml</IESCENA_FILE>
    </IESCENA>
  </SERV_PARAM>
</TASK>
</TASKLIST>
```

8.4 Web Recorder action condition definition file (wr.conf)

The Web Recorder action condition definition file is used to define the Web Recorder's action conditions. This file is read when the Web Recorder starts.

8.4.1 Format

```
[Web Recorder]
IE_flag={Y|N}
web_rec_browser_mode=Internet-Explorer-version-for-using-Web-Recorder
```

Note:

The following notes apply to specifying the Web Recorder action condition definition file:

- Each key name and its value must be connected by an equal sign (=).
- Each key name and its value must be specified on a single line.
- The specification must begin in column 1.

A line beginning with a hash mark (#) is treated as a comment line.

8.4.2 Definition

Web Recorder section:

Defines an item related to the Web Recorder.

Table 8–23: Definition in the Web Recorder section

Key name	Mandatory	Value to be specified
IE_flag ((Y or N))<<Y>>	--	Specifies whether or not the Internet Explorer is to be started. To start the Internet Explorer, specify Y; otherwise, specify N.
web_rec_browser_mode# ((IE7, IE8, IE9, IE10 or IE11))	--	Specifies the Internet Explorer version for using the Web Recorder. Before specifying this item, check the Internet Explorer version supported by the monitoring target and the version of Internet Explorer installed in an environment in which PFM - Agent for Service Response is installed. Internet Explorer 7 is the default version. <ul style="list-style-type: none">• IE7 Specify this when the monitoring target supports Internet Explorer 7.• IE8 Specify this when the monitoring target supports Internet Explorer 8.• IE9 Specify this when the monitoring target supports Internet Explorer 9. You can specify this option when Internet Explorer 9 or a later version is installed in an environment in which PFM - Agent for Service Response is installed.• IE10 Specify this when the monitoring target supports Internet Explorer 10. You can specify this option when Internet Explorer

Key name	Mandatory	Value to be specified
web_rec_browser_mode# ((IE7, IE8, IE9, IE10 or IE11))	--	<p>10 or a later version is installed in an environment in which PFM - Agent for Service Response is installed.</p> <ul style="list-style-type: none"> IE11 <p>Specify this when the monitoring target supports Internet Explorer 11. You can specify this option when Internet Explorer 11 or a later version is installed in an environment in which PFM - Agent for Service Response is installed.</p> <p>If a value is not specified or if an invalid value is specified, the default version (Internet Explorer 7) is used.</p>

Legend:

--: Optional item

(()): Specified value range of the tag

<< >>: Default value

#

Do not specify version of Internet Explorer that PFM - Agent for Service Response does not support.

8.4.3 Example

The following is an example of a Web Recorder action condition definition file:

```
[Web Recorder]
IE_flag=Y
web_rec_browser_mode=
```

8.5 Web transaction files

A Web transaction file is used to define a series of Web access information items. Multiple Web transactions can be defined in a single Web transaction file. You use a program such as a text editor to create a Web transaction file in the format shown below. You give it a name of your choosing (with the extension `.xml`), and you store it under `installation-folder\agtv\probe\webtrans`.

To apply the definitions specified in a Web transaction file, you must restart PFM - Agent for Service Response.

You can also use Web Recorder to create Web transaction files. For details about how to use Web Recorder to create a Web transaction file, see [4.4.1 Defining Web transactions \(creating Web transaction files\)](#).

8.5.1 Format and definition of the overall Web transaction file

(1) Format

```
<?xml version="1.0" encoding="US-ASCII" standalone="no"?>
<!DOCTYPE TRANSACTION_LIST SYSTEM "espwebtrans.dtd">
<TRANSACTION_LIST>
  <TRANSACTION>
    <TRANSACTION_PARAM>
      <!-- TRANSACTION_PARAM -->
    </TRANSACTION_PARAM>

    <STEP>
      <!-- STEP -->
    </STEP>
    ...
  </TRANSACTION>
  ...
</TRANSACTION_LIST>
```

(2) Definition

(a) XML declaration and document type declaration

Specify the XML declaration on the first line and the document type declaration on the second line. Specify exactly as shown below:

```
<?xml version="1.0" encoding="encoding-type" standalone="no"?>
<!DOCTYPE TRANSACTION_LIST SYSTEM "espwebtrans.dtd">
```

Specify either of `Shift_JIS`, `EUC-JP`, `ISO-2022-JP`, `UTF-8`, `US-ASCII`, or `GB18030`[#] as the encoding type, and then declare the Web transaction file with the specified encoding type.

#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

(b) XML definition

Table 8–24: XML definition

XML tag	Mandatory	Role of tag and value to be specified
<TRANSACTION_LIST>...</TRANSACTION_LIST>	Y	Indicates a list of transactions. This tag contains one or more <TRANSACTION> tags. A new <TRANSACTION> tag can start immediately after a </TRANSACTION> tag.
<TRANSACTION>...</TRANSACTION>	Y	Indicates a single item of transaction information. This tag contains one <TRANSACTION_PARAM> tag and one or more <STEP> tags.
<TRANSACTION_PARAM>...</TRANSACTION_PARAM>	Y	Indicates the parameters that define transaction measurement conditions. This tag contains the <TRANSACTION_NAME>, <TRANSACTION_COMMENT>, <DEFAULT_CHARSET>, <HTML_OUT>, <IGNORE_EMBEDDED_RESOURCE>, <NO_CACHE>, <KEEP_ALIVE>, <DEFAULT_PROXY>, and <USER_AGENT> tags. Some of these tags can be omitted. For details, see 8.5.2(1) <TRANSACTION_PARAM> tag.
<STEP>...</STEP>	Y	Indicates an information item for a single step. This tag contains the <STEP_ID>, <TITLE>, <FRAME_NAME>, <CHARSET>, <REQUEST>, <WEB_AUTH>, <PROXY>, <RESPONSE_PATTERN>, <VARIABLE>, <START_SCOPE>, and <END_SCOPE> tags. For details, see 8.5.2(2) <STEP> tag.

Legend:

Y: Mandatory item

8.5.2 Format and definition of the Web transaction measurement conditions

(1) <TRANSACTION_PARAM> tag

The <TRANSACTION_PARAM> tag specifies settings related to the measurement conditions for the Web transaction.

(a) Format

```

<TRANSACTION_PARAM>
  <TRANSACTION_NAME>Web-transaction-name</TRANSACTION_NAME>
  <TRANSACTION_COMMENT>comment</TRANSACTION_COMMENT>
  <DEFAULT_CHARSET>character-set</DEFAULT_CHARSET>
  <HTML_OUT></HTML_OUT>
  <IGNORE_EMBEDDED_RESOURCE></IGNORE_EMBEDDED_RESOURCE>
  <NO_CACHE></NO_CACHE>
  <KEEP_ALIVE></KEEP_ALIVE>
  <DEFAULT_PROXY>
    <PROXY_HOSTNAME>connection-target-proxy-host-name-or-IP-address</
PROXY_HOSTNAME>
    <PROXY_PORT>connection-target-proxy's-port-number</PROXY_PORT>
    <PROXY_USERNAME>user-name-used-for-proxy-authentication</PROXY_USERNAME>
    <PROXY_PASSWORD>password-used-for-proxy-authentication</PROXY_PASSWORD>
  </DEFAULT_PROXY>
  <SSL_AUTH_IGNORE></SSL_AUTH_IGNORE>
  <CLIENT_AUTH>
    <CLIENT_CERT_FILE>client-certificate-file-name</CLIENT_CERT_FILE>

```



```

    <CLIENT_CERT_PASSWORD>private-key-password</CLIENT_CERT_PASSWORD>
  </CLIENT_AUTH>
  <USER_AGENT>user-agent-name</USER_AGENT>
</TRANSACTION_PARAM>

```

(b) Definition

Table 8–25: Definition of <TRANSACTION_PARAM>

XML tag	Mandatory	Role of tag and value to be specified
<TRANSACTION_NAME>... </TRANSACTION_NAME> ((1 to 255 bytes of character string))	Y	Specifies the Web transaction name. Each Web transaction must have a unique name within the same Web transaction file. A Web transaction name cannot contain the vertical bar () character.
<TRANSACTION_COMMENT>... </TRANSACTION_COMMENT> ((0 to 255 bytes of character string))	--	Specifies a comment for the transaction.
<DEFAULT_CHARSET>... </DEFAULT_CHARSET> ((Shift_JIS EUC-JP ISO-2022-JP UTF-8 GB18030#8))	--	Specifies the default character set for an HTML file that is acquired by this transaction. The specifiable values are Shift_JIS, EUC-JP, ISO-2022-JP, UTF-8, and GB18030. The character set specified in the <DEFAULT_CHARSET> tag is assumed for HTML acquired by a step in this transaction for which the <CHARSET> tag is not specified. When the character set does not specified in the <DEFAULT_CHARSET> tag, Shift_JIS is assumed for Japanese OS, GB18030 is assumed for Chinese OS and US-ASCII is assumed for other OS.
<HTML_OUT> </HTML_OUT>#1	--	Specifies that you output the HTTP header and HTML acquired by this transaction to a file. The output data can be used as a reference when you specify the response determination and definition of variable strings. The system outputs only HTML acquired by a step for which the <STEP_ID> tag is specified within the <STEP> tag. HTML acquired by a step for which the <STEP_ID> tag is omitted will not be output. If the attribute of the acquired file is not HTML, then the file is not output. The following shows the output destination folder and the file name: The output destination folder: <ul style="list-style-type: none"> When the file is output by Probe Daemon <i>installation-folder\agtv\probe\probedata\webtrans</i> When the file is output by the test command (jpcvtest) <i>installation-folder\agtv\probe\probedata\webtrans_cmd</i> The file name (for HTML): <i>step-identifier.html</i> The file name (for HTTP header): <i>step-identifier.hdr</i> If the same file name already exists, that file will be overwritten unconditionally. When you specify the <HTML_OUT> tag, you must be careful to treat the output data because it may contain personal information.
<IGNORE_EMBEDDED_RESOURCE> </IGNORE_EMBEDDED_RESOURCE>#1	--	Specifies that resources embedded in the acquired page are to be ignored.
<NO_CACHE> </NO_CACHE>#1	--	Specifies that the cache is not to be referenced in HTTP(S) requests.

XML tag	Mandatory	Role of tag and value to be specified
<KEEP_ALIVE> </KEEP_ALIVE>#1	--	Specifies that the keep alive mode is to be used in HTTP(S) requests.
<DEFAULT_PROXY>... </DEFAULT_PROXY>	--	Specifies that a proxy is to be used. This tag contains the <PROXY_HOSTNAME>, <PROXY_PORT>, <PROXY_USERNAME>, and <PROXY_PASSWORD> tags. This tag is used to specify the default proxy settings for the overall transaction. To omit the specification, omit the <DEFAULT_PROXY> tag and all the tags contained in it.
<PROXY_HOSTNAME>... </PROXY_HOSTNAME> ((1 to 255 bytes of character string))#2	..#3	Specifies the default proxy server's host name or IP address.
<PROXY_PORT>... </PROXY_PORT> ((1 to 65535))	..#3	Specifies the default proxy server's port number.
<PROXY_USERNAME>... </PROXY_USERNAME> ((1 to 64 bytes of character string))	..#4	Specifies the user name when proxy authentication is to be performed at the default proxy server. Omitting this tag means that proxy authentication is not to be performed.
<PROXY_PASSWORD>... </PROXY_PASSWORD> ((0 to 64 bytes of character string))	..#5	Specifies the password when proxy authentication is to be performed at the default proxy server. Specifying a character string with a length of 0 bytes means that the null character string is to be used as the password. Omitting this tag means that the password set by the password utility is to be used.
<SSL_AUTH_IGNORE></SSL_AUTH_IGNORE>#1	--	Specifies that measurement is to continue if SSL server authentication fails when an HTTPS request is issued. To terminate measurement when SSL server authentication fails, omit this tag.
<CLIENT_AUTH>... </CLIENT_AUTH>	--	Specifies that client authentication is to be performed when an HTTPS request is issued. Use the <CLIENT_CERT_FILE> and <CLIENT_CERT_PASSWORD> tags to specify the settings related to client authentication. To omit the specification, omit the <CLIENT_AUTH> tag and all the tags contained in it.
<CLIENT_CERT_FILE>... </CLIENT_CERT_FILE> ((1 to 255 bytes of character string))	..#6	Specifies the file in which the client certificate and private key are stored. Specify the name of a file that is stored in <i>installation-folder</i> \agtv\probe\cert. Do not include the path. The file must be converted to Base64-encoded X.509 format.
<CLIENT_CERT_PASSWORD>... </CLIENT_CERT_PASSWORD> ((0 to 1,023 bytes of character string))	..#7	Specifies the private key password for the client certificate when client authentication is performed. If you specify this item, we recommend that you have registered a password by using the password utility. Specifying a character string with a length of 0 bytes means that the null character string is to be used as the password. Omitting this tag means that the password set by the password utility is to be used.
<USER_AGENT>... </USER_AGENT> ((1 to 255 bytes of character string)) <<PFM - Agent for Service Response (Windows)>>	--	Specifies the user agent name. Use this tag when accessible user agent names are limited.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

#1

You cannot specify any elements (including spaces or line breaks) within tags. If elements are specified within tags, the Web Recorder cannot open the Web transaction file.

#2

To specify an IPv4 address for the host name, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: ACE6:45:75:91::1).

#3

This is a mandatory item when a proxy is to be used.

#4

This is a mandatory item when proxy authentication is to be performed with a proxy.

#5

This is a mandatory item when proxy authentication is to be performed and the password has not been registered by the password utility.

#6

This is a mandatory item when client authentication is to be performed.

#7

This is a mandatory item when client authentication is to be performed and a password has not been registered by using the password utility.

#8

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

(2) <STEP> tag

The <STEP> tag specifies step information for the Web transaction.

(a) Format

```
<STEP>
  <STEP_ID>step-identifier</STEP_ID>
  <TITLE>page-title</TITLE>
  <FRAME_NAME>frame-name</FRAME_NAME>
  <CHARSET>character-set</CHARSET>
  <REQUEST>
    <REQUEST_CHARSET>character-set</REQUEST_CHARSET>
    <URL>URL-to-be-accessed</URL>
    <POST>
      <CONTENT_TYPE>

        When sending the message body as:
        application/x-www-form-urlencoded
        <FORM_URLENCODED></FORM_URLENCODED>

        When sending the message body as:
        text/plain
        <TEXT_PLAIN></TEXT_PLAIN>

        When sending the message body as:
        multipart/form-data
        <MULTIPART_FORM_DATA>
          <BOUNDARY>separator-for-message-body</BOUNDARY>
        </MULTIPART_FORM_DATA>

        When sending the message body as:
        a value other than the above
        <OTHER>Content-Type</OTHER>

      </CONTENT_TYPE>
    <MESSAGE_BODY>message-body</MESSAGE_BODY>
  </POST>
  <COOKIE>Cookie-header</COOKIE>
```

```

</REQUEST>
<WEB_AUTH>
  <WEB_USERNAME>user-name-used-for-Web-authentication</WEB_USERNAME>
  <WEB_PASSWORD>password-used-for-Web-authentication</WEB_PASSWORD>
</WEB_AUTH>
<PROXY>

  When a proxy is not used:
  <PROXY_NOUSE></PROXY_NOUSE>

  When using a non-default proxy:
  <PROXY_HOSTNAME>connection-target-proxy-host-name-or-IP-address</
PROXY_HOSTNAME>
  <PROXY_PORT>connection-target-proxy's-port-number</PROXY_PORT>
  <PROXY_USERNAME>user-name-used-for-proxy-authentication</PROXY_USERNAME>
  <PROXY_PASSWORD>password-used-for-proxy-authentication</PROXY_PASSWORD>

</PROXY>
<RESPONSE_PATTERN>condition-used-for-response-determination</
RESPONSE_PATTERN>
<VARIABLE>
  <!--VARIABLE -->
</VARIABLE>
<START_SCOPE>start-scope-name</START_SCOPE>
...
<END_SCOPE>end-scope-name</END_SCOPE>
...
</STEP>

```

(b) Definition

Table 8–26: Definition of <STEP>

XML tag	Mandatory	Role of tag and value to be specified
<STEP_ID>... </STEP_ID> (1 to 255 bytes of alphanumeric characters, hyphen, underscore, and space)	--	Defines a unique step identifier for identifying the step. This item must be specified if the HTML acquired by the step contains a substitute string for a variable string in the message body, and for the URL for the subsequent step; or if HTML is to be output to a file, and the HTML acquired by this step is to be output. If HTML is to be output to a file, this identifier is used in the file name; therefore, make sure that the specified step identifier is unique in all the defined transactions.
<TITLE>...</TITLE> (0 to 1,023 bytes of character string)	--	Defines the title for the page that is acquired by this step.
<FRAME_NAME>... </FRAME_NAME> (0 to 1,023 bytes of character string)	--	Defines the frame name for the page that is acquired by this step.
<CHARSET>... </CHARSET> (Shift_JIS EUC-JP ISO-2022-JP UTF-8 GB18030#13)	--	Specifies the character set for the HTML file that is acquired by this step. The specifiable values are Shift_JIS, EUC-JP, ISO-2022-JP, UTF-8, and GB18030. If this item is omitted, the default character set for this transaction is used. If the character set name is not specified correctly, substitute string search and response determination may fail.
<REQUEST>... </REQUEST>	Y	Specifies the request-related settings for this step. Use the <REQUEST_CHARSET>, <URL>, <POST>, and <COOKIE> tags.

XML tag	Mandatory	Role of tag and value to be specified
<REQUEST_CHARSET>... </REQUEST_CHARSET> ((Shift_JIS EUC-JP ISO-2022-JP UTF-8 GB18030#13))	--	Specifies the character set of request information sent at this step (URL, message body, cookie). The specifiable values are Shift_JIS, EUC-JP, ISO-2022-JP, UTF-8, and GB18030. The request information is encoded to send by the character set specified in this tag, not the character set specified in the XML declaration. If all the request information is defined by the ASCII code, you do not need to specify this item. If this tag is omitted, the request information is encoded by Shift_JIS on Japanese OS, GB18030 on Chinese OS, or US-ASCII on the other OS and sent. If you specify ISO-2022-JP in this item, you cannot specify the multibyte characters in the <URL> tag of the <STEP> tag. You cannot specify the variable strings.
<URL>...</URL> ((1 to 2,083 bytes of character string))#1	Y	Specifies the URL to be acquired by this step. This URL specification must include the protocol identifier (http:// or https://).
<POST>...</POST>	--	Specifies that the POST method is to be used. Use the <CONTENT_TYPE> and <MESSAGE_BODY> tags to specify the settings needed for using the POST method. When this item is omitted, the GET method is used.
<CONTENT_TYPE>... </CONTENT_TYPE>	..#2	Specifies Content-Type for using the POST method. For the element, specify one of the <FORM_URLENCODED>, <TEXT_PLAIN>, <MULTIPART_FORM_DATA>, or <OTHER> tag.
<FORM_URLENCODED> </FORM_URLENCODED>#3	..#4	Specifies that the message body is to be notified as application/x-www-form-urlencoded when the POST method is used.
<TEXT_PLAIN> </TEXT_PLAIN>#3	..#4	Specifies that the message body is to be notified as text/plain when the POST method is used.
<MULTIPART_FORM_DATA>... </MULTIPART_FORM_DATA>	..#4	Specifies that the message body is to be notified as multipart/form-data when the POST method is used. If you specify this item, you must use the <BOUNDARY> tag to specify the separator for the message body.
<BOUNDARY>...</BOUNDARY> ((1 to 255 bytes of character string))	..#5	Specifies the separator for the message body that is to be notified as multipart/form-data.
<OTHER>...</OTHER> ((1 to 255 bytes of character string))	..#4	Specifies a desired Content-Type when the Content-Type of the message body to be notified by the POST method is neither application/x-www-form-urlencoded, nor text/plain, nor multipart/form-data.
<MESSAGE_BODY>...</MESSAGE_BODY> ((0 to 512,000 bytes of character string))	..#2	Specifies the message body to be notified by the POST method.
<COOKIE>... </COOKIE> ((0 to 1,023 bytes of character string))	--	Specifies that a specific cookie is to be set for this step's request. Normally, there is no need to specify this item. Specify the value in the format <i>variable-name=value</i> . To define multiple cookies, specify as many <COOKIE> tags as there are cookies, up to a maximum of eight.
<WEB_AUTH>... </WEB_AUTH>	..#14	Specifies that Web authentication is to be performed during acquisition of this step. Use the <WEB_USERNAME> and <WEB_PASSWORD> tags to specify the settings related to Web authentication. To omit the specification, omit the <WEB_AUTH> tag and all the tags contained in it.

XML tag	Mandatory	Role of tag and value to be specified
<WEB_USERNAME>... </WEB_USERNAME> (1 to 64 bytes of character string)	..#6	Specifies the user name when Web authentication is to be performed.
<WEB_PASSWORD>... </WEB_PASSWORD> ((0 to 64 bytes of character string))	..#7	Specifies the password needed for Web authentication. Specifying a character string with a length of 0 bytes means that the null character string is to be used as the password. Omitting this tag means that the password set by the password utility is to be used.
<PROXY>...</PROXY>	--	Specifies the proxy settings to be used by this step. There are two ways to specify the proxy settings: using the <PROXY_NOUSE> tag; and, using the <PROXY_HOSTNAME>, <PROXY_PORT>, <PROXY_USERNAME>, and <PROXY_PASSWORD> tags. If this item is omitted, the default proxy settings for the transaction are used. To omit the specification, omit the <PROXY> tag and all the tags contained in it.
<PROXY_NOUSE> </PROXY_NOUSE>#3	--	Specifies that a proxy is not to be used in the measurement in this step.
<PROXY_HOSTNAME>... </PROXY_HOSTNAME> (1 to 255 bytes of character string)#8	..#9, #10	Specifies the proxy server's host name or IP address when non-default proxy settings are to be used in the measurement in this step.
<PROXY_PORT>... </PROXY_PORT> (1 to 65535)	..#9, #10	Specifies the proxy server's port number that is to be used in the measurement in this step.
<PROXY_USERNAME>... </PROXY_USERNAME> (1 to 64 bytes of character string)	..#11	Specifies the user name when proxy authentication is to be performed at the proxy server that is used for this step measurement. Omitting this tag means that proxy authentication is not to be performed.
<PROXY_PASSWORD>... </PROXY_PASSWORD> ((0 to 64 bytes of character string))	..#12	Specifies the password when proxy authentication is to be performed at the proxy server that is used for this step measurement. If the password has already been registered by the password utility, there is no need to specify this tag. Specifying a character string with a length of 0 bytes means that the null character string is to be used as the password. Omitting this tag means that the password set by the password utility is to be used.
<RESPONSE_PATTERN>... </RESPONSE_PATTERN > ((0 to 1,023 bytes of character string))	--	Specifies the condition to be used for response determination in this step according to the following rules: <ul style="list-style-type: none"> Permitted operators are * (AND) and + (OR). A permitted character string must be enclosed by { and }. A character string that is not permitted must be enclosed by ! { and }. Parentheses (()) may be used to indicate that * (AND) takes precedence over + (OR). A set of parentheses (()) indicating priority must contain at least one operator. It is not permissible to specify multiple consecutive left parentheses (()) to indicate priority. Define a condition that does not satisfy the condition in the parentheses (()) indicating priority as shown below: Example 1: Condition that does not satisfy ({aaa}*{bbb}) : (! {aaa}+! {bbb}) Example 2: Condition that does not satisfy ({aaa}+{bbb}) : (! {aaa} *! {bbb}) Specification example:

XML tag	Mandatory	Role of tag and value to be specified
<RESPONSE_PATTERN>... </RESPONSE_PATTERN > (0 to 1,023 bytes of character string)	--	Success is included, but Error is not included: {Success}*!{Error}
<VARIABLE>... </VARIABLE>	--	Specifies the variable string settings if you use the variable string at this step. Use the following tags to specify the variable string: <ul style="list-style-type: none"> • <VARIABLE_TARGET> tag • <SUBSTITUTE_TARGET> tag or <SUBSTITUTE_COMMAND> tag • <SUBSTITUTE_FORCE_URL_ENCODE> tag To specify multiple variable strings, use multiple <VARIABLE> tags. If you omit the specification, you omit the <VARIABLE> tag and all the tags contained in it. When you omit the specification, no variable string is set in this step. For details about <VARIABLE> tag, see (3) <VARIABLE> tag within a <STEP> tag.
<START_SCOPE>... </START_SCOPE>	--	Specifies the scope name to be used for a scope start point. The scope name must be one of the following: SCOPE1, SCOPE2, SCOPE3, SCOPE4, SCOPE5, SCOPE6, SCOPE7, or SCOPE8. To specify multiple starting scope names, use multiple <START_SCOPE> tags.
<END_SCOPE>... </END_SCOPE>	--	Specifies the scope name to be used for a scope end point. The scope name must be one of the following: SCOPE1, SCOPE2, SCOPE3, SCOPE4, SCOPE5, SCOPE6, SCOPE7, or SCOPE8. To specify multiple ending scope names, use multiple <END_SCOPE> tags.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

<<>>: Default value

#1

To use an IP address to specify the host name, use an IPv4 dotted-decimal address (for example: 172.16.233.12/example.html) or an IPv6 hexadecimal address enclosed in square brackets, using colons as separators (for example: [ACE6:45:75:91::1]/example.html).

Note that monitoring HTTPS pages is not supported in environments that use IPv6 for communications. For this reason, when monitoring HTTPS pages, you cannot specify an IPv6 address for the host name.

#2

This is a mandatory item when the POST method is to be used.

#3

You cannot specify any elements (including spaces or line breaks) within tags. If elements are specified within tags, the Web Recorder cannot open the Web transaction file.

#4

When the POST method is to be used, specify one of the <FORM_URL_ENCODED>, <TEXT_PLAIN>, <MULTIPART_FORM_DATA>, or <OTHER> tags.

#5

This is a mandatory item when <MULTIPART_FORM_DATA> is specified.

#6

This is a mandatory item when Web authentication is to be performed.

#7

This is a mandatory item when Web authentication is to be performed, but the password has not been registered by the password utility.

#8

To specify an IPv4 address for the host name, use dotted-decimal format (for example: 172.16.233.12). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: ACE6:45:75:91::1).

Note that monitoring HTTPS pages is not supported in environments that use IPv6 for communications. For this reason, when monitoring HTTPS pages, you cannot specify an IPv6 address for the host name.

#9

This item cannot be specified when you have specified the <PROXY_NOUSE> tag.

#10

This is a mandatory item when you use a specific proxy instead of the default proxy.

#11

This is a mandatory item when proxy authentication is to be performed without using the default proxy.

#12

This is a mandatory item when proxy authentication is to be performed without using the default proxy, but the password has not been registered by the password utility.

#13

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

#14

If multiple steps exist for accessing a Web server that requires Web authentication, each step requires a setting for Web authentication.

(3) <VARIABLE> tag within a <STEP> tag

The <VARIABLE> tag sets a variable string and substitute string in step information for the Web transaction. The substitute string is specified in the <SUBSTITUTE_TARGET> tag within the <VARIABLE> tag.

(a) Format

<VARIABLE> tag format

```
<VARIABLE>
  <VARIABLE_TARGET>
    <VARIABLE_TYPE>location-of-variable-string</VARIABLE_TYPE>
    <VARIABLE_PART>variable-part</VARIABLE_PART>
  </VARIABLE_TARGET>

If the received data contains the substitute string:
  <SUBSTITUTE_TARGET>
    <!-- SUBSTITUTE_TARGET -->
  </SUBSTITUTE_TARGET>

If you execute the command to acquire the substitute string:
  <SUBSTITUTE_COMMAND>
    <TARGET_COMMAND_LINE>executing-command-line</TARGET_COMMAND_LINE>
    <TARGET_COMMAND_ARG>
      <SUBSTITUTE_TARGET>
        <!-- SUBSTITUTE_TARGET -->
      </SUBSTITUTE_TARGET>
    </TARGET_COMMAND_ARG>
    . . .
  </SUBSTITUTE_COMMAND>

  <SUBSTITUTE_FORCE_URL_ENCODE></SUBSTITUTE_FORCE_URL_ENCODE>

</VARIABLE>
```

<SUBSTITUTE_TARGET> tag format


```
<SUBSTITUTE_TARGET>
  <TARGET_STEP_ID>step-specification</TARGET_STEP_ID>
```

If the acquired HTML contains the substitute string:

```
<TARGET_ELEMENT>
  <TARGET_ELEMENT_NAME>name-of-element-containing-substitute-string </
TARGET_ELEMENT_NAME>
  <TARGET_ELEMENT_ATTRIBUTE>
attribute-of-element-containing-substitute-string
  </TARGET_ELEMENT_ATTRIBUTE>
  ...
  <TARGET_ELEMENT_CONTENT>
character-string-in-contents-of-element-that-contains-substitute-string
  </TARGET_ELEMENT_CONTENT>
  ...
  <TARGET_ELEMENT_POSITION>
location-of-element-from-beginning-when-multiple-elements-match-the-
above-condition
  </TARGET_ELEMENT_POSITION>
</TARGET_ELEMENT>
<SUBSTITUTE_TYPE>
```

When the substitute string is contained in the element's contents
 <TYPE_CONTENT></TYPE_CONTENT>

When the substitute string is contained in the element's attribute
 value

```
<TYPE_ATTRIBUTE>name-of-attribute-containing-substitute-string</
TYPE_ATTRIBUTE>

</SUBSTITUTE_TYPE>
```

If the acquired HTML header contains the substitute string:

```
<TARGET_HEADER>
  <TARGET_HEADER_NAME>
name-of-header-containing-substitute-string
  </TARGET_HEADER_NAME>
  <TARGET_HEADER_VALUE>
value-of-header-containing-substitute-string
  </TARGET_HEADER_VALUE>
</TARGET_HEADER>
<SUBSTITUTE_RANGE>
  <BEFORE_RANGE>character-string-just-before-substitute-string</
BEFORE_RANGE>
  <AFTER_RANGE>character-string-just-after-substitute-string</
AFTER_RANGE>
</SUBSTITUTE_RANGE>
</SUBSTITUTE_TARGET>
```

(b) Definition

Table 8–27: Definition of <VARIABLE>

XML tag	Mandatory	Role of tag and value to be specified
<VARIABLE_TARGET>... </VARIABLE_TARGET>	Y	Specifies a variable string. This tag contains the <VARIABLE_TYPE> tag and <VARIABLE_PART> tags.

XML tag	Mandatory	Role of tag and value to be specified
<VARIABLE_TARGET>... </VARIABLE_TARGET>	Y	The variable string specified in this tag cannot even partially duplicate the variable string specified in the <VARIABLE_TARGET> tag contained in any other <VARIABLE> tag defined in this step.
<VARIABLE_TYPE>... </VARIABLE_TYPE> ((URL MESSAGE_BODY COOKIE))	Y	Specifies either URL, MESSAGE_BODY, or COOKIE as the value of the variable string.
<VARIABLE_PART>... </VARIABLE_PART> ((1 to 4095 bytes of character string))	Y	Specifies the variable part. This must be a variable string during recording that is in the value specified in <VARIABLE_TYPE> tag. If there are multiple applicable character strings, the search is conducted from the beginning, and only the first matching character string becomes the variable string during recording. Example: Dynamic session management is performed, and during recording, the session ID (variable string) is 0123456789 and the recorded URL is as follows: http://www.jp1.hitachi.co.jp/sample.cgi?id=0000&sessionid=0123456789 In this example, specify 0123456789 in <VARIABLE_PART> tag. Hitachi recommends that you should replace the variable string in the URL or message body with \$VAR1\$ or \$VAR2\$ in the following case: <ul style="list-style-type: none"> To replace multiple character strings. A variable string is multibyte characters. You specify the character code other than Shift_JIS (in a Japanese environment) or GB18030 (in a Chinese environment) in the <REQUEST_CHARSET> tag at same <STEP> tag. In this case, if the multibyte characters are specified in the <VARIABLE_PART> tag, the variable strings may not be recognized correctly.
<SUBSTITUTE_TARGET>... </SUBSTITUTE_TARGET>	..#1	Specifies a substitute string. This tag contains the <TARGET_STEP_ID>, <TARGET_ELEMENT>, <SUBSTITUTE_TYPE>, <TARGET_HEADER>, and <SUBSTITUTE_RANGE> tags. For details, see Table 8-28 .
<SUBSTITUTE_COMMAND>... </SUBSTITUTE_COMMAND>	..#1	Specifies the command to be executed for acquiring the substitute strings. This tag contains the <TARGET_COMMAND_LINE> and <TARGET_COMMAND_ARG> tags.
<TARGET_COMMAND_LINE>... </TARGET_COMMAND_LINE> ((1 or greater bytes of character string))	..#2	Specifies the command line to be executed for acquiring the substitute strings. You can specify the command to be executed and the arguments that do not change dynamically. The return value (exit code) of the command must be 0, if the command successfully terminates. If the return value (exit code) is other than 0, it is judged that the command terminates abnormally. If the command terminated abnormally or failed to be executed, the variable string specified by using the <VARIABLE_PART> tag is replaced with a null character. Hitachi recommends that the path to the command is surrounded by ";. If the path to the command is not surrounded by "; and contains the spaces, the command may fail to be executed.
<TARGET_COMMAND_ARG>... </TARGET_COMMAND_ARG>	--	Specifies this tag when you add the arguments to the command line specified by the <TARGET_COMMAND_LINE> tag. This tag contains the <SUBSTITUTE_TARGET> tag.

XML tag	Mandatory	Role of tag and value to be specified
<TARGET_COMMAND_ARG>... </TARGET_COMMAND_ARG>	--	The arguments to be added are cut down from the data received by using the <SUBSTITUTE_TARGET> tag. The character string cut down is surrounded by the double quotation marks (") and added to the command line as an argument. To add multiple arguments, specify multiple <TARGET_COMMAND_ARG> tags.
<SUBSTITUTE_FORCE URLENCODE> </SUBSTITUTE_FORCE URLENCODE>#3	--	Specifies this tag if you URL encode all the character string (including the characters used as delimiters in the URL) when the variable string is replaced with the substitute string. When you specify this tag, the characters are URL encoded as follows: Alphanumeric characters, *, -, ., @, _ Not encoded. Space Encoded to +. Other characters listed above Encoded into three characters in the format of "%xy" for each byte (x and y are the hex numbers with each one representing 4-bit).

Legend:

Y: The item is mandatory when the <VARIABLE> tag is specified.

--: The item is optional when the <VARIABLE> tag is specified.

(()): Specifiable value range of the tag.

#1

Specify either the <SUBSTITUTE_TARGET> tag or the <SUBSTITUTE_COMMAND> tag.

#2

The item is mandatory when you specify the <SUBSTITUTE_COMMAND> tag.

#3

You cannot specify any elements (including spaces or line breaks) within tags. If elements are specified within tags, the Web Recorder cannot open the Web transaction file.

Table 8–28: Definition of <SUBSTITUTE_TARGET>

XML tag	Mandatory	Role of tag and value to be specified
<TARGET_STEP_ID>... </TARGET_STEP_ID> (1 to 255 bytes of alphanumeric characters, hyphen, underscore, and space)	Y	Specifies the identifier of the step that acquires an HTML file containing the <i>substitute</i> string. The specified step identifier must be defined in the step preceding this step.
<TARGET_ELEMENT>... </TARGET_ELEMENT>	..#1	Identifies the element containing the <i>substitute</i> string within the HTML file that is acquired by the step specified in <TARGET_STEP_ID> tag. This tag contains the <TARGET_ELEMENT_NAME>, <TARGET_ELEMENT_ATTRIBUTE>, <TARGET_ELEMENT_CONTENT>, and <TARGET_ELEMENT_POSITION> tags. If the element cannot be identified by the <TARGET_ELEMENT_NAME> tag, you must specify all or some of the <TARGET_ELEMENT_ATTRIBUTE>, <TARGET_ELEMENT_CONTENT>, and <TARGET_ELEMENT_POSITION> tags so that the element that contains the <i>substitute</i> string can be identified.
<TARGET_ELEMENT_NAME>... </TARGET_ELEMENT_NAME> (1 to 1023 bytes of character string)	..#2	Specifies the name of the element that contains the <i>substitute</i> string. This name is not case sensitive. The system does not check whether or not the specified element name is a valid HTML element; the

XML tag	Mandatory	Role of tag and value to be specified
<TARGET_ELEMENT_NAME>... </TARGET_ELEMENT_NAME> (1 to 1023 bytes of character string)	..#2	system assumes that the specified character string is an element name. Example: To specify an INPUT element (<INPUT ... />), specify INPUT in the <TARGET_ELEMENT_NAME> tag.
<TARGET_ELEMENT_ATTRIBUTE>... </TARGET_ELEMENT_ATTRIBUTE> (1 to 1023 bytes of character string)	--	Specifies a single attribute of the element that contains the <i>substitute</i> string. This item is specified when the element cannot be identified by <TARGET_ELEMENT_NAME> tag alone (such as when multiple elements have the value specified in <TARGET_ELEMENT_NAME> tag), but when specifying the element's attribute can identify or narrow down the target element. Do not specify an attribute that changes dynamically. Note that validity checking is not performed on the specified attribute name and value. Specify the value in the format <i>attribute-name=attribute-value</i> . <i>attribute-name</i> is not case sensitive, but <i>attribute-value</i> is case sensitive. To specify multiple attributes, specify multiple <TARGET_ELEMENT_ATTRIBUTE> tags.
<TARGET_ELEMENT_CONTENT>... </TARGET_ELEMENT_CONTENT> (1 to 1023 bytes of character string)	--	Specifies the character string in the contents of the element that contains the <i>substitute</i> string. This item is specified when the element cannot be identified by <TARGET_ELEMENT_NAME> tag alone (such as when multiple elements have the value specified in <TARGET_ELEMENT_NAME> tag), but when specifying the element's contents can identify or narrow down the target element. Do not specify element contents that change dynamically. To specify multiple character strings that are in the contents of the element, specify multiple <TARGET_ELEMENT_CONTENT> tags.
<TARGET_ELEMENT_POSITION>... </TARGET_ELEMENT_POSITION> (1 to 1023) <<1>>	--	When multiple elements satisfy the conditions specified in all or some of the <TARGET_ELEMENT_NAME>, <TARGET_ELEMENT_ATTRIBUTE>, and <TARGET_ELEMENT_CONTENT> tags, this tag specifies the location from the beginning of the element that contains the <i>substitute</i> string.
<SUBSTITUTE_TYPE>... </SUBSTITUTE_TYPE>	..#2	Specifies the value that contains the <i>substitute</i> string. Specify the <TYPE_CONTENT> tag or the <TYPE_ATTRIBUTE> tag.
<TYPE_CONTENT> </TYPE_CONTENT>#3	..#4	Specifies that the <i>substitute</i> string is contained in the element's contents.
<TYPE_ATTRIBUTE>... </TYPE_ATTRIBUTE> (1 to 1023 bytes of character string)	..#4	When the <i>substitute</i> string is contained in the element's attribute value, this tag specifies the name of that attribute. The equal sign (=) must not be specified. The specified attribute name is not case sensitive.
<TARGET_HEADER>... </TARGET_HEADER>	..#1	Specify this tag to identify the element containing the substitute strings in the HTTP header that is responded at the step specified by <TARGET_STEP_ID> tag. This item contains the <TARGET_HEADER_NAME> and <TARGET_HEADER_VALUE> tags. If the header cannot be identified by the <TARGET_HEADER_NAME> tag alone, you specify the <TARGET_HEADER_VALUE> tag to identify the header containing the substitute strings. If the header cannot be identified by the <TARGET_HEADER_NAME> and

XML tag	Mandatory	Role of tag and value to be specified
<TARGET_HEADER>... </TARGET_HEADER>	..#1	<TARGET_HEADER_VALUE> tags, among the matched headers the first received header is treated as the specified header.
<TARGET_HEADER_NAME>... </TARGET_HEADER_NAME> ((1 or greater bytes of character string))	..#5	Specifies the name of the header that contains the substitute strings. The specified name is not case sensitive. Note that the validity of the specified value is not checked. The specified character string is treated as a header name. The header that matches completely the specified header name is searched in the received HTTP header. For example, to specify the Set-Cookie header (Set-Cookie: ...), you specify Set-Cookie in the <TARGET_HEADER_NAME> tag.
<TARGET_HEADER_VALUE>... </TARGET_HEADER_VALUE> ((1 or greater bytes of character string))	--	Specifies the character string that partially matches the value of the header containing the substitute strings. This item is specified when the header cannot be identified by <TARGET_HEADER_NAME> tag alone (such as when headers have the value specified in <TARGET_HEADER_NAME> tag) but when specifying the header's value can identify or narrow down the target header. Do not specify header values that change dynamically.
<SUBSTITUTE_RANGE>... </SUBSTITUTE_RANGE>	--	Specifies that only a part of the value specified in <SUBSTITUTE_TYPE> tag is to be treated as the <i>substitute</i> string. This item contains the <BEFORE_RANGE> and <AFTER_RANGE> tags. To omit the specification, omit the <SUBSTITUTE_RANGE> tag and all the tags contained in it. Omitting this item means specifying the entire value specified in <SUBSTITUTE_TYPE> tag.
<BEFORE_RANGE>... </BEFORE_RANGE> ((1 to 255 bytes of character string))	..#6	Specifies that the beginning of the value specified in <SUBSTITUTE_TYPE> tag is to be excluded from the <i>substitute</i> string. This item specifies the character string just before the <i>substitute</i> string (excluding the <i>substitute</i> string). If there are multiple identical character strings in the value specified in <SUBSTITUTE_TYPE> tag, the search is conducted from the beginning, and only the first matching character string is specified. If this item is omitted or if the specified character string is not found, the character string from the beginning of the value specified in <SUBSTITUTE_TYPE> tag is assumed to be the <i>substitute</i> string. If <TYPE_ATTRIBUTE> tag is specified in <SUBSTITUTE_TYPE> tag, neither double nor single quotation marks (", ') can be specified to indicate a range of attribute values.
<AFTER_RANGE>... </AFTER_RANGE> ((1 to 255 bytes of character string))	..#6	Specifies that the end of the value specified in <SUBSTITUTE_TYPE> tag is to be excluded from the <i>substitute</i> string. This item specifies the character string just after the <i>substitute</i> string (excluding the <i>substitute</i> string). If there are multiple identical character strings in the value specified in <SUBSTITUTE_TYPE> tag, the search is conducted from the end of the character string specified in <BEFORE_RANGE> tag and only the first matching character string is specified. If this item is omitted or the specified character string is not found, the character string through the end of the value specified in <SUBSTITUTE_TYPE> tag is assumed to be the <i>substitute</i> string. If <TYPE_ATTRIBUTE> tag is specified in <SUBSTITUTE_TYPE> tag, neither double nor single quotation marks (", ') can be specified to indicate a range of attribute values.

Legend:

Y: The item is mandatory when the <SUBSTITUTE_TARGET> tag is specified.

--: The item is optional when the <SUBSTITUTE_TARGET> tag is specified.

(()): Specifiable value range of the tag.

#1

Specify either the <TARGET_ELEMENT> tag or the <TARGET_HEADER> tag.

#2

The item is mandatory when the <TARGET_ELEMENT> tag is specified.

#3

You cannot specify any elements (including spaces or line breaks) within tags. If elements are specified within tags, the Web Recorder cannot open the Web transaction file.

#4

Specify either the <TYPE_CONTENT> tag or the <TYPE_ATTRIBUTE> tag.

#5

The item is mandatory when the <TARGET_HEADER> tag is specified.

#6

If the <SUBSTITUTE_RANGE> tag is specified, one or both must be specified.

(4) Examples

The following are examples of Web transaction files:

```
<?xml version="1.0" encoding="US-ASCII" standalone="no"?>
<!DOCTYPE TRANSACTION_LIST SYSTEM "espwebtrans.dtd">
<TRANSACTION_LIST>
<TRANSACTION>
  <TRANSACTION_PARAM>
    <TRANSACTION_NAME>transaction-in-email-system</TRANSACTION_NAME>
    <IGNORE_EMBEDDED_RESOURCE></IGNORE_EMBEDDED_RESOURCE>
    <NO_CACHE></NO_CACHE>
    <KEEP_ALIVE></KEEP_ALIVE>
  </TRANSACTION_PARAM>

  <STEP>
    <TITLE>login-window</TITLE>
    <REQUEST>
      <URL>http://www.xxx.co.jp/login.jsp</URL>
    </REQUEST>
    <START_SCOPE>SCOPE1</START_SCOPE>
  </STEP>

  <STEP>
    <FRAME_NAME>subframe</FRAME_NAME>
    <REQUEST>
      <URL>http://www.xxx.co.jp/subframe.html</URL>
    </REQUEST>
    <END_SCOPE>SCOPE1</END_SCOPE>
  </STEP>

  <STEP>
    <TITLE>login-success-window</TITLE>
    <REQUEST>
      <URL>http://www.xxx.co.jp/login_exec.jsp</URL>
      <POST>
        <CONTENT_TYPE>
          <FORM_URLENCODED></FORM_URLENCODED>
        </CONTENT_TYPE>
      </POST>
    </REQUEST>
  </STEP>
</TRANSACTION>
</TRANSACTION_LIST>
```

```
        <MESSAGE_BODY>login_name=hoge&password=hogehoge</MESSAGE_BODY>
    </POST>
</REQUEST>
    <RESPONSE_PATTERN>{successful-login}*(!{failure}*!{error})</
RESPONSE_PATTERN>
</STEP>

</TRANSACTION>
</TRANSACTION_LIST>
```

8.6 Command registration file (espcommand.xml)

The command registration file is used to register user-defined commands. It is read when the Probe Daemon starts.

To apply the definitions specified in the command registration file, you must restart PFM - Agent for Service Response.

8.6.1 Format

```
<?xml version="1.0" encoding="US-ASCII" standalone="no"?>
<!DOCTYPE COMMAND_LIST SYSTEM "espcommand.dtd">
<COMMAND_LIST>
  <ESP_NAME/>
  <COMMAND>
    <USER_COMMAND_ID>user-defined-service-ID</USER_COMMAND_ID>
    <USER_COMMAND>user-defined-command</USER_COMMAND>
    <EXECUTION_TIME></EXECUTION_TIME>
  </COMMAND>
  ...
</COMMAND_LIST>
```

8.6.2 Definition

(1) XML declaration and document type declaration

Specify the XML declaration on the first line and the document type declaration on the second line. Specify exactly as shown below:

```
<?xml version="1.0" encoding="encoding-type" standalone="no"?>
<!DOCTYPE COMMAND_LIST SYSTEM "espcommand.dtd">
```

Specify one of the following encoding types. You must declare the command registration file with the specified encoding type.

- Shift_JIS
- UTF-8
- US-ASCII
- GB18030#

GB18030 supports only in Chinese OS and you cannot use the 4 bytes characters.

(2) XML definition

Table 8–29: XML definition

XML tag	Mandatory	Role of tag and value to be specified
<COMMAND_LIST>... </COMMAND_LIST>	Y	Indicates a list of user-defined commands. This tag contains one or more <COMMAND> tags. A new <COMMAND> tag can start immediately after a </COMMAND> tag.
<ESP_NAME/>	Y	You must specify this tag.
<COMMAND>... </COMMAND>	Y	Specifies the user-defined command. This tag contains the <USER_COMMAND_ID>, <USER_COMMAND>, and <EXECUTION_TIME> tags.
<USER_COMMAND_ID>... </USER_COMMAND_ID> ((1 to 100))	Y	Specifies the user definition ID used to identify a user-defined command.
<USER_COMMAND>... </USER_COMMAND> ((character string of up to 512 bytes))	Y	Specifies a user-defined command. Even if the command requires options, the entire command, including the options, must be specified on one line.
<EXECUTION_TIME>... </EXECUTION_TIME>	--	Specifies that the time required to execute the user-defined command (from start to termination) is to be used as the response performance information. If this item is omitted, the value output to the standard output by the user-defined command is used as the response performance information.

Legend:

Y: Mandatory item

--: Optional item

(()): Specifiable value range of the tag.

8.6.3 Example

The following is an example of a command registration file:

```
<?xml version="1.0" encoding="US-ASCII" standalone="no"?>
<!DOCTYPE COMMAND_LIST SYSTEM "espcommand.dtd">
<COMMAND_LIST>
  <ESP_NAME/>
  <COMMAND>
    <USER_COMMAND_ID>1</USER_COMMAND_ID>
    <USER_COMMAND>command1.exe</USER_COMMAND>
  </COMMAND>
  <COMMAND>
    <USER_COMMAND_ID>2</USER_COMMAND_ID>
    <USER_COMMAND>command2.exe</USER_COMMAND>
    <EXECUTION_TIME></EXECUTION_TIME>
  </COMMAND>
</COMMAND_LIST>
```

8.7 Measurement condition label definition file (esptasklabel.conf)

The measurement condition label definition file is used to define labels of your choosing for measurement conditions.

Note:

If you define the label name of the same task ID in the measurement condition registration file (`esptask.xml`), then the label name defined in the measurement condition registration file takes precedence over those of the specified label name in the measurement condition label definition file.

You can check and edit the label names of the tasks defined in the measurement condition registration file as the **Task Label** property in PFM - Web Console. Yet, you cannot check and edit the label names of the tasks defined in the measurement condition label definition file by using PFM - Web Console.

8.7.1 Format

```
[label definition]
task_id=measurement-condition-ID
task_label=measurement-condition-label-name
```

Note:

The following notes apply to specifying the measurement condition label definition file:

- Each key name and its value must be connected by an equal sign (=).
- Each key name and its value must be specified on a single line.
- The specification must begin in column 1.

A line beginning with a hash mark (#) is treated as a comment line.

8.7.2 Definition

label definition section:

Specifies a combination of an ID and a label name for the measurement condition.

You specify this section for each measurement condition for which a measurement condition label is to be defined. If either the ID or the label name is not correct, the combination of the ID and the label name is not applied.

Table 8–30: Definition in the label definition section

Key name	Mandatory	Value to be specified
task_id	Y	Specifies the ID of the measurement condition for which a label is to be defined.
task_label ((character string of up to 63 bytes#))	Y	Specifies a name for the measurement condition. This name must be unique among all the measurement condition names.

Legend:

Y: Mandatory item

(()): Specifiable value range of the tag.

#

The comma (,), double quotation mark ("), and equal sign (=) cannot be specified.

8.7.3 Example

The following is an example of a measurement condition label definition file:

```
[label definition]
task_id=1
task_label=HTTP A Server
task_id=2
task_label=HTTPS shopping Server
task_id=3
task_label=POP3 Mail Server
```

8.8 IE Recorder action condition definition file (jpcvierec.conf)

The IE Recorder action condition definition file is used to define the IE Recorder's action conditions. This file is read when the IE Recorder starts.

8.8.1 Format

```
[IE Recorder]
replay_wait=replay-wait-time
operation_name=operation-name, recording-target-tag, attribute-
name=attribute-value
address_bar= initial-URL-of-Addressbar
ie_rec_browser_mode=Internet-Explorer-version-for-using-IE-Recorder
```

Note:

The following notes apply to specifying the IE Recorder action condition definition file:

- Each key name and its value must be connected by an equal sign (=).
- Each key name and its value must be specified on a single line.
- The specification must begin in column 1.

A line beginning with a hash mark (#) is treated as a comment line.

8.8.2 Definition

IE Recorder section:

Defines an item related to the IE Recorder.

Table 8–31: Definition in the IE Recorder section

Key name	Mandatory	Value to be specified
replay_wait ((0 to 99))(seconds)<<1>>	--	Specifies the wait time to replay for each operation in seconds. If this item is omitted, the wait time to replay is 1 (second). Specifies this item to replay slowly.
operation_name ((operation name ^{#1} , recording target tag [, attribute, ...]))	--	Specifies the operation name, the standard recording tag name, and the attribute ^{#2} that are displayed in the Operation List. Note that validity checking is not performed on the specified tag, attribute name and value.
address_bar ((URL)) ^{#3}	--	Specifies the URL to be displayed in the drop-down list of Addressbar. If you specify the URL beginning with other than the protocol identifier (<code>http://</code> or <code>https://</code>), the specified URL with the protocol identifier (<code>http://</code>) is displayed in the drop-down list. If you specify the URLs to use frequently in this item, you can use the IE Recorder addressbar like a bookmark.
ie_rec_browser_mode ((IE7, IE8, IE9, IE10 or IE11)) ^{#4}	--	Specifies the Internet Explorer version for using the IE Recorder. Before specifying this item, check the Internet Explorer version supported by the monitoring target and the version of Internet Explorer installed in an environment in which PFM - Agent for Service Response is installed.

Key name	Mandatory	Value to be specified
ie_rec_browser_mode (IE7, IE8, IE9, IE10 or IE11)#4	--	<p>Internet Explorer 7 is the default version.</p> <ul style="list-style-type: none"> • IE7 Specify this when the monitoring target supports Internet Explorer 7. • IE8 Specify this when the monitoring target supports Internet Explorer 8. • IE9 Specify this when the monitoring target supports Internet Explorer 9. You can specify this option when Internet Explorer 9 or a later version is installed in an environment in which PFM - Agent for Service Response is installed. • IE10 Specify this when the monitoring target supports Internet Explorer 10. You can specify this option when Internet Explorer 10 or a later version is installed in an environment in which PFM - Agent for Service Response is installed. • IE11 Specify this when the monitoring target supports Internet Explorer 11. You can specify this option when Internet Explorer 11 or a later version is installed in an environment in which PFM - Agent for Service Response is installed. <p>You must specify the Internet Explorer version that was specified when IE scenarios were created. This value must also be specified for <code>ie_probe_browser_mode</code> in the IE Probe section in the Probe action condition definition file.</p> <p>If a value is not specified or if an invalid value is specified, the default version(Internet Explorer 7) is used.</p>

Legend:

--: Optional item

(()): Specified value range of the tag.

<< >>: Default value

#1

You can specify only Japanese and English characters to the `operation_name`.

#2

Specifies the attribute in `attribute-name=attribute-value` format. You can omit the attribute and specify multiple attributes.

-- When you omit an attribute:

The specified operation name is displayed for the operation related to the specified recording target tag name in the Operation List.

-- When you specify multiple attributes:

The matched operation names are displayed for the operations in relation to the tags containing all the specified recording target tag names and attributes in the Operation List. If there are multiple recording target tag names and attributes that match the specified condition, only the first matched operation is enabled and the others are ignored.

#3

To use an IP address to specify a host name, use an IPv4 dotted-decimal address (for example: `http://172.16.233.12/example.html`) or an IPv6 hexadecimal address enclosed in square brackets, using colons as separators (for example: `http://[ACE6:45:75:91::1]/example.html`).

#4

Do not specify version of Internet Explorer that PFM - Agent for Service Response does not support.

8.8.3 Example

The following is an example of the IE Recorder action condition definition file:

```
[IE Recorder]
replay_wait=0
operation_name=Click link,a
operation_name=Click button,button
operation_name=Select check box,input,type=radio
operation_name=Select check box,input,type=checkbox
operation_name=Enter text,input,type=text
operation_name=Enter text,input,type=password
operation_name=Enter text,input,type=file
operation_name=Click button,input,type=submit
operation_name=Click button,input,type=reset
operation_name=Click button,input,type=button
operation_name=Click button,input,type=image
operation_name=Select value,select
operation_name=Enter text,textarea
address_bar=
ie_rec_browser_mode=
```

8.9 IE scenario files

An IE scenario file is a definition file to record a series of operation information by using the Internet Explorer. You can define one IE scenario in one IE scenario file. You use the IE Recorder to create an IE scenario file and save it as any name you specify (with the extension `.xml`) under

installation-folder\agt\probe\iescena.

You must not use a program such as a text editor to edit an IE scenario file directly. Use the IE Recorder to create an IE scenario file. For details about how to use the IE Recorder to create an IE scenario file, see [4.5.2 Defining IE scenarios \(creating IE scenario files\)](#). For details about how to apply the definitions specified in an IE scenario file, see [4.7.4 Applying the Task information](#).

9

Monitoring template

This chapter describes the monitoring template for PFM - Agent for Service Response.

Overview of the monitoring template

The Performance Management products enable you to use the following three methods to create alarms and reports:

- By using the alarms and reports defined by PFM - Agent
- By copying and customizing the alarms and reports defined by PFM - Agent
- By using a wizard to define new information

The set of alarms and reports provided by PFM - Agent is called the *monitoring template*. Because all needed information is predefined for the reports and alarms in the monitoring template, you can simply copy them to use the monitoring template as is. Alternatively, you can customize the predefined reports and alarms as appropriate for your environment. These methods eliminate the need to use the wizard to create new definitions, and they simplify the preparations for monitoring the operating status of desired programs.

This chapter describes the alarm and report settings in the monitoring template that has been defined by PFM - Agent for Service Response.

For details about how to use the monitoring template, see the chapter that describes report creation for operation analysis, or the chapter that describes operation monitoring by alarms, in the *JPI/Performance Management User's Guide*.

Note:

The thresholds set for the alarms in the monitoring template are reference examples. To use the alarms in the monitoring template, copy the setting and specify the thresholds appropriate for the environment and OS.

Format of alarm explanations

This section describes the format used to explain alarms. Alarms are presented in alphabetical order.

Alarm name

Shows the name of an alarm in the monitoring template.

Overview

Provides an overview of program monitoring by the alarm.

Main settings

Explains in table format the principal settings for this alarm. The table lists the correspondence between alarm settings and the Properties window, which is displayed in PFM - Web Console when **Properties** is chosen for an entry in the **Alarms** tree. For details about the settings for each alarm, check the Properties window for the alarm when you select it in the **Alarms** tree in PFM - Web Console.

Two hyphens (--) in the settings indicates a setting that is always ignored.

If the abnormal condition is the same as the warning condition in a conditional expression, the system issues only the abnormal alarm event.

Related reports

Indicates the reports in the monitoring template that are associated with this alarm.

List of alarms

The alarm table named `PFM SR Solution Alarms 09.00` contains the alarms that are defined in the monitoring template for `PFM - Agent for Service Response (09.00)` (09.00 indicates the version of the alarm table).

`PFM - Agent for Service Response` provides 2 types of the alarm as the monitoring template. Use the alarm or alarms that match your objectives so that the necessary alarms are given.

The following table shows the Alarm types and the purpose of use:

Table 9–1: Alarm types and Monitoring purpose

Alarm type	Purpose of use
<code><service-name> Response Time</code> <code><service-name> Replay Time</code>	Alarms for detecting that the measurement value is abnormal. Use these alarms to detect that the measurement results are beyond the specified threshold values. If errors (such as a timeout error) occur while measuring, use also <code><service-name> Failure</code> , because <code><service-name> Response Time</code> and <code><service-name> Replay Time</code> cannot detect the errors while measuring.
<code><service-name> Failure</code>	Alarms for detecting errors while measuring. This alarm does not check the measurement values, but checks whether errors (such as a timeout error) occur while measuring.

This alarm table is stored in the `Service Response` folder, which is displayed on the **Alarms** tree in `PFM - Web Console`. The following table lists the alarms defined in the monitoring template.

Table 9–2: List of alarms

Alarm name	Monitoring target
<i>FTP Failure</i>	Whether or not measurement of the FTP service has failed
<i>FTP Response Time</i>	FTP service's total response time
<i>IES Failure</i>	Whether or not measurement of the IE scenario has failed
<i>IES Replay Time</i>	IE scenario's total response time
<i>IMAP4 Failure</i>	Whether or not measurement of the IMAP4 service has failed
<i>IMAP4 Response Time</i>	IMAP4 service's total response time
<i>POP3 Failure</i>	Whether or not measurement of the POP3 service has failed
<i>POP3 Response Time</i>	POP3 service's total response time
<i>SMTP Failure</i>	Whether or not measurement of the SMTP service has failed
<i>SMTP Response Time</i>	SMTP service's total response time
<i>TCP Failure</i>	Whether or not measurement of the TCP service has failed
<i>TCP Response Time</i>	TCP service's total response time
<i>WT Failure</i>	Whether or not measurement of the Web transaction service has failed
<i>WT Response Time</i>	Web transaction's total response time

FTP Failure

Overview

The FTP Failure alarm monitors whether or not measurement of the FTP service has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure FTP service. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	FTP (PI_FTP)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Pastmary

FTP Response Time

Overview

The FTP Response Time alarm monitors the FTP service's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	FTP Response time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	FTP (PI_FTP)
	Field	Total Response Time
	Abnormal condition	Total Response Time > 30
	Warning condition	Total Response Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/FTP Response Time Summary

IES Failure

Overview

The IES Failure alarm monitors whether or not measurement of the IE scenario has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure IE Scenario. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	IE Scenario (PI_IES)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/IE Scenario Replay Time Summary

IES Replay Time

Overview

The IES Response Time alarm monitors the IE scenario's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	IES Replay time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	IE Scenario (PI_IES)
	Field	Total Replay Time
	Abnormal condition	Total Replay Time > 30
	Warning condition	Total Replay Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/IE Scenario Replay Time Summary

IMAP4 Failure

Overview

The IMAP4 Failure alarm monitors whether or not measurement of the IMAP4 service has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure IMAP4 service. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	IMAP4 (PI_IMP4)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/IMAP4 Response Time Summary

IMAP4 Response Time

Overview

The IMAP4 Response Time alarm monitors the IMAP4 service's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	IMAP4 Response time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	occurrence(s) during
	Interval(s)	Interval(s)
Alarm Conditions	Record	IMAP4 (PI_IMP4)
	Field	Total Response Time
	Abnormal condition	Total Response Time > 30
	Warning condition	Total Response Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/IMAP4 Response Time Summary

POP3 Failure

Overview

The POP3 Failure alarm monitors whether or not measurement of the POP3 service has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure POP3 service. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	POP3 (PI_POP3)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/POP3 Response Time Summary

POP3 Response Time

Overview

The POP3 Response Time alarm monitors the POP3 service's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	POP3 Response time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	POP3 (PI_POP3)
	Field	Total Response Time
	Abnormal condition	Total Response Time > 30
	Warning condition	Total Response Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/POP3 Response Time Summary

SMTP Failure

Overview

The SMTP Failure alarm monitors whether or not measurement of the SMTP service has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure SMTP service. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	SMTP (PI_SMTP)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/SMTP Response Time Summary

SMTP Response Time

Overview

The SMTP Response Time alarm monitors the SMTP service's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	SMTP Response time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	SMTP (PI_SMTP)
	Field	Total Response Time
	Abnormal condition	Total Response Time > 30
	Warning condition	Total Response Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/SMTP Response Time Summary

TCP Failure

Overview

The TCP Failure alarm monitors whether or not measurement of the TCP service has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure TCP service. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	TCP (PI_TCP)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/TCP Response Time Summary

TCP Response Time

Overview

The TCP Response Time alarm monitors the TCP service's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	TCP Response time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	TCP (PI_TCP)
	Field	Total Response Time
	Abnormal condition	Total Response Time > 30
	Warning condition	Total Response Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/TCP Response Time Summary

WT Failure

Overview

The WT Failure alarm monitors whether or not measurement of the Web transaction service has failed.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	Failed to measure Web Transaction service. (%CVS)
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	Web Transaction (PI_WT)
	Field	Result Strings
	Abnormal condition	< > SUCCESS
	Warning condition	< > SUCCESS
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/Web Transaction Response Time Summary

WT Response Time

Overview

The WT Response Time alarm monitors the Web transaction's total response time.

Main settings

Alarm properties in PFM - Web Console		Setting
Item	Details	
Main Information	Product	Service Response
	Alarm message	WEBTRANS Response time is %CVS sec.
	Check whether the value exists	Not selected
	Enable alarm	Selected
	Alarm notification	Notify when the state changed
	Notification target	State changes for the alarm
	Evaluate all data	Not selected
	Monitoring time range	Always monitor
	Report alarm when the following damping condition is reached	Not selected
	occurrence(s) during	--
	Interval(s)	--
Alarm Conditions	Record	Web Transaction (PI_WT)
	Field	Total Response Time
	Abnormal condition	Total Response Time > 30
	Warning condition	Total Response Time > 15
Actions	E-mail	--
	Command	--
	SNMP	Abnormal, Warning, Normal

Related reports

Reports/Service Response/Troubleshooting/Recent Past/Web Transaction Response Time Summary

Format of report explanations

This section describes the format used to explain reports. Reports are presented in alphabetical order.

Report name

Shows the name of a report in the monitoring template.

Overview

Provides an overview of the information that can be displayed in the report.

Display format

Shows the display format of a report.

Storage location

Indicates the storage location of the report.

Record

Indicates the record that contains the performance data used in the report. To display a historical report, you must specify information in advance in order to collect the indicated record. Before displaying a report, check the Properties window for the entry when you select it in the **Services** tree in PFM - Web Console to see if **Log** is set to **Yes**. This setting is not needed to display a real-time report.

Fields

Provides a table that describes the fields used in the report.

Drilldown reports (report level)

Provides a table listing other reports in the monitoring template that are related to this report. To display a drilldown report, in the PFM - Web Console report window, select the name of the desired drilldown report from the Drilldown Report pull-down menu, then click **Display Reports**. Note that some reports do not have any drilldown reports.

Drilldown reports (field level)

Provides a table describing reports in the monitoring template that are associated with fields used in this report. To display these drilldown reports, in the PFM - Web Console report window, choose **Graph**, **List**, or **Table**. In the case of a historical report, you can display a drilldown report in smaller intervals by displaying it from the time item. Note that some reports do not have any drilldown reports.

For details about drilldown reports, see the chapter that describes report creation for operation analysis in the *JPI/Performance Management User's Guide*.

Organization of report folders

The following shows the organization of the report folders for PFM - Agent for Service Response. Angle brackets enclose folder names:

```
<Service Response>
  +-- <Monthly Trend>
  |   +-- DHCP Response Time Trend
  |   +-- DNS Response Time Trend
  |   +-- FTP Response Time Trend
  |   +-- HTTP Response Time Trend
  |   +-- HTTPS Response Time Trend
  |   +-- IE Scenario Replay Time Trend
  |   +-- IMAP4 Response Time Trend
  |   +-- POP3 Response Time Trend
  |   +-- SMTP Response Time Trend
  |   +-- TCP Response Time Trend
  |   +-- User Defined Service Response Time Trend
  |   +-- Web Transaction Response Time Trend
  +-- <Status Reporting>
  |   +-- <Daily Trend>
  |   |   +-- DHCP Response Time Status
  |   |   +-- DNS Response Time Status
  |   |   +-- FTP Response Time Status
  |   |   +-- HTTP Response Time Status
  |   |   +-- HTTPS Response Time Status
  |   |   +-- IE Scenario Replay Time Status
  |   |   +-- IMAP4 Response Time Status
  |   |   +-- POP3 Response Time Status
  |   |   +-- SMTP Response Time Status
  |   |   +-- TCP Response Time Status
  |   |   +-- User Defined Service Response Time Status
  |   |   +-- Web Transaction Response Time Status
  |   +-- <Real-Time>
  |   |   +-- DHCP Response Time Status
  |   |   +-- DNS Response Time Status
  |   |   +-- FTP Response Time Status
  |   |   +-- HTTP Response Time Status
  |   |   +-- HTTPS Response Time Status
  |   |   +-- IE Scenario Replay Time Status
  |   |   +-- IMAP4 Response Time Status
  |   |   +-- POP3 Response Time Status
  |   |   +-- SMTP Response Time Status
  |   |   +-- TCP Response Time Status
  |   |   +-- User Defined Service Response Time Status
  |   |   +-- Web Transaction Response Time Status
  +-- <Troubleshooting>
  |   +-- <Real-Time>
  |   |   +-- FTP Top 10
  |   |   +-- HTTP Top 10
  |   |   +-- HTTPS Top 10
  |   |   +-- IE Scenario Scope Detail
  |   |   +-- IE Scenario Scope Rate
  |   |   +-- IE Scenario Top 10
  |   |   +-- IMAP4 Top 10
  |   |   +-- POP3 Top 10
  |   |   +-- SMTP Top 10
```

```

|      +--- Web Transaction Scope Detail
|      +--- Web Transaction Scope Rate
|      +--- Web Transaction Top 10
|      +--- <Drilldown Only>
|          +--- FTP Rate
|          +--- HTTP Rate
|          +--- HTTPS Rate
|          +--- IE Scenario Detail
|          +--- IMAP4 Rate
|          +--- POP3 Rate
|          +--- Scope Detail
|          +--- SMTP Rate
|          +--- Transaction Detail
+--- <Recent Past>
    +--- DHCP Response Time Summary
    +--- DNS Response Time Summary
    +--- FTP Response Time Summary
    +--- HTTP Response Time Summary
    +--- HTTPS Response Time Summary
    +--- IE Scenario Logged Message
    +--- IE Scenario Replay Time Summary
    +--- IMAP4 Response Time Summary
    +--- POP3 Response Time Summary
    +--- SMTP Response Time Summary
    +--- TCP Response Time Summary
    +--- User Defined Service Response Time Summary
    +--- Web Transaction Response Time Summary

```

The folders are described below:

- Monthly Trend folder

This folder contains historical reports that display daily information for the past month. Use these reports to check monthly trends in the system.
- Status Reporting folder

This folder contains reports that display daily or weekly information. Use these reports to check the overall status of the system.

 - Daily Trend folder

This folder contains reports that display hourly information for the past 24 hours. Use these reports to check the daily status of the system.
 - Real-Time folder

This folder contains real-time reports for checking the system status.
- Troubleshooting folder

This folder contains reports that display information useful for resolving problems. In the event of a system problem, use these reports to check the cause of the problem.

 - Real-Time folder

This folder contains real-time reports for checking the current system status.

These folders may also include the following folder:
 - Drilldown Only folder

This folder contains reports that are displayed as drilldown reports (field level). Use it to display detailed information about fields contained in the applicable report.

- Recent Past folder

This folder contains historical reports that display minute-by-minute information for the past hour.

List of reports

The following table lists (in alphabetical order) the reports defined in the monitoring template.

Table 9–3: List of reports

Report name	Displayed information	Storage location
<i>DHCP Response Time Status</i>	DHCP-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>DHCP Response Time Status (real-time report)</i>	DHCP-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>DHCP Response Time Summary</i>	DHCP-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>DHCP Response Time Trend</i>	DHCP-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>DNS Response Time Status</i>	DNS-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>DNS Response Time Status (real-time report)</i>	DNS-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>DNS Response Time Summary</i>	DNS-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>DNS Response Time Trend</i>	DNS-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>FTP Rate</i>	Percentage ratio of the detailed response time for each operation in FTP service	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>FTP Response Time Status</i>	FTP-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>FTP Response Time Status (real-time report)</i>	FTP-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>FTP Response Time Summary</i>	FTP-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>FTP Response Time Trend</i>	FTP-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>FTP Top 10</i>	Top 10 FTP services in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time
<i>HTTP Rate</i>	Percentage ratio of the detailed response time for each operation in HTTP service	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>HTTP Response Time Status</i>	HTTP-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>HTTP Response Time Status (real-time report)</i>	HTTP-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>HTTP Response Time Summary</i>	HTTP-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>HTTP Response Time Trend</i>	HTTP-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>HTTP Top 10</i>	Top 10 HTTP services in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time

Report name	Displayed information	Storage location
<i>HTTPS Rate</i>	Percentage ratio of the detailed response time for each operation in HTTPS service	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>HTTPS Response Time Status</i>	HTTPS-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>HTTPS Response Time Status (real-time report)</i>	HTTPS-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>HTTPS Response Time Summary</i>	HTTPS-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>HTTPS Response Time Trend</i>	HTTPS-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>HTTPS Top 10</i>	Top 10 HTTPS services in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time
<i>IE Scenario Detail</i>	Total replay time for each scope in an IE scenario	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>IE Scenario Logged Message</i>	IE scenario-related historical information in the Event Log and messages in the logfiles are written over the past hour	Reports/Service Response/Troubleshooting/Recent Past
<i>IE Scenario Replay Time Status</i>	IE scenario-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>IE Scenario Replay Time Status (real-time report)</i>	IE scenario-related replay time	Reports/Service Response/Status Reporting/Real-Time
<i>IE Scenario Replay Time Summary</i>	IE scenario-related replay time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>IE Scenario Replay Time Trend</i>	IE scenario-related replay time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>IE Scenario Scope Detail</i>	Replay time for each scope in each IE scenario	Reports/Service Response/Troubleshooting/Real-Time
<i>IE Scenario Scope Rate</i>	Percentage ratio of each scope in an IE scenario	Reports/Service Response/Troubleshooting/Real-Time
<i>IE Scenario Top 10</i>	Top 10 IE scenarios in terms of total replay time	Reports/Service Response/Troubleshooting/Real-Time
<i>IMAP4 Rate</i>	Percentage ratio of each detail in IMAP4 service	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>IMAP4 Response Time Status</i>	IMAP4-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>IMAP4 Response Time Status (real-time report)</i>	IMAP4-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>IMAP4 Response Time Summary</i>	IMAP4-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>IMAP4 Response Time Trend</i>	IMAP4-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>IMAP4 Top 10</i>	Top 10 IMAP4 services in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time

Report name	Displayed information	Storage location
<i>POP3 Rate</i>	Percentage ratio of the detailed response time for each operation in POP3 service	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>POP3 Response Time Status</i>	POP3-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>POP3 Response Time Status (real-time report)</i>	POP3-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>POP3 Response Time Summary</i>	POP3-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>POP3 Response Time Trend</i>	POP3-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>POP3 Top 10</i>	Top 10 POP3 services in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time
<i>Scope Detail</i>	Details of each scope of the Web transaction	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>SMTP Rate</i>	Percentage ratio of the detailed response time for each operation in SMTP service	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>SMTP Response Time Status</i>	SMTP-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>SMTP Response Time Status (real-time report)</i>	SMTP-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>SMTP Response Time Summary</i>	SMTP-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>SMTP Response Time Trend</i>	SMTP-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>SMTP Top 10</i>	Top 10 SMTP services in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time
<i>TCP Response Time Status</i>	TCP-related response time over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>TCP Response Time Status (real-time report)</i>	TCP-related response time	Reports/Service Response/Status Reporting/Real-Time
<i>TCP Response Time Summary</i>	TCP-related response time over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>TCP Response Time Trend</i>	TCP-related response time over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>Transaction Detail</i>	Total response time of each scope of the Web transaction	Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only
<i>User Defined Service Response Time Status</i>	Response time for a user-defined service over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>User Defined Service Response Time Status (real-time report)</i>	Response time for a user-defined service	Reports/Service Response/Status Reporting/Real-Time
<i>User Defined Service Response Time Summary</i>	Response time for a user-defined service over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>User Defined Service Response Time Trend</i>	Response time for a user-defined service over the past month (on a daily basis)	Reports/Service Response/Monthly Trend

Report name	Displayed information	Storage location
<i>Web Transaction Response Time Status</i>	Response time for a Web transaction over the past 24 hours (on an hourly basis)	Reports/Service Response/Status Reporting/Daily Trend
<i>Web Transaction Response Time Status (real-time report)</i>	Response time for a Web transaction	Reports/Service Response/Status Reporting/Real-Time
<i>Web Transaction Response Time Summary</i>	Response time for a Web transaction over the past hour (on a minute-by-minute basis)	Reports/Service Response/Troubleshooting/Recent Past
<i>Web Transaction Response Time Trend</i>	Response time for a Web transaction over the past month (on a daily basis)	Reports/Service Response/Monthly Trend
<i>Web Transaction Scope Detail</i>	Response time for a scope in a Web transaction	Reports/Service Response/Troubleshooting/Real-Time
<i>Web Transaction Scope Rate</i>	Percentage ratio of each scope in a Web transaction	Reports/Service Response/Troubleshooting/Real-Time
<i>Web Transaction Top 10</i>	Top 10 Web transactions in terms of total response time	Reports/Service Response/Troubleshooting/Real-Time

DHCP Response Time Status

Overview

The DHCP Response Time Status report displays the DHCP-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

DHCP (PI_DHCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for searching for the target DHCP server and then dynamically acquiring its IP address

DHCP Response Time Status (real-time report)

Overview

The DHCP Response Time Status report displays the DHCP-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

DHCP (PI_DHCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for searching for the target DHCP server and then dynamically acquiring its IP address
Result Strings	Measurement result

DHCP Response Time Summary

Overview

The DHCP Response Time Summary report displays the DHCP-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

DHCP (PI_DHCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for dynamically acquiring the IP address from the measurement target
Result Strings	Measurement result

DHCP Response Time Trend

Overview

The DHCP Response Time Trend report displays the DHCP-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

DHCP (PI_DHCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for dynamically acquiring the IP address from the measurement target

DNS Response Time Status

Overview

The DNS Response Time Status report displays the DNS-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

DNS (PI_DNS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for querying the DNS server for the IP address corresponding to the specified search-target host name, and then receiving the response

DNS Response Time Status (real-time report)

Overview

The DNS Response Time Status report displays the DNS-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

DNS (PI_DNS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for querying the DNS server for the IP address corresponding to the specified search-target host name, and then receiving the response
Result Strings	Measurement result

DNS Response Time Summary

Overview

The DNS Response Time Summary report displays the DNS-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

DNS (PI_DNS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for querying the DNS server for the IP address corresponding to the specified search-target host name, and then receiving the response
Result Strings	Measurement result

DNS Response Time Trend

Overview

The DNS Response Time Trend report displays the DNS-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

DNS (PI_DNS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for querying the DNS server for the IP address corresponding to the specified search-target host name, and then receiving the response

FTP Rate

Overview

The FTP Rate report displays the percentage ratio of the detailed response time for each operation in FTP service on a real-time basis. This is a drilldown report.

Display format

A list and pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

FTP (PI_FTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
DNS Time	DNS time
TCP Connection Time	TCP connection time
Preprocessing Time	Preprocessing time
Data Transfer Time	Data transfer time

FTP Response Time Status

Overview

The FTP Response Time Status report displays the FTP-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

FTP (PI_FTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for acquiring a measurement file on the FTP server, or for transferring a provided measurement file to the target FTP server

FTP Response Time Status (real-time report)

Overview

The FTP Response Time Status report displays the FTP-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

FTP (PI_FTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for acquiring a measurement file on the FTP server, or for transferring a provided measurement file to the target FTP server
Result Strings	Measurement result

FTP Response Time Summary

Overview

The FTP Response Time Summary report displays the FTP-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

FTP (PI_FTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for acquiring a measurement file on the FTP server, or for transferring a provided measurement file to the target FTP server
Result Strings	Measurement result

FTP Response Time Trend

Overview

The FTP Response Time Trend report displays the FTP-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

FTP (PI_FTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for acquiring a measurement file on the FTP server, or for transferring a provided measurement file to the target FTP server

FTP Top 10

Overview

The FTP Top 10 report displays the top 10 FTP services in terms of the total response time.

Display format

A bar graph

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

FTP (PI_FTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for acquiring a measurement file on the FTP server, or for transferring a provided measurement file to the target FTP server

Drilldown reports (field level)

Report name	Description
FTP Rate	Displays the percentage ratio of the detailed response time for each operation in FTP service

HTTP Rate

Overview

The HTTP Rate report displays the percentage ratio of the detailed response time for each operation in HTTP service on a real time basis. This is a drilldown report.

Display format

A list and pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

HTTP (PI_HTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
DNS Time	DNS time
TCP Connection Time	TCP connection time
Server Processing Time	Server processing time
Data Transfer Time	Data transfer time

HTTP Response Time Status

Overview

The HTTP Response Time Status report displays the HTTP-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

HTTP (PI_HTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to issue an HTTP request to the specified URL and then to acquire a page by the GET method or register data by the POST method

HTTP Response Time Status (real-time report)

Overview

The HTTP Response Time Status report displays the HTTP-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

HTTP (PI_HTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to issue an HTTP request to the specified URL and then to acquire a page by the GET method or register data by the POST method
Result Strings	Measurement result

HTTP Response Time Summary

Overview

The HTTP Response Time Summary report displays the HTTP-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

HTTP (PI_HTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to issue an HTTP request to the specified URL and then to acquire a page by the GET method or register data by the POST method
Result Strings	Measurement result

HTTP Response Time Trend

Overview

The HTTP Response Time Trend report displays the HTTP-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

HTTP (PI_HTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for issuing an HTTP request to the specified URL and then acquiring a page by the GET method or registering data by the POST method

HTTP Top 10

Overview

The HTTP Top 10 report displays the top 10 HTTP services in terms of total response time.

Display format

A bar graph

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

HTTP (PI_HTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to issue an HTTP request to the specified URL and then to acquire a page by the GET method or register data by the POST method

Drilldown reports (field level)

Report name	Description
HTTP Rate	Displays the percentage ratio of the detailed response time for each operation in HTTP service

HTTPS Rate

Overview

The HTTPS Rate report displays the percentage ratio of the detailed response time for each operation in HTTPS service on a real time basis. This is a drilldown report.

Display format

A list and pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

HTTPS (PI_HTTPS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
DNS Time	DNS time
TCP Connection Time	TCP connection time
Server Processing Time	Server processing time
Data Transfer Time	Data transfer time

HTTPS Response Time Status

Overview

The HTTPS Response Time Status report displays the HTTPS-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

HTTPS (PI_HTTPS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to establish an SSL-protected connection with the target server being measured, to issue an HTTPS request to the URL specified on the connection, and then to acquire a page by the GET method or register data by the POST method

HTTPS Response Time Status (real-time report)

Overview

The HTTPS Response Time Status report displays the HTTPS-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

HTTPS (PI_HTTPS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to establish SSL-protected connection with the target server being measured, to issue an HTTPS request to the URL specified on the connection, and then to acquire a page by the GET method or register data by the POST method
Result Strings	Measurement result

HTTPS Response Time Summary

Overview

The HTTPS Response Time Summary report displays the HTTPS-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

HTTPS (PI_HTTPS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to establish SSL-protected connection with the target server being measured, to issue an HTTPS request to the URL specified on the connection, and then to acquire a page by the GET method or register data by the POST method
Result Strings	Measurement result

HTTPS Response Time Trend

Overview

The HTTPS Response Time Trend report displays the HTTPS-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

HTTPS (PI_HTTPS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to establish SSL-protected connection with the target server being measured, to issue an HTTPS request to the URL specified on the connection, and then to acquire a page by the GET method or register data by the POST method

HTTPS Top 10

Overview

The HTTPS Top 10 report displays the top 10 HTTPS services in terms of total response time.

Display format

A bar graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time

Record

HTTPS (PI_HTTPS)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required to establish SSL-protected connection with the target server being measured, to issue an HTTPS request to the URL specified on the connection, and then to acquire a page by the GET method or register data by the POST method

Drilldown reports (field level)

Report name	Description
HTTPS Rate	Displays the percentage ratio of the detailed response time for each operation in HTTPS service

IE Scenario Detail

Overview

The IE Scenario Detail report displays the total response time for each scope in an IE scenario on a real-time basis.

Display format

A column graph

Data label 1

Measurement Condition Name

Data label 2

Scope Name

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Conditional expression

Total Replay Time <> "0"

AND Scope ID <> "0"

Record

IE Scenario (PI_IES)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Replay Time	Replay time required for a series of operations in an IE scenario (time per scope)

IE Scenario Logged Message

Overview

The IE Scenario Logged Message report displays the IE scenario-related historical information of Event Log and messages in the logfiles are written over the past hour.

Display format

A table and a list

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

Logged Message for IE Scenario (PL_IESM)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Sequence Number	Sequence number of the operations that are replayed when outputting the messages
IE Scenario Result Code	Result code of replaying the operation
IE Scenario Result Message	Result message text of replaying the operation
IE Scenario Result Detail	Result detail text of replaying the operation

IE Scenario Replay Time Status

Overview

The IE Scenario Replay Time Status report displays the IE scenario-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Y-axis of the graph

Total Replay Time

Data label 1

Measurement Condition Name

Data label 2

Scope Name

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Conditional expression

Total Replay Time <> "0"

Record

IE Scenario (PI_IES)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name

IE Scenario Replay Time Status (real-time report)

Overview

IE Scenario Replay Time Status report displays the IE scenario-related replay time on a real-time basis.

Display format

A table and a line graph

Y-axis of the graph

Total Replay Time

Data label 1

Measurement Condition Name

Data label 2

Scope Name

Storage location

Reports/Service Response/Status Reporting/Real-Time

Conditional expression

Total Replay Time > "0"

Record

IE Scenario (PI_IES)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Replay Time	Total replay time required for a series of the operations in an IE scenario (time for the entire IE scenario)
Result Strings	Measurement result

Drilldown reports (field level)

Report name	Description
IE Scenario Detail	Displays the response time for each scope in an IE scenario
IE Scenario Scope Rate	Displays the percentage ratio of each scope in an IE scenario
IE Scenario Top 10	Displays the top 10 IE scenarios in terms of total replay time

IE Scenario Replay Time Summary

Overview

The IE Scenario Replay Time Summary report displays the IE scenario-related replay time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Y-axis of the graph

Total Replay Time

Data label 1

Measurement Condition Name

Data label 2

Scope Name

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Conditional expression

Total Replay Time > "0"

Record

IE Scenario (PI_IES)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Replay Time	Total replay time required for a series of operations (time for the entire IE scenario)
Result Strings	Measurement result

IE Scenario Replay Time Trend

Overview

The IE Scenario Replay Time Trend report displays the IE scenario-related replay time over the past month on a daily basis.

Display format

A table and a line graph

Y-axis of the graph

Total Replay Time

Data label 1

Measurement Condition Name

Data label 2

Scope Name

Storage location

Reports/Service Response/Monthly Trend

Conditional expression

Total Replay Time > "0"

Record

IE Scenario (PI_IES)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Replay Time	Total replay time required for a series of the operations (time for the entire IE scenario)

IE Scenario Scope Detail

Overview

IE Scenario Scope Detail report displays the replay time for each scope in an IE scenario.

Display format

A stacked column graph

Y-axis of the graph

Total Replay Time

Data label 1

Measurement Condition Name

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

IE Scenario Overview (PI_IESO)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Replay Time 1	Replay time required for a series of the operations specified as the scope 1
Total Replay Time 2	Replay time required for a series of the operations specified as the scope 2
Total Replay Time 3	Replay time required for a series of the operations specified as the scope 3
Total Replay Time 4	Replay time required for a series of the operations specified as the scope 4
Total Replay Time 5	Replay time required for a series of the operations specified as the scope 5
Total Replay Time 6	Replay time required for a series of the operations specified as the scope 6
Total Replay Time 7	Replay time required for a series of the operations specified as the scope 7
Total Replay Time 8	Replay time required for a series of the operations specified as the scope 8
Total Replay Time 9	Replay time required for a series of the operations specified as the scope 9
Total Replay Time 10	Replay time required for a series of the operations specified as the scope 10
Total Replay Time 11	Replay time required for a series of the operations specified as the scope 11
Total Replay Time 12	Replay time required for a series of the operations specified as the scope 12
Total Replay Time 13	Replay time required for a series of the operations specified as the scope 13
Total Replay Time 14	Replay time required for a series of the operations specified as the scope 14
Total Replay Time 15	Replay time required for a series of the operations specified as the scope 15
Total Replay Time 16	Replay time required for a series of the operations specified as the scope 16

Drilldown reports (field level)

Report name	Description
IE Scenario Detail	Displays the detailed information for the scopes in an IE scenario

IE Scenario Scope Rate

Overview

IE Scenario Scope Rate report displays the percentage ratio of each scope in an IE scenario.

Display format

A pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time

Record

IE Scenario Overview (PI_IESO)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Replay Time 1	Replay time required for a series of IE scenarios specified as the scope 1
Total Replay Time 2	Replay time required for a series of IE scenarios specified as the scope 2
Total Replay Time 3	Replay time required for a series of IE scenarios specified as the scope 3
Total Replay Time 4	Replay time required for a series of IE scenarios specified as the scope 4
Total Replay Time 5	Replay time required for a series of IE scenarios specified as the scope 5
Total Replay Time 6	Replay time required for a series of IE scenarios specified as the scope 6
Total Replay Time 7	Replay time required for a series of IE scenarios specified as the scope 7
Total Replay Time 8	Replay time required for a series of IE scenarios specified as the scope 8
Total Replay Time 9	Replay time required for a series of IE scenarios specified as the scope 9
Total Replay Time 10	Replay time required for a series of IE scenarios specified as the scope 10
Total Replay Time 11	Replay time required for a series of IE scenarios specified as the scope 11
Total Replay Time 12	Replay time required for a series of IE scenarios specified as the scope 12
Total Replay Time 13	Replay time required for a series of IE scenarios specified as the scope 13
Total Replay Time 14	Replay time required for a series of IE scenarios specified as the scope 14
Total Replay Time 15	Replay time required for a series of IE scenarios specified as the scope 15
Total Replay Time 16	Replay time required for a series of IE scenarios specified as the scope 16

IE Scenario Top 10

Overview

The IE Scenario Top 10 report displays the top 10 IE scenario in terms of total replay time.

In descending order check box

You must specify.

Display format

A bar graph

Y-axis of the graph

Total Replay Time

Data label 1

Measurement Condition Name

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

IE Scenario Overview (PI_IESO)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Replay Time	Total replay time required for the IE scenario

Drilldown reports (field level)

Report name	Description
IE Scenario Detail	Displays the detailed information for the IE scenario

Drilldown conditions

Report name	Condition
IE Scenario Detail	(Total Replay Time <> "0" AND Measurement Condition ID = metric("Measurement Condition ID"))AND Scope Id <> "0"

IMAP4 Rate

Overview

The IMAP4 Rate report displays the percentage ratio of the detailed response time for each operation in IMAP4 service on a real-time basis. This is a drilldown report.

Display format

A list and a pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

IMAP4 (PI_IMP4)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
DNS Time	DNS time
TCP Connection Time	TCP connection time
Preprocessing Time	Preprocessing time
Data Transfer Time	Data transfer time
Deletion Time	Deletion time

IMAP4 Response Time Status

Overview

The IMAP4 Response Time Status report displays the IMAP4-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

IMAP4 (PI_IMP4)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving in an inbox a new email addressed to the specified user

IMAP4 Response Time Status (real-time report)

Overview

The IMAP4 Response Time Status report displays the IMAP4-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

IMAP4 (PI_IMP4)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving in an inbox a new email addressed to the specified user
Result Strings	Measurement result

IMAP4 Response Time Summary

Overview

The IMAP4 Response Time Summary report displays the IMAP4-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

IMAP4 (PI_IMP4)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving in an inbox a new email addressed to the specified user
Result Strings	Measurement result

IMAP4 Response Time Trend

Overview

The IMAP4 Response Time Trend report displays the IMAP4-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

IMAP4 (PI_IMP4)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving in an inbox a new email addressed to the specified user

IMAP4 Top 10

Overview

The IMAP4 Top 10 report displays the top 10 IMAP4 services in terms of total response time. This is a drilldown report.

Display format

A bar graph

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

IMAP4 (PI_IMP4)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving in an inbox a new email addressed to the specified user

Drilldown reports (field level)

Report name	Description
IMAP4 Rate	Percentage ratio of the detailed response time for each operation in IMAP4 service

POP3 Rate

Overview

The POP3 Rate report displays the percentage ratio of the detailed response time for each operation in POP3 service on a real time basis. This is a drilldown report.

Display format

A list and a pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

POP3 (PI_POP3)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
DNS Time	DNS time
TCP Connection Time	TCP connection time
Preprocessing Time	Preprocessing time
Data Transfer Time	Data transfer time
Deletion Time	Deletion time

POP3 Response Time Status

Overview

The POP3 Response Time Status report displays the POP3-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

POP3 (PI_POP3)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving an email addressed to the specified user

POP3 Response Time Status (real-time report)

Overview

The POP3 Response Time Status report displays the POP3-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

POP3 (PI_POP3)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving an email addressed to the specified user
Result Strings	Measurement result

POP3 Response Time Summary

Overview

The POP3 Response Time Summary report displays the POP3-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

POP3 (PI_POP3)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving an email addressed to the specified user
Result Strings	Measurement result

POP3 Response Time Trend

Overview

The POP3 Response Time Trend report displays the POP3-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

POP3 (PI_POP3)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving an email addressed to the specified user

POP3 Top 10

Overview

The POP3 Top 10 report displays the top 10 POP3 services in terms of total response time.

Display format

A bar graph

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

POP3 (PI_POP3)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for receiving an email addressed to the specified user

Drilldown reports (field level)

Report name	Description
POP3 Rate	Percentage ratio of the detailed response time for each operation in POP3.

Scope Detail

Overview

The Scope Detail report displays the details of each scope of the Web transaction on a real-time basis. This is a drilldown report.

Display format

A list

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

Web Transaction (PI_WT)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Measurement Start Time	Character string corresponding to the measurement result code
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses (time per scope)
Setup Time	Setup time
HTTP Time	HTTP time
DNS Time	DNS time
TCP Connection Time	TCP connection time
Server Procession Time	Server processing time
Data Transfer Time	Data transfer time
Total Amount of Data	Total amount of data
Total Resource Size	Total resource size
Throughput	Throughput
Result Strings	Measurement start time

SMTP Rate

Overview

The SMTP Rate report displays the percentage ratio of the detailed response time for each operation in SMTP on a real-time basis. This is a drilldown report.

Display format

A list and a pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

SMTP (PI_SMTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
DNS Time	DNS time
TCP Connection Time	TCP connection time
Preprocessing Time	Preprocessing time
Data Transfer Time	Data transfer time

SMTP Response Time Status

Overview

The SMTP Response Time Status report displays the SMTP-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

SMTP (PI_SMTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for completing message transmission to the target server being measured, or for creating a message with the specified message size and then completing its transmission to the destination address

SMTP Response Time Status (real-time report)

Overview

The SMTP Response Time Status report displays the SMTP-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

SMTP (PI_SMTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for completing message transmission to the target server being measured, or for creating a message with the specified message size and then completing its transmission to the destination address
Result Strings	Measurement result

SMTP Response Time Summary

Overview

The SMTP Response Time Summary report displays the SMTP-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

SMTP (PI_SMTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for completing message transmission to the target server being measured, or for creating a message with the specified message size and then completing its transmission to the destination address
Result Strings	Measurement result

SMTP Response Time Trend

Overview

The SMTP Response Time Trend report displays the SMTP-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

SMTP (PI_SMTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for completing message transmission to the target server being measured, or for creating a message with the specified message size and then completing its transmission to the destination address

SMTP Top 10

Overview

The SMTP Top 10 report displays the top 10 SMTP services in terms of total response time.

Display format

A bar graph

Storage location

Reports/Service Response/ Troubleshooting/Real-Time

Record

SMTP (PI_SMTP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for completing message transmission to the target server being measured, or for creating a message with the specified message size and then completing its transmission to the destination address

Drilldown reports (field level)

Report name	Description
SMTP Rate	Percentage ratio of the detailed response time for each operation in SMTP

TCP Response Time Status

Overview

The TCP Response Time Status report displays the TCP-related response time over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

TCP (PI_TCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for establishing connection with the target server being measured

TCP Response Time Status (real-time report)

Overview

The TCP Response Time Status report displays the TCP-related response time on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

TCP (PI_TCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for establishing connection with the target server being measured
Result Strings	Measurement result

TCP Response Time Summary

Overview

The TCP Response Time Summary report displays the TCP-related response time over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

TCP (PI_TCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for establishing connection with the target server being measured
Result Strings	Measurement result

TCP Response Time Trend

Overview

The TCP Response Time Trend report displays the TCP-related response time over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

TCP (PI_TCP)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for establishing connection with the target server being measured

Transaction Detail

Overview

The Transaction Detail report displays the total response time for each scope of the Web transaction on a real-time basis. This is a drilldown report.

Display format

A column graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time/Drilldown Only

Record

Web Transaction (PI_WT)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses (time per scope)

Drilldown reports (field level)

Report name	Description
Scope Detail	Details of each scope of the Web transaction

User Defined Service Response Time Status

Overview

The User Defined Service Response Time Status report displays the response time for a user-defined service over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

User Defined Service (PI_UDEF)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Measurement result of the user-defined program, such as a program for measuring response time

User Defined Service Response Time Status (real-time report)

Overview

The User Defined Service Response Time Status report displays the response time for a user-defined service on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

User Defined Service (PI_UDEF)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Measurement result of the user-defined program, such as a program for measuring response time
Result Strings	Measurement result

User Defined Service Response Time Summary

Overview

The User Defined Service Response Time Summary report displays the response time for a user-defined service over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

User Defined Service (PI_UDEF)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Measurement result of the user-defined program, such as a program for measuring response time
Result Strings	Measurement result

User Defined Service Response Time Trend

Overview

The User Defined Response Time Trend report displays the response time for a user-defined service over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

User Defined Service (PI_UDEF)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Measurement result of the user-defined program, such as a program for measuring response time

Web Transaction Response Time Status

Overview

The Web Transaction Response Time Status report displays the response time for a Web transaction over the past 24 hours on an hourly basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Daily Trend

Record

Web Transaction (PI_WT)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses (time for the entire transaction)

Web Transaction Response Time Status (real-time report)

Overview

The Web Transaction Response Time Status report displays the response time for a Web transaction on a real-time basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Status Reporting/Real-Time

Record

Web Transaction (PI_WT)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses (time for the entire transaction)
Result Strings	Measurement result

Drilldown reports (field level)

Report name	Description
Web Transaction Scope Detail	Displays the response time for each scope in a Web transaction
Web Transaction Rate	Displays the percentage ratio of each scope in a Web transaction
Web Transaction Top 10	Displays the top 10 Web transactions in terms of total response

Web Transaction Response Time Summary

Overview

The Web Transaction Response Time Summary report displays the response time for a Web transaction over the past hour on a minute-by-minute basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Troubleshooting/Recent Past

Record

Web Transaction (PI_WT)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses (time for the entire transaction)
Result Strings	Measurement result

Web Transaction Response Time Trend

Overview

The Web Transaction Response Time Trend report displays the response time for a Web transaction over the past month on a daily basis.

Display format

A table and a line graph

Storage location

Reports/Service Response/Monthly Trend

Record

Web Transaction (PI_WT)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Scope Name	Scope name
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses (time for the entire transaction)

Web Transaction Scope Detail

Overview

The Web Transaction Scope Detail report displays the response time for each scope in a Web transaction.

Display format

A stacked column graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time

Record

Web Transaction Overview (PI_WTO)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time 1	Time required for the series of HTTP or HTTPS requests and responses specified in scope 1
Total Response Time 2	Time required for the series of HTTP or HTTPS requests and responses specified in scope 2
Total Response Time 3	Time required for the series of HTTP or HTTPS requests and responses specified in scope 3
Total Response Time 4	Time required for the series of HTTP or HTTPS requests and responses specified in scope 4
Total Response Time 5	Time required for the series of HTTP or HTTPS requests and responses specified in scope 5
Total Response Time 6	Time required for the series of HTTP or HTTPS requests and responses specified in scope 6
Total Response Time 7	Time required for the series of HTTP or HTTPS requests and responses specified in scope 7
Total Response Time 8	Time required for the series of HTTP or HTTPS requests and responses specified in scope 8

Drilldown reports (field level)

Report name	Description
Scope Detail	Details of each scope of the Web transaction

Web Transaction Scope Rate

Overview

The Web Transaction Scope Rate report displays the percentage ratio of each scope in a Web transaction.

Display format

A pie graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time

Record

Web Transaction Overview (PI_WTO)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time 1	Time required for the series of HTTP or HTTPS requests and responses specified in scope 1
Total Response Time 2	Time required for the series of HTTP or HTTPS requests and responses specified in scope 2
Total Response Time 3	Time required for the series of HTTP requests and responses specified in scope 3
Total Response Time 4	Time required for the series of HTTP or HTTPS requests and responses specified in scope 4
Total Response Time 5	Time required for the series of HTTP or HTTPS requests and responses specified in scope 5
Total Response Time 6	Time required for the series of HTTP or HTTPS requests and responses specified in scope 6
Total Response Time 7	Time required for the series of HTTP or HTTPS requests and responses specified in scope 7
Total Response Time 8	Time required for the series of HTTP or HTTPS requests and responses specified in scope 8

Drilldown reports (field level)

Report name	Description
Scope Detail	Details of each scope of the Web transaction

Web Transaction Top 10

Overview

The Web Transaction Top 10 report displays the top 10 Web transactions in terms of the total response time.

Display format

A bar graph

Storage location

Reports/Service Response/Troubleshooting/Real-Time

Record

Web Transaction Overview (PI_WTO)

Fields

Field name	Description
Measurement Condition Name	Label corresponding to the measurement condition ID
Total Response Time	Time required for a series of HTTP or HTTPS requests and responses

Drilldown reports (field level)

Report name	Description
Transaction Detail	Total response time for each scope of the Web transaction

10

Records

This chapter explains PFM - Agent for Service Response. For details about how to collect performance data for each record, see the chapter explaining the functions of Performance Management in the *JP1/Performance Management Planning and Configuration Guide*, or the chapter explaining the management of operation monitoring data in the *JP1/Performance Management User's Guide*.

Data model

Each PFM - Agent's records and fields are referred to collectively as a *data model*. There is a specific version number for each PFM - Agent and its data model. For details about data model versions of PFM - Agent for Service Response, see *H. Version Compatibility*.

The version number of each PFM - Agent's data model is displayed in the windows for defining the monitoring template for alarms, reports, and PFM - Web Console alarms.

For details about the data model, see the chapter that describes the functions of Performance Management in the *JPI/Performance Management Planning and Configuration Guide*.

Format of record explanations

This chapter describes the records for PFM - Agent for Service Response in alphabetical order. Each record explanation contains the subsections described below.

Function

Provides an overview of the performance data that is stored in the record, and includes important information that should be noted.

Default and changeable values

Consists of a table of the default values for the performance data under the collection conditions defined for the record; also indicates whether or not each value can be changed by the user. The table below lists and describes each item that is included in *Default and changeable values*. For details about the items described in this table, see the chapter that describes management of operation monitoring data in the *JPI/Performance Management User's Guide*.

Table 10–1: Default values and changeable values

Item	Description	Changeable
Collection Interval	Shows the performance data collection interval (in seconds)	Y: Changeable
Collection Offset	Shows the offset value for starting performance data collection (in seconds). For details about the offset value, see the chapter that describes management of operation monitoring data in the <i>JPI/Performance Management User's Guide</i> . For details about the start time of performance data collection, see the chapter explaining the functions of Performance Management in the <i>JPI/Performance Management Planning and Configuration Guide</i> .	N: Not changeable
Log	Shows whether or not collected performance data is stored in the Store database: Yes: Stored (however, if <code>Collection Interval=0</code> is set, collected performance data is not stored) No: Not stored	
LOGIF	Shows any conditions for storing collected performance data in the Store database	
Over 10 Sec Collection Time ^{#1,#2}	Whether the collection of records might require 10 seconds or more. Yes: Might require 10 seconds or more. No: Does not require 10 seconds.	

#1

This property is displayed if the collection of historical data is prioritized over the display processing of real-time reports. For details, see the chapter on troubleshooting in the *JPI/Performance Management User's Guide*.

#2

The value of this item is an approximation at best. Depending on the environment being monitored, the configuration, the load status, and even the collection of records whose value is `No` might require 10 seconds or more. In such cases, real-time reports might not be displayed.

In addition, depending on the collection interval and offset settings, real-time reports might not be displayed if the collection of historical data takes place successively for multiple records, even when the collection time for each record is short.

ODBC key fields

These fields display the primary keys that are necessary to use the data retrieved from records stored in the Store database on either PFM - Manager or PFM - Base. Some ODBC key fields are common to all records, and some are specific to particular records. This section presents the ODBC key fields that are specific to the particular record. Only multi-instance records have specific ODBC key fields.

For details about the ODBC key fields common to all records, see *List of ODBC key fields* in this chapter.

Lifetime

Indicates the period during which consistency is guaranteed for the performance data that is collected in the record. For details about the lifetime, see the chapter that describes the functions of Performance Management in the *JP1/Performance Management System Configuration and User's Guide*.

Record size

Indicates the amount of performance data that can be collected and stored in the record at one time.

Fields

Provides a table that describes the record's fields. The table contains the following columns:

- View name (Manager name)
 - View name
Indicates the field name (PFM - View name) that is displayed with PFM - Web Console.
 - Manager name
Indicates the field name (PFM - Manager name) to be specified in SQL statements used from PFM - Manager to access the field data stored in the Store database.
You specify the record ID at the beginning of an SQL statement. For example, to specify the Total Response Time (`TOTAL_RESP_TIME`) field of the DNS (`PI_DNS`) record, specify `PI_DNS_TOTAL_RESP_TIME`.
- Description
Explains the performance data that is stored in the field.
- Summary
Indicates the method (summarization rules) to be used by Agent Store when summarizing data. For details about summarization rules, see *Summary rules* later in this chapter.
- Format
Shows the data type of the field's values, such as `char` or `float`. For details about the data types, see *List of data types* later in this chapter.
- Delta
In contrast to data collected as a cumulative value, the so-called *delta* is data that indicates the change in the values. For details about delta, see *Field values* later in this chapter.
- Data source
Identifies the method used to obtain the field value or the source of the data. For details about field values, see *Field values* later in this chapter.

List of ODBC key fields

Some ODBC key fields are common to all records, and some are specific to particular records. This section explains the ODBC key fields that are common to all records. The ODBC key fields are necessary to use the data retrieved from records stored in the Store database on PFM - Manager.

The table below lists the ODBC key fields common to all records. For details about the ODBC key fields specific to particular records, see the descriptions of the records.

Table 10–2: List of ODBC key fields common to all records

ODBC key field	ODBC format	Data	Description
<i>record-ID</i> _DATE	SQL_INTEGER	Internal	Record key field that indicates the record's creation date
<i>record-ID</i> _DATETIME	SQL_INTEGER	Internal	Combination of the two fields <i>record-ID</i> _DATE and <i>record-ID</i> _TIME
<i>record-ID</i> _DEVICEID	SQL_VARCHAR	Internal	Name of the host where PFM - Agent is running
<i>record-ID</i> _DRAWER_TYPE	SQL_VARCHAR	Internal	Type. Valid values are as follows: m: Minute H: Hour D: Day W: Week M: Month Y: Year
<i>record-ID</i> _PROD_INST	SQL_VARCHAR	Internal	Instance name of PFM - Agent
<i>record-ID</i> _PRODID	SQL_VARCHAR	Internal	Product ID of PFM - Agent
<i>record-ID</i> _RECORD_TYPE	SQL_VARCHAR	Internal	Identifier indicating the record type (4 bytes)
<i>record-ID</i> _TIME	SQL_INTEGER	Internal	Record creation time (Greenwich mean time (GMT))

Summary rules

For records of the PI record type, two types of data are stored in the Store database: the data collected at the interval set in *Collection Interval*, and the data summarized for a specific period of time (minute, hour, day, week, month, or year) according to a predefined rule. The type of summarization is defined for each field. This definition is called a *summarization rule*. Depending on the summarization rule, intermediate data used during the summarization period must sometimes be retained. In this case, a field for holding the intermediate data is added to a record in the Store database. This field is called an *added field*.

Some added fields are displayed as record fields in PFM - Web Console; these added fields can be used as fields to be displayed in historical reports.

To distinguish from *added fields* that are added by the process of summarization, the fields that are explained in the description of each record are called *fixed fields*.

The name of an added field is as follows:

- Name of an added field when it is stored in the Store database
Manager name of the fixed field with a suffix
- Name of an added field when it is displayed in PFM - Web Console
View name of the fixed field with a suffix

The following table lists the suffixes for the Manager name, the suffixes for the corresponding View names, and the data that is stored in the fields.

Table 10–3: List of suffixes for added fields

Manager name	View name	Stored data
<code>_TOTAL</code>	(Total)	Sum of the field's values in the records collected over the summary period
<code>_COUNT</code>	--	Number of records collected over the summary period
<code>_HI</code>	(Max)	Field's maximum value in the records collected over the summary period
<code>_LO</code>	(Min)	Field's minimum value in the records collected over the summary period

Legend:

--: There is no added field.

The following table lists and describes the summary rules.

Table 10–4: List of summary rules

Summary rule name	Summary rule
COPY	Stores the field's value that is set in the most recent record within the summary period.
AVG	Stores the field's average value over the summary period. The formula is as follows: $\frac{\text{(Sum of field values)}}{\text{(number of collected records)}}$ Added fields (Store database) <ul style="list-style-type: none">• <code>_TOTAL</code>• <code>_COUNT</code> Added field (PFM - Web Console)

Summary rule name	Summary rule
AVG	<ul style="list-style-type: none">• (Total)
--	No summarization

List of data types

The table below lists the data types for field values and the corresponding C and C++ data types. The values shown in the *Format* column of the record field tables are those shown below in the *Field* column under *Data type*.

Table 10–5: List of data types

Data type		Size (bytes)	Description
Field	C and C++		
char (<i>n</i>)	char ()	Number inside ()	Character data (0x20 to 0x7e) Character string having a length of <i>n</i> bytes
double	double	8	Numeric value (1.7E±308 (15 digits))
float	float	4	Numeric value (3.4E±38 (7 digits))
long	long	4	Numeric value (-2,147,483,648 to 2,147,483,647)
short	short	2	Numeric value (-32,768 to 32,767)
string (<i>n</i>)	char[]	Value in parentheses	Character string with a length of <i>n</i> bytes. The last character is null.
time_t	unsigned long	4	Numeric value (0 to 4,294,967,295)
timeval	Structure	8	Numeric value (first 4 bytes are seconds, next 4 bytes are microseconds)
ulong	unsigned long	4	Numeric value (0 to 4,294,967,295)
utime	Structure	8	Numeric value (first 4 bytes are seconds, next 4 bytes are microseconds)
word	unsigned short	2	Numeric value (0 to 65,535)
(Not applicable)	unsigned char	1	Numeric value (0 to 255)

Field values

This section describes the values stored in the fields.

Data source

Each field contains a value obtained from a Performance Management product or monitored program, or a value derived by applying a formula. In the tables, the *Data source* column indicates the source of the value or the formula used to produce the value.

For PFM - Agent for Service Response, the value of each field is the result of measurement by the IE Probe Daemon and the Probe Daemon.

Delta

In contrast to data collected as a cumulative value, the so-called *delta* is data that indicates the change in values. For example, if the performance data value obtained during the first collection is 3 and the performance data value obtained during the second collection is 4, then the cumulative value is 7, and the change in the values is 1. In the tables, the *Delta* column indicates whether or not a field's value is the delta value.

The following table explains the delta characteristics of performance data collected by PFM - Agent for Service Response:

Table 10–6: Performance data collected by PFM - Agent for Service Response

Record type	Delta	Data type	Indicate delta value#	Record value
PI record type	Yes	--	--	--
	No	Real-time data	Selected	The displayed value was the actual value at the time of data collection.
			Not selected	The displayed value was the actual value at the time of data collection.
		- Historical data - Alarm monitoring data	--	The displayed value was the actual value at the time of data collection.
PD record type	Yes	--	--	--
		- Historical data - Alarm monitoring data	--	The displayed value is the cumulative value.
	No	Real-time data	Selected	The displayed value was the actual value at the time of data collection.
			Not selected	The displayed value was the actual value at the time of data collection.
		- Historical data - Alarm monitoring data	--	The displayed value was the actual value at the time of data collection.
PL record type	No	Real-time data	Selected	The displayed value was the actual value at the time of data collection.

Record type	Delta	Data type	Indicate delta value [#]	Record value
PL record type	No	Real-time data	Not selected	The displayed value was the actual value at the time of data collection.
		- Historical data - Alarm monitoring data	--	The displayed value was the actual value at the time of data collection.

Legend:

--: Not applicable

#

Indicates whether or not the following PFM - Web Console items are selected:

- **Indicate delta value** in the report wizard's New Report > Indication settings(Realtime) window
- **Indicate delta value** in **Indication settings(Realtime)** on the **Properties** page in the report window

Fields that are added only when a record is recorded in the Store database

The following table lists the fields that are added only when data is recorded in the Store database:

Table 10–7: Fields that are added only when a record is recorded in the Store database

View name (Manager name)	Description	Format	Delta	Supported version	Data source#1
Agent Host (DEVICEID)	Name of host where PFM - Agent is running	string (256)	No	All	--
Agent Instance (PROD_INST)	Name of host where PFM - Agent is running	string (256)	No	All	--
Agent Type (PRODID)	Product ID of PFM - Agent (1-byte identifier)	char	No	All	--
Date (DATE)	Record creation date (GMT)#1,#2	char (3)	No	All	--
Date and Time (DATETIME)	Combination of the Date (DATE) and Time (TIME) fields#2	char (6)	No	All	--
Drawer Type (DRAWER_TYPE)	For a record of the PI record type, this is the data summarization type.	char	No	All	--
GMT Offset (GMT_ADJUST)	Difference (in seconds) between Greenwich Mean Time and local time	long	No	All	--
Time (TIME)	Record creation time (GMT)#1,#2	char (3)	No	All	--

Legend:

--: Indicates that the field's value is obtained without processing acquired performance data.

#1

Reference time during summarization is set because data is summarized for records of the PI record type. The following table shows the setting value for each record type:

Table 10–8: Setting for each record category

Type	Setting value for each record type
Minute	0 second of the time when the record was created
Hour	0 minute and 0 second of the time when the record was created
Day	0:00 and 0 second of the day when the record was created
Week	0:00 and 0 second on Monday of the week when the record was created
Month	0:00 and 0 second on the 1st day of the month when the record was created
Year	0:00 and 0 second on January 1st of the year when the record was created

#2

When data is displayed in reports, the Date field is displayed in the format *YYYYMMDD*, the Date and Time field is displayed in the format *YYYYMMDD hh:mm:ss*, and the Time field is displayed in the format *hh:mm:ss*.

Common fields

The following table lists and describes the fields that are common to all records of PFM - Agent for Service Response.

The following table shows the fields that are common to all records of PFM - Agent for Service Response, other than the unique fields of each record:

Table 10–9: List of Common fields (to PD_record, PI_record, and PL_record)

View name (Manager name)	Description	Summary	Format	Delta	Data source
Interval (INTERVAL)	Collection interval during which the record was stored.	ADD	ulong	Yes	Agent Collector
Record Time (RECORD_TIME)	Time at which the record was created.	COPY	time_t	No	Agent Collector
Record Type (INPUT_RECORD_TYPE)	The <i>xxxx</i> part of the record IDs shown in the Table 10-13 (PD_XXXX, PI_XXXX, and PL_XXXX).	COPY	string(8)	No	Agent Collector

The following table shows the fields that are common only to PI_record.

Table 10–10: Common fields (only to PI_record)

View name (Manager name)	Description	Summary	Format	Delta	Data source
Measurement Start Time (MSR_START_TIME)	Measurement start time	COPY	time_t	No	Probe Daemon and IE Probe Daemon ^{#1}
Measurement Condition ID (MSR_COND_ID)	Measurement condition ID	COPY	Long	No	Probe Daemon and IE Probe Daemon ^{#1}
Measurement Condition Name (MSR_COND_NAME)	The label (any specified name) corresponding to the measurement condition. Stores the first matched label by searching within the following labels in this order: <ol style="list-style-type: none"> The labels defined in the measurement condition registration file. The labels defined in the measurement condition label definition file. <p>If the label of the measurement condition is not defined in the both file, <i>service-type-name_measurement-condition-ID</i> is stored.</p>	COPY	string (up to 63 bytes)	No	Probe Daemon and IE Probe Daemon ^{#1}
Result Code (RESULT_CODE)	Measurement result code ^{#2}	COPY	short	No	Probe Daemon and IE Probe Daemon ^{#1}
Result Strings (RESULT_STR)	Character string corresponding to the measurement result code ^{#2}	COPY	string (up to 31 bytes)	No	Probe Daemon

View name (Manager name)	Description	Summary	Format	Delta	Data source
Result Strings (RESULT_STR)	Character string corresponding to the measurement result code ^{#2}	COPY	string (up to 31 bytes)	No	and IE Probe Daemon ^{#1}
Service Type ID (SERV_TYPE_ID)	Service type ID ^{#3}	COPY	short	No	Probe Daemon and IE Probe Daemon ^{#1}
Service Type Name (SERV_TYPE_NAME)	Service type name	COPY	string (up to 31 bytes)	No	Probe Daemon

#1

For IE Scenario (PI_IE) record, IE Scenario Overview (PI_IEO) record, and Logged Message for IE Scenario (PL_IESM) record, their data source is the IE Probe Daemon.

Otherwise, the data source is the Probe Daemon.

#2

The following table lists and describes the result codes and the character strings that correspond to the result codes. For details about the error, see the integrated trace log.

Table 10–11: Result code

Value	Code	Character string	Description
0	Success	SUCCESS	Measurement terminated normally.
1	Network error	NETWORK ERROR	Processing was cancelled due to a network or server failure that interrupted communication. For example: <ul style="list-style-type: none"> Name resolution has failed by DNS. TCP connection has failed. To close TCP connection has failed. Web server has stopped. For details about the network error, see the integrated trace log.
2	Timeout	TIME OUT	Processing cannot be completed within the specified timeout value.
3	Service error	SERVICE ERROR	The server is running normally, but the requested page or file cannot be acquired. For example: <ul style="list-style-type: none"> The user name or the password is incorrect. SSL authentication failed in measurements of HTTPS (including Web transactions).
4	User-defined command error	USER_DEF_COMMAND ERROR	A user-defined command resulted in an error, such as in a program that does not support the user-defined command.
5	Unmatched response contents	UNMATCHED CONTENT	The page acquired by an IE scenario or a Web transaction does not satisfy the conditions (response determination information).
6	Replay IE scenario error	IE SCENARIO REPLAY ERROR	An error occurred while replaying the IE scenario. For example:

Value	Code	Character string	Description
6	Replay IE scenario error	IE SCENARIO REPLAY ERROR	<ul style="list-style-type: none"> The tag operated when the IE scenario was recorded is not found. The frame is not found. A dialog box that is not recorded appears. For details, see <i>5.2.3(3) Notes on recording and replaying the IE scenarios</i> .
7	IE scenario Navigation error	IE SCENARIO NAVIGATE ERROR	A navigation error occurred during replaying the IE scenario. For details, see <i>5.2.4 Notes on the navigation</i> .
99	Other	OTHER ERROR	Other error For example: <ul style="list-style-type: none"> Memory was insufficient during measurement. An unexpected error occurred.

#3

The following table lists the service type IDs.

Table 10–12: Service type IDs

Service	Service type name	Service type ID
HTTP	HTTP	101
HTTPS	HTTPS	102
SMTP	SMTP	103
POP3	POP3	104
IMAP4	IMAP4	105
DNS	DNS	106
DHCP	DHCP	107
FTP	FTP	108
TCP	TCP	109
Web transaction	WEBTRANS	110
IE scenario	IESCENA	111
User-defined service	USERSERV	199

List of records

The following tables list, in the alphabetical order of the record names (view name), the records that can be collected by PFM - Agent for Service Response and the information that is stored in each record.

Table 10–13: List of records for PFM - Agent for Service Response (in the order of record name)

Record name (View name)	Record ID (Manager name)	Information stored in record
<i>DHCP</i>	PI_DHCP	DHCP service response time
<i>DNS</i>	PI_DNS	DNS service response time
<i>FTP</i>	PI_FTP	FTP service response time
<i>HTTP</i>	PI_HTP	HTTP service response time
<i>HTTPS</i>	PI_HTTPS	HTTPS service response time
<i>IE Scenario</i>	PI_IES	IE scenario replaying time for each scope
<i>IE Scenario Overview</i>	PI_IESO	Summary information about the replaying time for each scope in an IE scenario
<i>IMAP4</i>	PI_IMP4	IMAP4 service response time
<i>Logged Message for IE Scenario</i>	PL_IESM	Message information that is output in the Event Log and the log files
<i>POP3</i>	PI_POP3	POP3 service response time
<i>Service Summary Interval</i>	PI_PI	Response time of each service
<i>SMTP</i>	PI_SMTP	SMTP service response time
<i>TCP</i>	PI_TCP	TCP service response time
<i>User Defined Service</i>	PI_UDEF	User-defined service response time
<i>Web Transaction</i>	PI_WT	Web transaction service response time for a scope
<i>Web Transaction Overview</i>	PI_WTO	Summary information about the response times for the scopes in a Web transaction
Product Detail	PD_PD	Reserved record not available for use

DHCP (PI_DHCP)

Function

The DHCP (PI_DHCP) record stores information about DHCP service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_DHCP_MSR_COND_ID

Lifetime

None

Record size

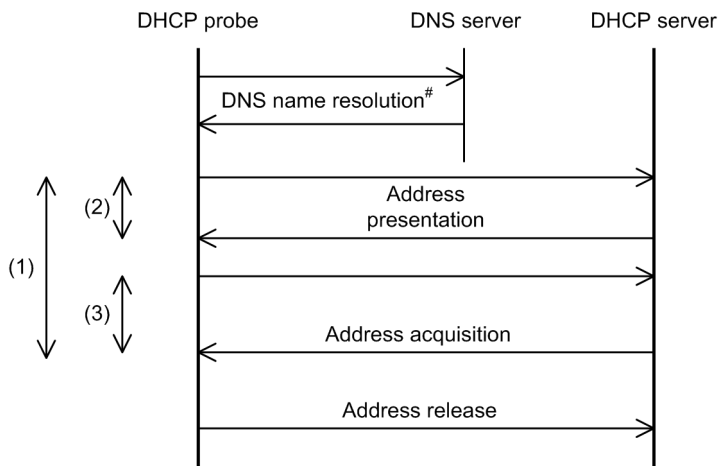
- Fixed part: 681 bytes
- Variable part: 220 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Address Assignment Time (ADDR_ASSIGN_TIME)	Address presentation time (seconds) ((2) in Figure 10-1)	AVG	double	No	Probe Daemon
Address Reservation Time (ADDR_RESERV_TIME)	Address acquisition time (seconds) ((3) in Figure 10-1)	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the DHCP probe and the monitored server on UDP (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-1)	AVG	double	No	Probe Daemon

The following figure shows the DHCP sequence.

Figure 10–1: DHCP sequence



If an IP address is specified for the DHCP server host name in the measurement condition, name resolution is not performed by DNS.

DHCP operating environment and notes

A DHCP probe searches for the measurement-target DHCP server and measures the time required for dynamically acquiring the IP address.

The following describes and provides notes on a DHCP operating environment.

Acquisition of IP address

The DHCP probe broadcasts an address presentation request and receives an address presentation from the DHCP server. To accept the presented IP address, address acquisition as shown in Figure 10-1 is performed. If the presented IP address is not to be accepted, address acquisition is not performed.

The address presentation request, address acquisition request, and their responses are all sent by broadcasting.

Release of IP address

If IP address acquisition is successful, address release as shown in Figure 10-1 is performed. If the presented IP address is not to be accepted, or if acquisition fails, address release is not performed. The time required for this address release is not included in the total response time.

Port number of the probe

Specify the port number of the DHCP client that has been defined at the monitoring-target DHCP server. Do not define more than one measurement item with the same probe port number.

RFC compliance

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- For the functions that are not compliance with RFCs and the restrictions, see the above notes.

DNS (PI_DNS)

Function

The DNS (PI_DNS) record stores information about DNS service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_DNS_MSR_COND_ID

Lifetime

None

Record size

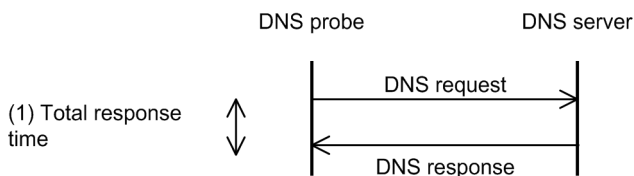
- Fixed part: 681 bytes
- Variable part: 180 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the DNS probe and the measurement-target server on UDP (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-2)	AVG	double	No	Probe Daemon

The following figure shows the DNS sequence.

Figure 10–2: DNS sequence



DNS operating environment and notes

A DNS probe queries the DNS server for the IP address of the specified search-target host name, and measures the time required for receiving the response.

The following describes and provides notes on a DNS operating environment.

Retry timeout value

The retry timeout value is determined automatically by the following formula:

Retry timeout value = timeout value/(retries count + 1)

Resolution of search-target host name

Measurement fails if the IP address cannot be obtained due to an error in resolving the search-target host name.

RFC compliance

- RFC1034: Domain Names - Concepts and Facilities
- RFC1035: Domain Names - Implementation and Specification
- For the functions that are not compliance with RFCs and the restrictions, see the above notes.

FTP (PI_FTP)

Function

The FTP (PI_FTP) record stores information about FTP service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_FTP_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 340 bytes

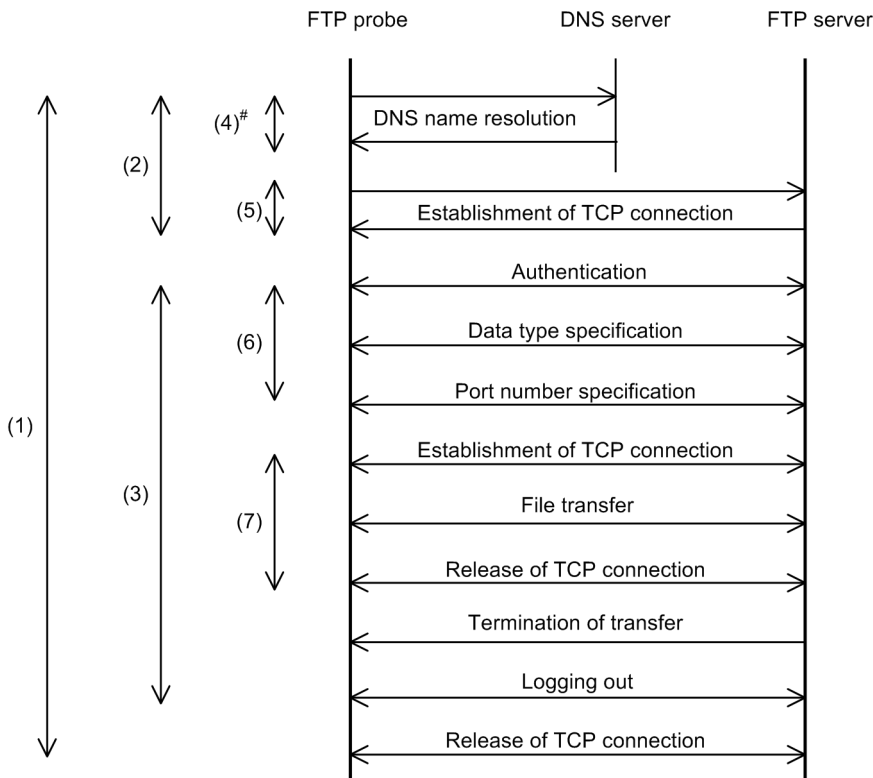
Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds) ((7) in Figure 10-3)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	DNS time (seconds) ((4) in Figure 10-3)	AVG	double	No	Probe Daemon
FTP Time (FTP_TIME)	FTP time (seconds) ((3) in Figure 10-3)	AVG	double	No	Probe Daemon
Preprocessing Time (PRE_PROCESS_TIME)	Preprocessing time (seconds) ((6) in Figure 10-3)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds) ((2) in Figure 10-3)	AVG	double	No	Probe Daemon
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds) ((5) in Figure 10-3)	AVG	double	No	Probe Daemon
Throughput (THROUGHPUT)	Throughput (bits/second). This is determined by the size of the file to be transferred and the data transfer time.	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the FTP probe and the measurement-target server via the TCP connection (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-3)	AVG	double	No	Probe Daemon
Transfer File Size (TRANS_FILE_SIZE)	Size of the transferred file	AVG	double	No	Probe Daemon

The following figure shows the FTP sequence.

Figure 10–3: FTP sequence



If an IP address is specified for the FTP server host name in the measurement condition, name resolution is not performed by DNS.

FTP operating environment and notes

A FTP probe acquires a measurement file from the measurement-target FTP server, or transfers a prepared measurement file to the measurement-target server and measures the time required for file transfer. The measurement file must already be stored in the following folder:

- Transfer to the FTP server
installation-folder\agtv\probedata\ftp
- Transfer from the FTP server
Under the user's home directory specified in the measurement condition

The following describes and provides notes on a FTP operating environment.

Handling of the transferred file

Handling of the transferred file depends on the transfer direction, as described below:

UPLOAD

If the file to be transferred has the same name as a file in the home directory of a user at the target FTP server, the file is overwritten. Therefore, the total size of the data in the target measurement file does not keep increasing.

DOWNLOAD

Data in the acquired file is discarded each time measurement is completed.

Data type during transfer

The FTP probe supports only the ASCII data type during transfer.

RFC compliance

- RFC959: File Transfer Protocol (FTP)

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

HTTP (PI_HTP)

Function

The HTTP (PI_HTP) record stores information about HTTP service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_HTP_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 360 bytes

Fields

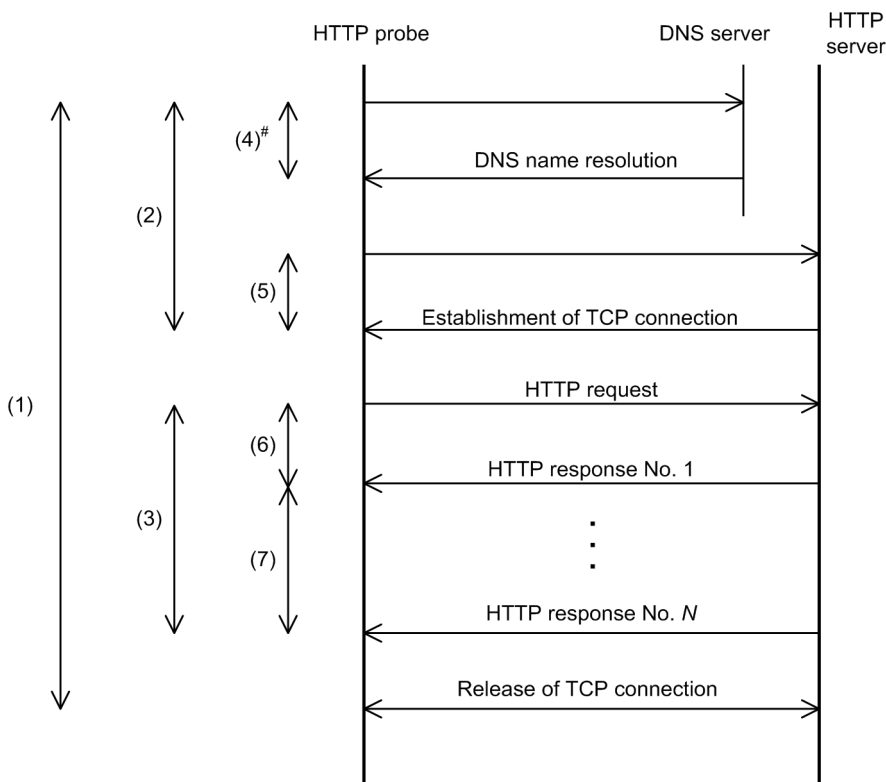
View name (Manager name)	Description	Summary rule	Format	Delta	Data source
DNS Time (DNS_TIME)	DNS time (seconds) ((4) in Figure 10-4)	AVG	double	No	Probe Daemon
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds) ((7) in Figure 10-4)	AVG	double	No	Probe Daemon
HTTP Time (HTTP_TIME)	HTTP time (seconds) ((3) in Figure 10-4)	AVG	double	No	Probe Daemon
Request Count (REQ_COUNT)	Number of requests issued (count)	AVG	double	No	Probe Daemon
Server Processing Time (SERV_PROCESS_TIME)	Server processing time (seconds) ((6) in Figure 10-4)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds) ((2) in Figure 10-4)	AVG	double	No	Probe Daemon
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds) ((5) in Figure 10-4)	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Throughput (THROUGHPUT)	Resource transfer throughput (bits/second). This is determined by the total size of resources and the data transfer time.	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the HTTP probe and the measurement-target server via the TCP connection (bytes)	AVG	double	No	Probe Daemon
Total Resource Size (TOTAL_RES_SIZE)	Total size of resources acquired (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-4)	AVG	double	No	Probe Daemon

Note:
If the page to be measured contains embedded images and frames, and if the depth of measurement condition is 2 or greater, measurement is executed more than once. In such a case, the value of each item, except the throughput, is the sum of the results obtained by the multiple measurements.

The following figure shows the HTTP sequence.

Figure 10–4: HTTP sequence



If an IP address is specified for the HTTP server host name in the measurement condition, name resolution is not performed by DNS.

HTTP operating environment and notes

A HTTP probe issues a HTTP request to the specified URL, uses the GET method to acquire the page or the POST method to register data, and measures the response time.

The following describes and provides notes on a HTTP operating environment.

Web authentication

The Basic Authentication method is used.

Cookie

PFM - Agent for Service Response accepts cookies based on Netscape Communication's specifications. The information sent as a cookie from the HTTP server is stored in the Cookie file that is created for each measurement condition. The Cookie files remain undeleted even after measurement is completed. If measurement cannot be performed correctly due to a change made to the contents of a measurement condition, delete the Cookie file for that measurement condition, which can be identified by the measurement condition ID. The following is the naming convention for Cookie files:

```
cookies_<measurement-condition-ID>
```

Cookie files are stored in the following folder:

```
installation-folder\agtv\probe\probedata\http
```

Program execution

Plug-ins, JavaScripts, and applets are downloaded but not executed.

Depth

For example, specifying a depth of 2 acquires the pages displayed in the resources and frames that are embedded in the page at the specified URL. No linked pages are acquired. PFM - Agent for Service Response repeats the acquisition of resources and frames embedded in the acquired page or frame as many times as the specified value.

For the embedded resources and frames, PFM - Agent for Service Response analyzes the acquired HTML, and acquires the resources and frames that are specified by the value of the tag and attribute shown in the table below.

Table 10–14: Embedded resources and frames to be acquired

Tag name	Attribute name
applet	code
frame	src
iframe	src
img	src
script	src

Note that PFM - Agent for Service Response cannot acquire resources or frames from HTML files that are returned after being compressed or transformed by commands such as `gzip` or `compress`. Moreover, PFM - Agent for Service Response cannot acquire resources or frames from HTML files that have any attributes other than those listed in the above table. Such attributes include the `archive` attribute of the `<applet>` tag, which specifies a compressed file as the value of an attribute name.

Use of proxy

If acquiring the Web page specified by the URL and the embedded resources and frames involves use of a proxy for only part of the acquisition target, measurement cannot be performed.

HTTP Version

HTTP/1.0 is applicable.

RFC compliance

- RFC1866: Hypertext Markup Language - 2.0
- RFC2616: Hypertext Transfer Protocol - HTTP/1.1
- RFC2396: Uniform Resource Identifiers (URI): Generic Syntax

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

HTTPS(PI_HTTPS)

Function

The HTTPS (PI_HTTPS) record stores information about HTTPS service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_HTTPS_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 360 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds) ((7) in Figure 10-5)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	Data transfer time (seconds) ((4) in Figure 10-5)	AVG	double	No	Probe Daemon
HTTP Time (HTTP_TIME)	HTTP time (seconds) ((3) in Figure 10-5)	AVG	double	No	Probe Daemon
Request Count (REQ_COUNT)	Number of requests issued (count)	AVG	double	No	Probe Daemon
Server Processing Time (SERV_PROCESS_TIME)	Server processing time (seconds) ((6) in Figure 10-5)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds) ((2) in Figure 10-5)	AVG	double	No	Probe Daemon
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds), including the time required for establishing an SSL connection ((5) in Figure 10-5)	AVG	double	No	Probe Daemon

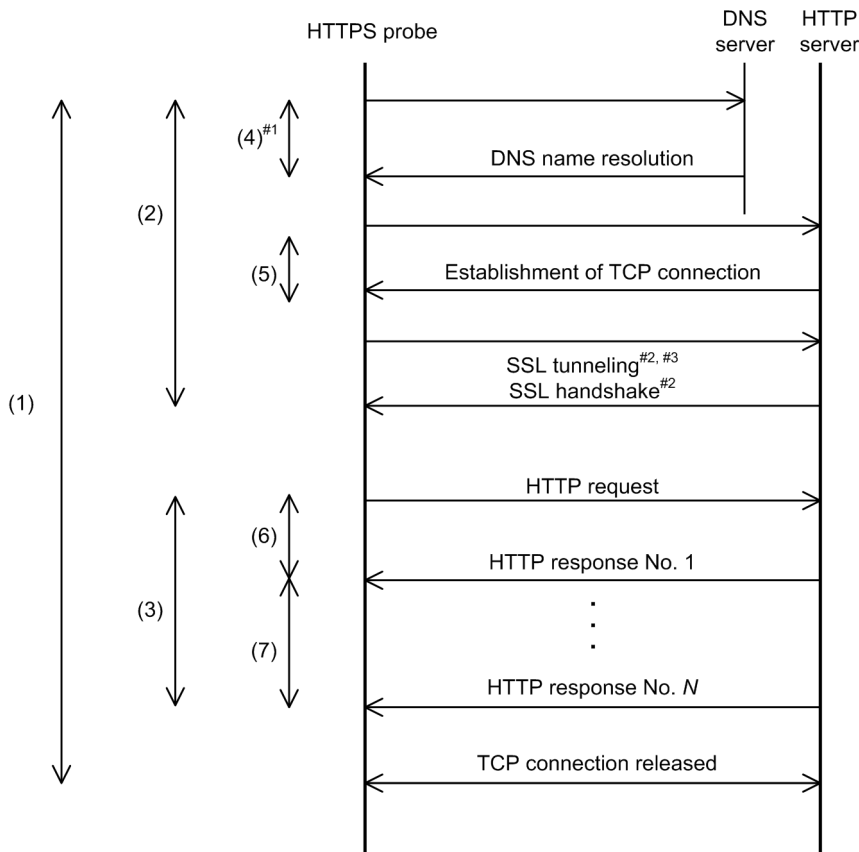
View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Throughput (THROUGHPUT)	Resource transfer throughput (bits/second). This is determined by the total size of resources and the data transfer time.	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	The total amount of data transferred between the HTTPS probe and the measurement-target server via the TCP connection (bytes). For the data transferred via an SSL-protected connection, the total amount of text data is calculated. The amount of data associated with server authentication for establishing an SSL connection and the amount of data associated with an SSL handshake are not included.	AVG	double	No	Probe Daemon
Total Resource Size (TOTAL_RES_SIZE)	Size of acquired resources (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-5)	AVG	double	No	Probe Daemon

Note:

If the page to be measured contains embedded images and frames, and if the depth of measurement condition is 2 or greater, measurement is executed more than once. In such a case, the value of each item, except the throughput, is the sum of the results obtained by the multiple measurements.

The following figure shows the HTTPS sequence.

Figure 10–5: HTTPS sequence



#1: If the measurement conditions specify an IP address for the HTTP server host name, name resolution is not performed by DNS.

#2: Not performed if HTTP embedded resources and frames are to be acquired.

#3: Performed when the proxy server is used.

HTTPS operating environment and notes

An HTTPS probe establishes an SSL-protected connection with the server that provides the target service. Then the HTTPS probe issues an HTTP request to the URL specified on the connection, uses the GET method to acquire the page or the POST method to register data, and measures the response time. Note that when the SSL connection is established, server authentication is performed to confirm that the connection target is a reliable HTTP server.

The following describes, and provides notes on, an HTTPS operating environment.

Web authentication

The Basic Authentication method is used.

Cookie

PFM - Agent for Service Response accepts cookies based on Netscape Communication's specifications. The information sent as a cookie from the HTTP server is stored in the Cookie file that is created for each measurement condition. The Cookie files remain undeleted even after measurement is completed. If measurement cannot be performed correctly due to a change made to the contents of a measurement condition, delete the Cookie file for that measurement condition, which can be identified by the measurement condition ID. The following is the naming convention for Cookie files:

`cookies_<measurement-condition-ID>`

Cookie files are stored in the following folder:

```
installation-folder\agtv\probe\probedata\http
```

Program execution

Plug-ins, JavaScripts, and applets are downloaded but not executed.

Depth

For example, specifying a depth of 2 acquires the pages displayed in the resources and frames that are embedded in the page at the specified URL. No linked pages are acquired. PFM - Agent for Service Response repeats the acquisition of resources and frames embedded in the acquired page or frame as many times as the specified value.

For the embedded resources and frames, PFM - Agent for Service Response analyzes the acquired HTML, and acquires the resources and frames that are specified by the value of the tag and attribute shown in the table below.

Table 10–15: Embedded resources and frames to be acquired

Tag name	Attribute name
applet	code
frame	src
iframe	src
img	src
script	src

Note that PFM - Agent for Service Response cannot acquire resources or frames from HTML files that are returned after being compressed or transformed by commands such as `gzip` or `compress`. Moreover, PFM - Agent for Service Response cannot acquire resources or frames from HTML files that have any attributes other than those listed in the above table. Such attributes include the `archive` attribute of the `<applet>` tag, which specifies a compressed file as the value of an attribute name.

Use of proxy

If acquiring the Web page specified by the URL and the embedded resources and frames involves use of a proxy for only part of the acquisition target, measurement cannot be performed.

Cipher strength

The table below shows the encryption types supported by the HTTPS probe. You cannot access a page protected with unsupported cipher strength.

Table 10–16: Supported encryption types

Cryptographic algorithm	Key length
AES	256,128
AESGCM	256,128
Camellia	256,128
DES	56
IEDA	128
RC4	128
3DES	168

Hash algorithm that can be used for certificates

SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and MD5 are supported as hash algorithms for certificate signatures and message digests. Use certificates that have been created by using one of the supported hash algorithms.

Server authentication

For server authentication, PFM - Agent for Service Response verifies the validity period of a server certificate sent from the HTTP server and confirms that the server certificate was issued from an authorized Certificate Authority. To verify the server certificate, the root certificate of either the Certificate Authority that issued the server certificate or its higher-level Certificate Authority is required. Because the root certificate has a validity period, you need to re-install the root certificate before it expires. If there is no root certificate or if the server certificate has expired, server authentication fails.

To install a root certificate, use the following procedure:

Acquire a root certificate:

Export a PEM root certificate from a Web browser. The following shows an example using Internet Explorer 8.

1. Select **Tools, Internet Options**, and then click the **Contents** tab.
2. Click the **Certificate** button. Then, in the dialog box that opens, click the **Trusted Root Certification Authorities** tab.
3. In the list, select the root certificate of the Certificate Authority that issued the server certificate.
To check the Certificate Authority that issued the server certificate, open the monitoring target Web page in Internet Explorer, and then click the key icon on the status bar. Then look at the information on the **Details** page.
4. Click the **Export** button to start the certificate export wizard.
Specify the settings as instructed by the export wizard.
For the format of the exported file, select **Base64 encoded X.509(.CER)**.
For the file name, enter `c:\cacert.cer`. The extension `.cer` is automatically added.

Install the root certificate:

Change the extension of the exported root certificate (`cacert.cer`) to `.pem`, and then copy the file to *installation-folder\agtv\probe\cert*.

Note that the `cacert.pem` file can contain multiple root certificates. To add a root certificate to the existing `cacert.pem` file, use a text editor to copy the contents of the exported root certificate (from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----`) to the `cacert.pem` file.

Client certificate

PFM - Agent for Service Response sends a client certificate to the HTTP server. The HTTP server then verifies the validity period and confirms that the client certificate was issued from an authorized Certificate Authority. The client certificate and the private key can be obtained in either of the following ways.

- Obtained from a certification authority
- Exported from the Internet Explorer used for accessing the monitoring-target Web site

The file containing the client certificate and private key must be stored under *installation-folder\agtv\probe\cert*. The file must be in Base64 encoded X.509 format. If the provided client certificate file is not in Base64 encoded X.509 format, use any tool to convert it to X.509 format.

The following shows how to export a client certificate and its private key by using Internet Explorer 8. Note that the client certificate to be exported must have been specified to allow export of the private key when they were imported to Internet Explorer.

1. Start Internet Explorer, and select **Tools**, and then **Internet Options**.
The Internet Options dialog box opens.
2. Select the **Contents** tab, and then click the **Certificates** button.
The Certificates dialog box opens.
3. Select the **Personal** tab.
The **Personal** page is displayed.
4. Select the client certificate to be exported, and then click **Export**.
The certificate export wizard starts. Export the certificate as instructed by the wizard.
For **Export Private Key**, select **Yes, export the private key**.
For the export file format, select **Personal Information Exchange-PKCS#12(PFX)**.
Clear the **Enable strong protection** check box.
Enter any values for the password and file name.
5. Convert the certificate format from PKCS#12 to Base64-encoded X.509.
You can use any tool for conversion.
6. Store the exported file under *installation-folder\agtv\probe\cert*.

RFC compliance

- RFC1866: Hypertext Markup Language - 2.0
- RFC2616: Hypertext Transfer Protocol - HTTP/1.1
- RFC2396: Uniform Resource Identifiers (URI): Generic Syntax
- RFC2818 HTTP over TLS

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

IE Scenario(PI_IES)

Function

The IE Scenario (PI_IES) record stores information about the replay time for each scopes in an IE Scenario. This is a multi-instance record. Each scope becomes an instance.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_MSR_COND_ID, PI_IES_SCOPE_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 312 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Scope ID (SCOPE_ID)	Scope number. The value 0 to 16 is set. For the overall IE scenario, 0 is set.	COPY	long	No	IE Probe Daemon
Scope Name (SCOPE_NAME)	Scope name. For the overall IE scenario, ALL is set. You can specify any name as a scope name.	COPY	string (up to 127 bytes)	No	IE Probe Daemon
Total Busy Time (TOTAL_BUSY_TIME)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Replay Time (TOTAL_RPLY_TIME)	Total replay time (seconds)	AVG	double	No	IE Probe Daemon

IE Scenario Overview(PI_IESO)

Function

The IE Scenario Overview (PI_IESO) record stores summary information about the replay times for each scopes in an IE scenario. This is a multi-instance record. Each IE scenario becomes an instance.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_IESO_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 820 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Busy Time (TOTAL_BUSY_TIME)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 1 (TOTAL_BUSY_TIME_1)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 2 (TOTAL_BUSY_TIME_2)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 3 (TOTAL_BUSY_TIME_3)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 4 (TOTAL_BUSY_TIME_4)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 5 (TOTAL_BUSY_TIME_5)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 6 (TOTAL_BUSY_TIME_6)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Busy Time 7 (TOTAL_BUSY_TIME_7)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 8 (TOTAL_BUSY_TIME_8)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 9 (TOTAL_BUSY_TIME_9)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 10 (TOTAL_BUSY_TIME_10)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 11 (TOTAL_BUSY_TIME_11)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 12 (TOTAL_BUSY_TIME_12)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 13 (TOTAL_BUSY_TIME_13)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 14 (TOTAL_BUSY_TIME_14)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 15 (TOTAL_BUSY_TIME_15)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Busy Time 16 (TOTAL_BUSY_TIME_16)	This field is reserved and cannot be used.	AVG	double	No	IE Probe Daemon
Total Replay Time (TOTAL_RPLY_TIME)	Total replay time (entire IE Scenario) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 1 (TOTAL_RPLY_TIME_1)	Total replay time (scope 1) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 2 (TOTAL_RPLY_TIME_2)	Total replay time (scope 2) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 3 (TOTAL_RPLY_TIME_3)	Total replay time (scope 3) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 4 (TOTAL_RPLY_TIME_4)	Total replay time (scope 4) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 5 (TOTAL_RPLY_TIME_5)	Total replay time (scope 5) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 6 (TOTAL_RPLY_TIME_6)	Total replay time (scope 6) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 7 (TOTAL_RPLY_TIME_7)	Total replay time (scope 7) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 8 (TOTAL_RPLY_TIME_8)	Total replay time (scope 8) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 9 (TOTAL_RPLY_TIME_9)	Total replay time (scope 9) (seconds)	AVG	double	No	IE Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Replay Time 10 (TOTAL_RPLY_TIME_10)	Total replay time (scope 10) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 11 (TOTAL_RPLY_TIME_11)	Total replay time (scope 11) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 12 (TOTAL_RPLY_TIME_12)	Total replay time (scope 12) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 13 (TOTAL_RPLY_TIME_13)	Total replay time (scope 13) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 14 (TOTAL_RPLY_TIME_14)	Total replay time (scope 14) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 15 (TOTAL_RPLY_TIME_15)	Total replay time (scope 15) (seconds)	AVG	double	No	IE Probe Daemon
Total Replay Time 16 (TOTAL_RPLY_TIME_16)	Total replay time (scope 16) (seconds)	AVG	double	No	IE Probe Daemon

IMAP4 (PI_IMP4)

Function

The IMAP4 (PI_IMP4) record stores information about IMAP4 service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_IMP4_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 380 bytes

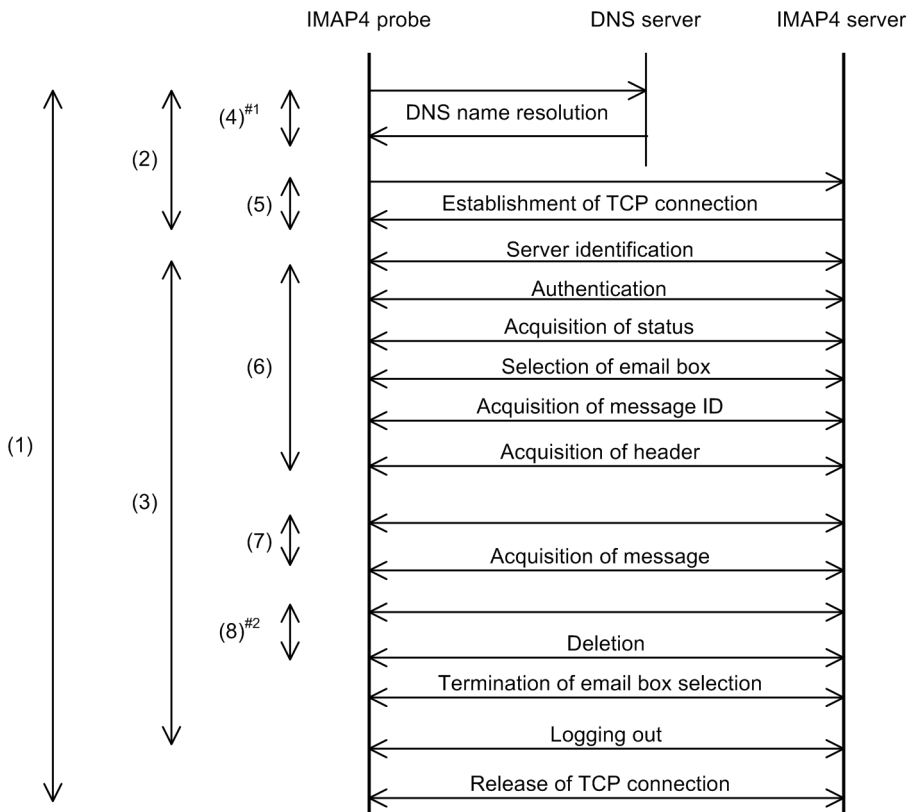
Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds) ((7) in Figure 10-6)	AVG	double	No	Probe Daemon
Deletion Time (DELETION_TIME)	Deletion time (seconds) ((8) in Figure 10-6)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	DNS time (seconds) ((4) in Figure 10-6)	AVG	double	No	Probe Daemon
Download Count (DOWNLOAD_COUNT)	Number of acquired emails	AVG	double	No	Probe Daemon
IMAP Time (IMAP4_TIME)	IMAP4 time (seconds) ((3) in Figure 10-6)	AVG	double	No	Probe Daemon
Preprocessing Time (PRE_PROCESS_TIME)	Preprocessing time (seconds) ((6) in Figure 10-6)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds) ((2) in Figure 10-6)	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds) ((5) in Figure 10-6)	AVG	double	No	Probe Daemon
Throughput (THROUGHPUT)	Throughput for email acquisition (bits/second). This is determined by the total size of emails and the data transfer time.	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the IMAP4 probe and the measurement-target server via the TCP connection (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-6)	AVG	double	No	Probe Daemon
Total Size of Email (TOTAL_EMAIL_SIZE)	Total size of acquired email (bytes)	AVG	double	No	Probe Daemon

The following figure shows the IMAP4 sequence.

Figure 10–6: IMAP4 sequence



^{#1} If an IP address is specified for the IMAP4 server host name in the measurement condition, name resolution is not performed by DNS.

^{#2} If emails are not deleted from the IMAP4 server, there will be no deletion time.

IMAP4 operating environment and notes

An IMAP4 probe measures the time required for completing reception of emails addressed to a specified user.

The following describes and provides notes on an IMAP4 operating environment.

Email size

The total size of an email for the IMAP4 probe is the received header plus the message text. There is no limitation to the size of an email that can be acquired.

Deleting emails

The IMAP4 probe acquires the newly arrived emails in an inbox. Executing deletion deletes all the emails in that inbox. This means that at the next measurement, the number of emails to be measured would be zero. Therefore, send emails for measurement again before the next measurement occurs.

Deletion method

The two email deletion methods for IMAP4 are logical deletion and physical deletion. An IMAP4 probe uses the physical email deletion method, so that emails are not accumulated when the IMAP4 probe receives emails that are sent periodically by a program such as a SMTP probe.

RFC compliance

- RFC1733: Distributed Electronic Mail Models in IMAP4
- RFC2060: Internet Message Access Protocol (IMAP) - Version 4 Rev 1
- RFC2683: IMAP4 Implementation Recommendations
- RFC2822: Internet Message Format

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

Logged Message for IE Scenario(PL_IESM)

Function

The Logged Message for IE Scenario (PL_IESM) record stores information about the messages output in Event Log and the log files. Record are created for each message output in the log files. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_IESM_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 664 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
IE Scenario Result Code (IESCENA_RESULT_CODE)	IE scenario result code	--	string (up to 7 bytes)	No	IE Probe Daemon
IE Scenario Result Detail (IESCENA_RESULT_DETAIL)	Detail text of IE scenario result. This field shows blank.	--	string (up to 255 bytes)	No	IE Probe Daemon
IE Scenario Result Message (IESCENA_RESULT_MESS)	Replay result message text of IE scenario result.	--	string (up to 255 bytes)	No	IE Probe Daemon
Measurement Condition ID (MSR_COND_ID)	Measurement condition ID	--	long	No	IE Probe Daemon
Measurement Condition Name (MSR_COND_NAME)	A label corresponding to the measurement condition. Stores the first matched label by searching within the following labels in this order:	--	string (up to 63 bytes)	No	IE Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Measurement Condition Name (MSR_COND_NAME)	<p>1. The labels defined in the measurement condition registration file.</p> <p>2. The labels defined in the measurement condition label definition file.</p> <p>If the label of the measurement condition is not defined in the both file, <i>service-type-name_measurement-condition-ID</i> is stored.</p>	--	string (up to 63 bytes)	No	IE Probe Daemon
Measurement Start Time (MSR_START_TIME)	Measurement start time	--	time_t	No	IE Probe Daemon
Sequence Number (SEQ_NUM)	Number of the replaying operation while outputting the messages. If the message is not related to the operations, 0 is set.	--	long	No	IE Probe Daemon

Examples of output contents

IE Scenario Result Code	IE Scenario Result Message
89101	The response determination condition was not satisfied. (OpNum=10)
89102	A page transition error occurred during playback. (OpNum=10, CODE=404, URL= http://host:20358/PFMWebConsole/login.do)
89103	The target frame page is not found. (OpNum=10, URL= http://host:20358/PFMWebConsole/login.do)
89109	The error occurred during playback(OpNum=10).
89110	The time-out was generated during playback(OpNum=10).
89504	A pop-up dialog box not contained in the IE scenario appeared. (OpNum=10)

POP3 (PI_POP3)

Function

The POP3 (PI_POP3) record stores information about POP3 service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_POP3_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 380 bytes

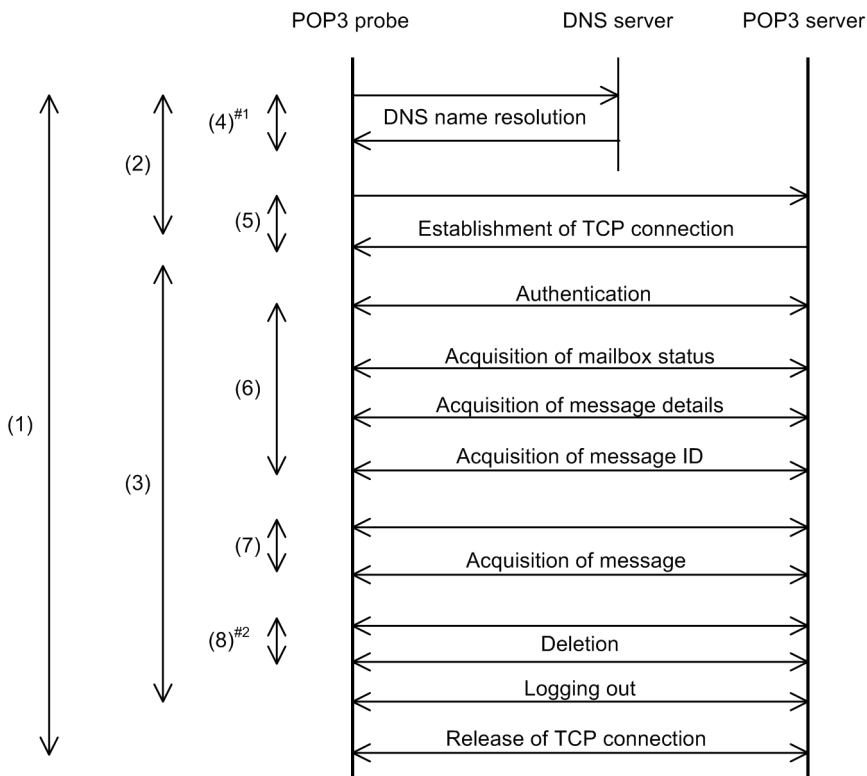
Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds) ((7) in Figure 10-7)	AVG	double	No	Probe Daemon
Deletion Time (DELETION_TIME)	Deletion time (seconds) ((8) in Figure 10-7)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	DNS time (seconds) ((4) in Figure 10-7)	AVG	double	No	Probe Daemon
Download Count (DOWNLOAD_COUNT)	Number of acquired emails	AVG	double	No	Probe Daemon
POP3 Time (POP3_TIME)	POP time (seconds) ((3) in Figure 10-7)	AVG	double	No	Probe Daemon
Preprocessing Time (PRE_PROCESS_TIME)	Preprocessing time (seconds) ((6) in Figure 10-7)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds) ((2) in Figure 10-7)	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds) ((5) in Figure 10-7)	AVG	double	No	Probe Daemon
Throughput (THROUGHPUT)	Throughput (bits/second). This is determined by the total size of emails and the data transfer time.	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the POP3 probe and the measurement-target server via the TCP connection (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-7)	AVG	double	No	Probe Daemon
Total Size of Email (TOTAL_EMAIL_SIZE)	Total size of acquired email (bytes)	AVG	double	No	Probe Daemon

The following figure shows the POP3 sequence.

Figure 10–7: POP3 sequence



^{#1} If an IP address is specified for the POP3 server host name in the measurement condition, name resolution is not performed by DNS.

^{#2} If emails are not deleted from the POP3 server, there will be no deletion time.

POP3 operating environment and notes

A POP3 probe measures the time required for completing reception of email addressed to a specified user.

The following describes and provides notes on a POP3 operating environment.

Email size

The total size of an email for the POP3 probe is the received header plus the message text. There is no limitation to the size of an email that can be acquired.

Deleting emails

Executing deletion deletes all the emails. This means that at the next measurement, the number of emails to be measured would be zero. Therefore, send emails for measurement again before the next measurement occurs.

RFC compliance

- RFC1939: Post Office Protocol - Version 3
- RFC2822: Internet Message Format

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

Service Summary Interval (PI_PI)

Function

The Service Summary Interval (PI_PI) record stores information about the response time of each service. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	Yes	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 160 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds)	AVG	double	No	Probe Daemon

SMTP (PI_SMTP)

Function

The SMTP (PI_SMTP) record stores information about SMTP service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_SMTP_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 320 bytes

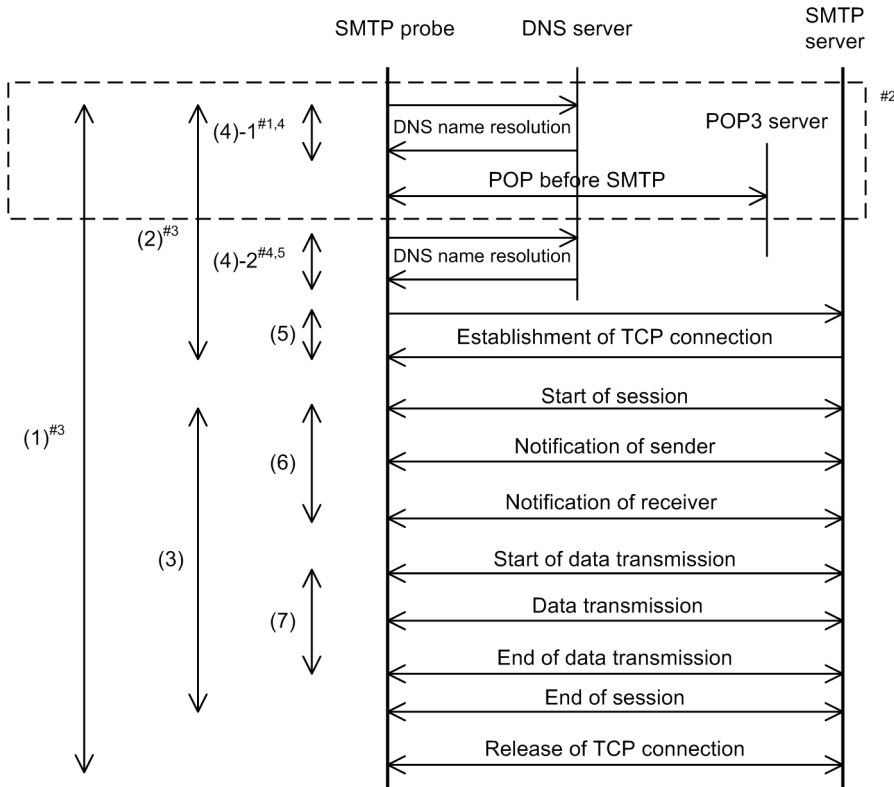
Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds) ((7) in Figure 10-8)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	DNS time (seconds) ((4) in Figure 10-8)	AVG	double	No	Probe Daemon
Preprocessing Time (PRE_PROCESS_TIME)	Preprocessing time (seconds) ((6) in Figure 10-8)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds) ((2) in Figure 10-8)	AVG	double	No	Probe Daemon
SMTP Time (SMTP_TIME)	SMTP time (seconds) ((3) in Figure 10-8)	AVG	double	No	Probe Daemon
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds) ((5) in Figure 10-8)	AVG	double	No	Probe Daemon
Throughput (THROUGHPUT)	Throughput (bits/second). This is determined by the size of sent email and the data transfer time.	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data transferred between the SMTP probe and the measurement-target server via the TCP connection (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-8)	AVG	double	No	Probe Daemon

The following figure shows the SMTP sequence.

Figure 10–8: SMTP sequence



#1 If an IP address is specified for the POP3 server host name in the measurement condition, name resolution is not performed by DNS.

#2 Processing during execution of POP before SMTP

#3 If POP3 authentication is not performed, the total response time ((1)) and the setup time ((2)) do not include the POP3 server's DNS name resolution time and the POP before SMTP time.

#4 If POP3 authentication is not performed, the DNS time (sum of (4)-1 and (4)-2) does not include the POP3 server's DNS name resolution time.

#5 If an IP address is specified for the SMTP server host name in the measurement condition, name resolution is not performed by DNS ((4)-2).

SMTP operating environment and notes

A SMTP probe creates a message text of a specified size and measures the time required for completing message transmission to the destination address.

The following describes and provides notes on a SMTP operating environment.

Subject

The subject in the measurement email header is "Test mail from PFM - Agent for Service Response."

Text

The text for measurement emails is a character string consisting of the character o.

Attached file

The SMTP probe sends only the header and text; it does not attach any file to measurement emails.

Handling of the transmitted measurement emails

After sending measurement emails to the target server, the SMTP probe does not delete the emails. If the measurement covers a long period of time, a large number of measurement emails will accumulate, and a shortage of disk space may occur at the target mail server. To avoid this, you should use one of the following methods to delete emails periodically from the target mail server:

- Deleting emails by registering a measurement condition
Register a POP3 or IMAP4 measurement condition with the email deletion option enabled, and then perform that measurement to delete emails.
- Having the user delete emails
Have the user periodically delete the measurement emails that were sent by the SMTP probe.

RFC compliance

- RFC1939: Post Office Protocol - Version 3
- RFC2821: Simple Mail Transfer Protocol
- RFC2822: Internet Message Format

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

TCP (PI_TCP)

Function

The TCP (PI_TCP) record stores information about TCP service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_TCP_MSR_COND_ID

Lifetime

None

Record size

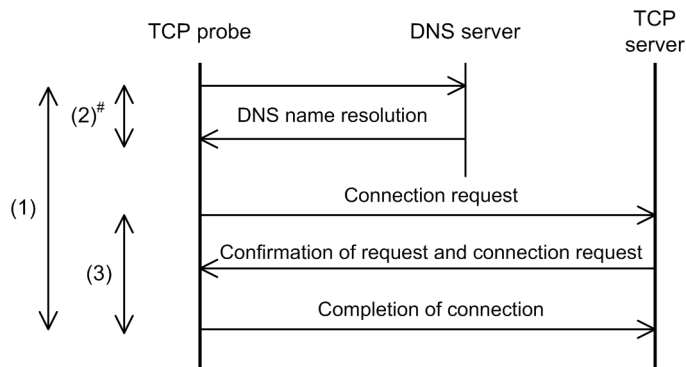
- Fixed part: 681 bytes
- Variable part: 200 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
DNS Time (DNS_TIME)	DNS time (seconds) ((2) in Figure 10-9)	AVG	double	No	Probe Daemon
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds) ((3) in Figure 10-9)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds) ((1) in Figure 10-9)	AVG	double	No	Probe Daemon

The following figure shows the TCP sequence.

Figure 10–9: TCP sequence



If an IP address is specified for the TCP server host name in the measurement condition, name resolution is not performed by DNS.

TCP operating environment and notes

A TCP probe measures the time required for establishing connection with the server that provides the TCP service.

The following describes and provides notes on a TCP operating environment.

RFC compliance

- RFC793: Transmission Control Protocol

User Defined Service (PI_UDEF)

Function

The User Defined Service (PI_UDEF) record stores information about a user-defined service response time. This is a multi-instance record.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_UDEF_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 160 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds)	AVG	double	No	Probe Daemon

Web Transaction (PI_WT)

Function

The Web Transaction (PI_WT) record stores information about a Web transaction service response time. This is a multi-instance record. Each scope becomes an instance.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_WT_MSR_COND_ID, PI_WT_SCOPE_NAME

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 392 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (seconds)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	DNS time (seconds)	AVG	double	No	Probe Daemon
HTTP Time (HTTP_TIME)	HTTP time (seconds)	AVG	double	No	Probe Daemon
Request Count (REQ_COUNT)	Number of requests (count)	AVG	double	No	Probe Daemon
Scope Name (SCOPE_NAME)	Scope name. For the overall transaction, ALL is set. For a scope name, scope N is set (N: 1 to 8).	COPY	string (up to 31 bytes)	No	Probe Daemon
Server Processing Time (SERV_PROCESS_TIME)	Server processing time (seconds)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (seconds)	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
TCP Connection Time (TCP_CON_TIME)	TCP connection time (seconds)	AVG	double	No	Probe Daemon
Throughput (THROUGHPUT)	Throughput (bits/second)	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data (bytes)	AVG	double	No	Probe Daemon
Total Resource Size (TOTAL_RES_SIZE)	Total size of resource (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (seconds)	AVG	double	No	Probe Daemon

Web transaction operating environment and notes

A Web transaction probe performs not only a measurement consisting of a single set of a request and a response but also a measurement in which a series of HTTP(S) requests and responses constitute a single Web transaction.

A Web transaction's measurement result covers the playback of the entire Web transaction. A measurement result is also output for each specified scope (any page transactions) in the same manner.

The Web transaction probe plays back the information defined in the Web transaction file according to the measurement condition. A specified URL's response is checked according to the response determination information defined in the Web transaction file. Any measurement that does not meet the condition results in a measurement failure. The checking based on the response determination information is applicable only when the response acquired from the specified URL is in HTML format (`Content-Type` is `text/html`). If the received data is compressed, the response check results in a measurement failure. This checking is not performed for acquisition of embedded resources.

The following describes and provides notes on a Web transaction operating environment.

- Acquisition is made for each HTML frame.
- Programs, such as plug-ins and Java Scripts, are downloaded but not executed.
- With respect to acquisition of embedded resources, if the Web transaction is defined to acquire embedded resources, they are acquired automatically during measurement. The Web transaction analyzes the HTML acquired during measurement (only when the received data is not compressed), and acquires the resources specified in the values of the tags and attributes listed in the table below.
- Note that the tag and attribute names are not case sensitive.

Table 10–17: Embedded resources and frames to be acquired

Tag name	Attribute name
applet	code
body	background
embed	src
img	src
object	data
script	src

- Note that PFM - Agent for Service Response cannot acquire resources or frames from HTML files that are returned after being compressed or transformed by commands such as `gzip` or `compress`. Moreover, PFM - Agent for Service Response cannot acquire resources or frames from HTML files that have any attributes other than those listed in the above table. Such attributes include the `archive` attribute of the `<applet>` tag, which specifies a compressed file as the value of an attribute name.
- A Web transaction does not acquire a resource embedded in a page that is created dynamically by a program such as JavaScript.
- For a cookie that is generated (received) during measurement, the Web transaction performs measurement accordingly. Therefore, unless this is necessary for other reasons, there is no need to specify cookies in the Web transaction file. Cookies that are specified in the Web transaction file are sent together with the cookies generated (received) during measurement.
- For the user agent specified when a HTTP(S) request is issued, PFM - Agent for Service Response (Windows) is used by default.
- If a Web transaction that uses the same user name for login is defined in multiple measurement conditions, and multiple logins by the same user name are not permitted, measurement may fail. Therefore, if multiple logins by the same user name are not permitted, you must take appropriate action, such as providing a different user for measurement of each measurement condition.
- You can define a Web transaction with the same contents in multiple measurement conditions.
- For Web authentication, the Basic Authentication method is used.
- A Web transaction accepts cookies based on Netscape Communication's specifications.
- If acquisition of a Web page specified by a URL and embedded resources involves use of a proxy for only part of the acquisition target, measurement cannot be performed.
- When HTTPS is measured in a Web transaction, the supported encryption types are the same as those for the HTTPS probe. You cannot access a page protected with unsupported cipher strength. For details, see [HTTPS](#).
- To apply server authentication and client authentication, a certificate file must be registered in the same way as for the HTTPS probe. For details, see [HTTPS](#).

HTTP Version

HTTP/1.0 is applicable.

Referer Header

The Web transaction probe does not issue the requests with the Referer Header.

RFC compliance

- RFC1866: Hypertext Markup Language - 2.0
- RFC2616: Hypertext Transfer Protocol - HTTP/1.1
- RFC2396: Uniform Resource Identifiers (URI): Generic Syntax
- RFC2818: HTTP over TLS

For the functions that are not compliance with RFCs and the restrictions, see the above notes.

HTTP(S) processing sequence

For details about a sequence of HTTP(S) communication processing performed in a Web transaction, see [HTTP \(PI_HTP\)](#) and [HTTPS \(PI_HTTPS\)](#) in this chapter.

Web Transaction Overview (PI_WTO)

Function

The Web Transaction Overview (PI_WTO) record stores summary information about the response times for the scopes in a Web transaction. This is a multi-instance record. Each transaction becomes an instance.

Default and changeable values

Item	Default value	Changeable
Collection Interval	360	Y
Collection Offset	0	Y
Log	No	Y
LOGIF	(Blank)	Y
Over 10 Sec Collection Time	No	N

ODBC key fields

PI_WTO_MSR_COND_ID

Lifetime

None

Record size

- Fixed part: 681 bytes
- Variable part: 520 bytes

Fields

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Data Transfer Time (DATA_TRANS_TIME)	Data transfer time (entire transaction) (seconds)	AVG	double	No	Probe Daemon
DNS Time (DNS_TIME)	DNS time (entire transaction) (seconds)	AVG	double	No	Probe Daemon
HTTP Time (HTTP_TIME)	HTTP time (entire transaction) (seconds)	AVG	double	No	Probe Daemon
Request Count (REQ_COUNT)	Number of requests (entire transaction) (count)	AVG	double	No	Probe Daemon
Server Processing Time (SERV_PROCESS_TIME)	Server processing time (entire transaction) (seconds)	AVG	double	No	Probe Daemon
Setup Time (SETUP_TIME)	Setup time (entire transaction) (seconds)	AVG	double	No	Probe Daemon
TCP Connection Time (TCP_CON_TIME)	TCP connection time (entire transaction) (seconds)	AVG	double	No	Probe Daemon

View name (Manager name)	Description	Summary rule	Format	Delta	Data source
Throughput (THROUGHPUT)	Throughput (entire transaction) (bits/second)	AVG	double	No	Probe Daemon
Total Amount of Data (TOTAL_DATA_SIZE)	Total amount of data (entire transaction) (bytes)	AVG	double	No	Probe Daemon
Total Resource Size (TOTAL_RES_SIZE)	Total size of resources (entire transaction) (bytes)	AVG	double	No	Probe Daemon
Total Response Time (TOTAL_RESP_TIME)	Total response time (entire transaction) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 1 (TOTAL_RESP_TIME_1)	Total response time (scope 1) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 2 (TOTAL_RESP_TIME_2)	Total response time (scope 2) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 3 (TOTAL_RESP_TIME_3)	Total response time (scope 3) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 4 (TOTAL_RESP_TIME_4)	Total response time (scope 4) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 5 (TOTAL_RESP_TIME_5)	Total response time (scope 5) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 6 (TOTAL_RESP_TIME_6)	Total response time (scope 6) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 7 (TOTAL_RESP_TIME_7)	Total response time (scope 7) (seconds)	AVG	double	No	Probe Daemon
Total Response Time 8 (TOTAL_RESP_TIME_8)	Total response time (scope 8) (seconds)	AVG	double	No	Probe Daemon

11

Commands

This chapter describes the commands supported by PFM - Agent for Service Response.

List of commands

The table below lists the commands supported by PFM - Agent for Service Response.

Table 11–1: Commands supported by PFM - Agent for Service Response

Function	Command name
Registering, changing, and deleting passwords	<code>esppasswd</code>
Changing the settings for the integrated trace log	<code>hntr2util</code>
Pausing/resuming the measurement [#] of a task	<code>jpcvtaskctl</code>
Executing Web transaction measurement tests	<code>jpcvtest</code>

#

This measurement refers to measurements through the probe and IE probe, in which PFM - Agent for Service Response issues requests to monitored targets and receives responses.

Details of commands

This section describes the command storage folders and the order in which the commands are described.

Command storage folders

The command storage folders are as follows:

Command storage folder for PFM - Agent for Service Response

installation-folder\agtv\probe\bin

Command storage folder for integrated trace log

system-drive\Program Files\Hitachi\HNTRLib2\bin

Order of command descriptions

The commands and their syntax are explained in alphabetical order by command name.

esppasswd (registers, changes, and deletes passwords)

Format

```
esppasswd {{-a | -c | -d }-s password-identification-name -o authentication-target -u user-name  
| -l [ -f file-name ]}
```

Function

- Use this command for measuring Web transactions.
- This command adds, changes, and deletes passwords in the password file (i.e. the password utility).
- This command outputs a list of password keys (password identification name, authentication target, and user name) to the standard output or to a specified file.

Execution permission

Administrator permissions

Storage folder

installation-folder\agtv\probe\bin

Arguments

-a

Specifies that a password is to be added.

-c

Specifies that a password is to be changed.

-d

Specifies that a password is to be deleted.

-s *password-identification-name*

Specifies the identification name of the processing that requires the password.

-o *authentication-target*

Specifies the target that requires authentication.

-u *user-name*

Specifies the user requiring a password.

-l

Specifies that a list of keys is to be output.

-f *file-name*

Specifies the file to which the list of keys is to be output. If the **-l** option is specified but this option is omitted, the list of keys is output to the standard output only.

The following table lists the values to be specified for the password identification name, authentication target, and user name.

Table 11–2: Value to be specified in the arguments

Service	Password identification name (value to be specified)	Authentication target	User name
HTTP(S) Web authentication	HTTP-W	URL ^{#1}	User name ^{#2}
HTTP(S) Proxy authentication	HTTP-P	Proxy server host name ^{#2}	User name ^{#2}
HTTPS client authentication	HTTPS-C	Client certificate file name ^{#2,#3}	A user name is not needed, and is ignored if specified.
SMTP, POP3	POP3	POP3 server host name ^{#2}	User name ^{#2}
IMAP4	IMAP4	IMAP4 server host name ^{#2}	User name ^{#2}
FTP	FTP	FTP server host name ^{#2}	User name ^{#2}

#1

You must not include a protocol identifier (`http://` or `https://`) in the URL that you specify. Note also that the URL to be authenticated during the measurement of an HTTP(S) service must match the URL specified by the `<URL>` tag in the measurement condition registration file.

#2

Make sure that the value specified as an argument matches the value specified in `esptask.xml`.

#3

Specify a file name (without including its path) that is located in `installation-folder\agtv\probe\cert`.

Notes

- If the specified key already exists, the password cannot be added.
- If the specified key does not exist, the password cannot be changed, added, or deleted.
- Of the names that can be specified as the authentication target, the following names are not case sensitive:
 - Host name (including a host name included in the URL)

Return values

0	Normal termination
1	The same key was found when a password was to be added.
2	The specified key was not found when a password was to be changed or deleted.
Other value	Abnormal termination

Examples

- Add a Web authentication password for the Web authentication user name `hitachi` with the URL `www.hitachi.co.jp/index.html`

```
esppasswd -a -s HTTP-W -o www.hitachi.co.jp/index.html -u hitachi
```

- Change the POP3 password for the user name `hitachi` with the POP3 server name `pop3.hitachi.co.jp`

```
esppasswd -c -s POP3 -o pop3.hitachi.co.jp -u hitachi
```

- Delete the POP3 password for the user name `hitachi` with the POP3 server name `pop3.hitachi.co.jp`

```
esppasswd -d -s POP3 -o pop3.hitachi.co.jp -u hitachi
```

- Output a list of keys to the standard output

```
esppasswd -l
```

Example of output

```
No., Password identification name, Authentication target, User name
1, HTTP-W, www.hitachi.co.jp/index.html, esp
2, HTTP-P, proxy.hitachi.co.jp, esp
3, POP3, pop3.hitachi.co.jp, esp
4, IMAP4, imap4.hitachi.co.jp, esp
5, FTP, ftp.hitachi.co.jp, esp
6, FTP, 192.168.1.21, esp
```

- Output a list of keys to the file `pwdkey`

```
esppasswd -l -f pwdkey
```

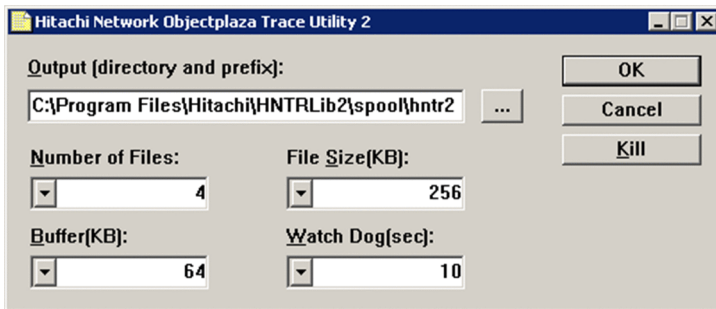
hntr2util (changes the integrated trace log settings)

Format

hntr2util

Function

The `hntr2util` command changes the size, number of files, and output destination of the integrated trace log that is output by the Hitachi Network Objectplaza Trace Library (HNTRLib2). The following dialog box appears when you execute this command, enabling you to change integrated trace log settings as necessary:



Settings

The following describes the items that can be set in this dialog box.

Output (directory and prefix):

Specifies the log file output destination and the prefix for the log file name. The default setting is as follows:

`system-drive\Program Files\Hitachi\HNTRLib2\spool\hntr2[n].log`

Number of Files:

Specifies the number of log files. As many files as are specified here are created at the output destination specified in **Output**. The default setting is 4.

File Size (KB):

Specifies the size of a log file. The default setting is 256 kilobytes.

Buffer (KB): and Watch Dog (sec):

Do not change these settings.

Kill button:

Terminates the active monitor processing. This button can terminate the integrated trace service (service name: Hitachi Network Objectplaza Trace Monitor 2); however, in normal circumstances we recommend that you do not use this button. Instead, use the Services dialog box on the Windows **Control Panel**.

Execution permission

Administrator permissions

Storage directory

`system-drive\Program Files\Hitachi\HNTRLib2\bin`

jpcvtaskctl (pauses/resumes the measurement of a task)

Format

Format 1 (pause the measurement by specifying a particular task ID)

```
jpcvtaskctl pause -t task-ID [-v]
```

Format 2 (resume the measurement by specifying a particular task ID)

```
jpcvtaskctl continue -t task-ID [-v]
```

Format 3 (output the list of IDs of paused tasks to the standard output in ascending order)

```
jpcvtaskctl list
```

Format 4 (notify the probe or IE probe of pauses and resumption)[#]

```
jpcvtaskctl sync [-v]
```

#

Even after you successfully register or remove the task ID as a target for pausing or resuming the task as a result of the command execution in format 1 or 2, a communication error may occur due to system load or other reasons. Such an error may cause the pause or resumption notification to the probe or IE probe to fail, possibly preventing the command from taking effect. In this case, remove the cause of the communication error and then execute the command in format 4. In doing so, the probe or IE probe is notified of again, enabling the pause or resumption to take effect.

Function

This command enables you to pause a measurement through the probe or IE probe, in which PFM - Agent for Service Response issues requests to monitoring targets and receives responses, on a task-ID basis. The command can also output the list of IDs of paused tasks to the standard output in ascending order, so that you can view the IDs of paused tasks or resume the measurement of a paused task by specifying the ID of the task.

You can pause tasks up to 500 task IDs.

Execution permission

Administrator permissions

Storage folder

installation-folder\agt\probe\bin

Arguments

-t *task-ID*

Specifies the ID of a task to be paused or resumed. The `jpcvtaskctl` command does not check if the specified task ID can be found in the measurement condition registration file (`esptask.xml`).

-v

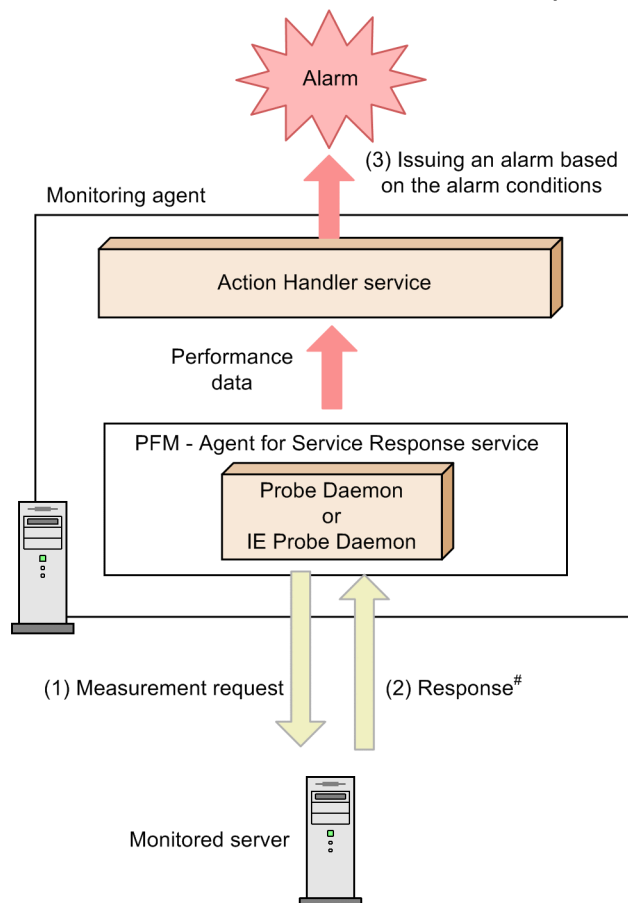
Outputs detailed information to the standard output when the `jpcvtaskctl` command is executed.

Notes

1. You should execute only one `jpcvtaskctl` command at a time. If more than one command is executed, the second and subsequent `jpcvtaskctl` commands result in errors.

2. You can execute the `jpcvtaskctl` command regardless of whether the probe is running or not. If you execute the command while the probe is not running, you can get the result after the probe is started. The same applies to the IE probe.
3. If you execute the `jpcvtaskctl` command on the monitoring target whose operation is monitored through the alarm function, start or stop monitoring through the alarm in combination with the execution of the `jpcvtaskctl` command.

Figure 11–1: Use of the alarm function for operation monitoring



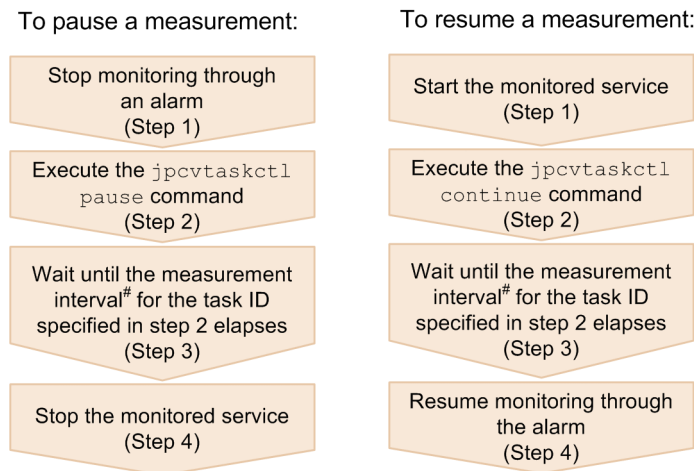
(1) and (2): The `jpcvtaskctl` command controls pausing and resuming measurements.
 (3): Alarms control starting and stopping monitoring.

 When the monitored server is not running, a server error is returned.

For details about starting or stopping monitoring through the alarm, see the *JP1 Version 11 JP1/Performance Management User's Guide*.

Make sure that you follow the steps below to pause or resume the measurement. If not, an alarm may be issued while PFM - Agent for Service Response is not performing any measurement or the monitoring target itself is not running, which is reported as an error.

Figure 11–2: Steps for pausing/resuming the measurement of the monitoring target whose operation is being monitored through the alarm function



It is specified in the `<INTERVAL>` tag for each task ID in the measurement condition registration file (`esptask.xml`).

To pause the measurement:

1. Stop monitoring through the alarm.
2. Execute the `jpcvtaskctl pause` command to pause the measurement by PFM - Agent for Service Response.
3. Wait until the measurement interval[#] for the task ID specified in step 2 elapses.
4. Stop the monitored service.

To resume the measurement:

1. Start the monitored service.
2. Execute the `jpcvtaskctl continue` command to resume the measurement by PFM - Agent for Service Response.
3. Wait until the measurement interval[#] for the task ID specified in step 2 elapses.
4. Resume monitoring through the alarm.

The measurement interval refers to the value of the `<INTERVAL>` tag specified for each task ID in the measurement condition registration file (`esptask.xml`). For details, see [8.3.2 Format and definition of measurement conditions \(common section\)](#).

Make sure that you wait for the period specified as the measurement interval before proceeding with the steps; otherwise, the first alarm after the resumption may be issued on the measurement result obtained before PFM - Agent for Service Response pauses or resumes the measurement completely, which will be reported as an error.

4. When you pause the measurement for a task ID using the `jpcvtaskctl pause` command, PFM - Agent for Service Response maintains the information that the task ID is on the list of command targets until you resume it with the `jpcvtaskctl continue` command.
Even if the task itself is removed when its ID is on the list of IDs of paused tasks, defining a new task with the same task ID will cause it to have the same state, meaning that it will be in a paused state.
For details about checking if a task ID is on the list of IDs of paused tasks, use the `jpcvtaskctl list` command to output the list of IDs of paused tasks to the standard output.
5. When pausing or resuming the measurement with the `jpcvtaskctl` command, do not start or reload PFM - Agent for Service Response at the same time. Otherwise, the PFM - Agent for Service Response service may terminate abnormally.

6. In a cluster system, the `jpcvtaskctl` command cannot be executed from the standby host.
7. When you move from a non-clustered configuration to the cluster system, the registered list of IDs of paused tasks is not inherited. If you paused tasks in the non-clustered configuration, set up the cluster environment and then use the `jpcvtaskctl pause` command to pause the measurements.

Return values

0	Normal termination
1	An error with an argument or definition was found during command execution, or operations could not continue due to a memory shortage. Error details are also output in a message.
2	The executed command resulted in an error. Error examples: <ul style="list-style-type: none"> • Storing the ID of the task to be paused failed. • Notifying the probe or IE probe failed. Error details are also output in a message.
3	More than one command is being executed at the same time.

Example 1 (pausing the measurement with a particular task ID)

The following shows an example of how to pause the measurement with task ID 100 in accordance with the projected outage of the monitored Web server below:

Projected outage of the monitored Web server

```
2016/07/07 01:00:00 Time to shut down the server
2016/07/07 06:00:00 Time to start the server
```

(1) Pre-measurement check

Before executing the `jpcvtaskctl pause` command, you must precheck the time specified as the measurement interval for task ID 100. You can see the interval in the measurement condition registration file (`esptask.xml`). Look for the `<TASKID>` tag whose value is 100, and check the value of the `<INTERVAL>` tag, in seconds, right below that tag.

In the measurement condition registration file (`esptask.xml`) below, the measurement interval for task ID 100 is 300 seconds (5 minutes):

```
<?xml version="1.0" encoding="Shift_JIS" standalone="no"?>
<!DOCTYPE TASKLIST SYSTEM "esptask.dtd">
<TASKLIST>
  <TASK>
    <GEN_PARAM>
      <TASKID>100</TASKID>
      <INTERVAL>300</INTERVAL>
    </GEN_PARAM>
    <SERV_PARAM>
      <HTTP>
        <URL>www.example.com/</URL>
      </HTTP>
    </SERV_PARAM>
  </TASK>
</TASKLIST>
```

(2) General procedure for shutting down the monitored Web server

1. 2016/07/07 00:55:00: Before this time, stop monitoring through the alarm.
2. 2016/07/07 00:55:00: Before this time, execute the `jpcvtaskctl pause` command to stop the measurement with task ID 100.
3. Wait until the measurement interval for task ID 100 elapses (5 minutes).
4. 2016/07/07 01:00:00: At this time, shut down the monitored Web server as scheduled.

Before 00:55:00 on July 07, 2016, make sure that you stop alarm-based monitoring of the task with task ID 100, which is to be paused, and pause the measurement by executing the `jpcvtaskctl pause` command. Make sure that you stop the alarm-based monitoring first. If you pause the measurement before stopping the alarm-based monitoring, a failed-measurement error may be issued as an error.

When the `jpcvtaskctl pause` command is successful, the KAVK43004-I message is output as follows:

```
>jpcvtaskctl pause -t 100
KAVK43004-I The command was successfully executed.
```

Example 2 (resuming the paused measurement with a particular task ID)

The following shows an example of how to resume the measurement with task ID 100, which was paused in Example 1, right after the scheduled server start time (2016/07/07 06:00:00).

(1) General procedure for starting the monitored Web server

1. 2016/07/07 06:00:00: Start the monitored Web server.
2. 2016/07/07 06:03:00: Confirm that the monitored Web server is now started, execute the `jpcvtaskctl continue` command, and then resume the measurement with task ID 100.
3. Wait until the measurement interval for task ID 100 elapses (5 minutes).
4. 2016/07/07 06:08:00: After this time, start alarm-based monitoring.

After you resume the measurement by executing the `jpcvtaskctl continue` command, wait until the measurement interval for task ID 100, which can be found in the measurement condition registration file (`esptask.xml`), elapses (5 minutes) just like Example 1. Then, after 06:08:00 on July 7, 2016, when the measurement should be started completely, start alarm-based monitoring of the task with task ID 100.

When the `jpcvtaskctl continue` command is successful, the KAVK43004-I message is output as follows:

```
>jpcvtaskctl continue -t 100
KAVK43004-I The command was successfully executed.
```

Example 3 (pausing the measurement does not take effect due to an error or any other reason)

In Example 1, you may see one of the following messages when executing the `jpcvtaskctl pause` command. The following subsections show how to handle the situation in these cases.

(1) KAVK43008-E is output

```
>jpcvtaskctl pause -t 100
KAVK43008-E An internal file operation failed. OP=WRITE, ERRNO=xx, P1=xx,
P2=xx, ERRINFO=xx
KAVK43003-E An attempt to execute the command has failed.
```

The task ID for the task to be paused could not be registered. Remove the cause of the error based on the description for KAVK43008-E in [12.4 Messages](#), and then re-execute the `jpcvtaskctl pause` command.

To check if the task ID for the task to be paused has been registered successfully, execute the `jpcvtaskctl list` command and see the result of it. If the task has been registered successfully, the task ID specified in the argument `-t` on the execution of the `jpcvtaskctl pause` command appears as the execution result of the `jpcvtaskctl list` command, as shown below:

```
>jpcvtaskctl list
100
```

(2) KAVK43009-E is output

```
>jpcvtaskctl pause -t 100
KAVK43009-W A communication to the service failed. SERVICE=PROBE
KAVK43009-W A communication to the service failed. SERVICE=IEPROBE
KAVK43004-I The command was successfully executed.
```

The task ID for the task to be paused was registered successfully, but the notification of pausing the task to the probe or IE probe failed. A possible failure scenario includes a communication error caused by heavy system load or any other reason.

If the probe or IE probe is not running, the KAVK43009-W message is output. Thus, check the value of `SERVICE` in the KAVK43009-W message first, and then identify whether the probe or IE probe is running. If the value of `SERVICE` is `PROBE`, then check that the probe is running, and if the value is `IEPROBE`, then check that the IE probe is running. If you are performing a measurement other than IE scenarios, then check that the probe is running, and if performing the measurement of an IE scenario, then check that the IE probe is running. The only service that matters is services being measured; thus ignore this message if a service that is not measured is not running.

If the probe or IE probe is running, but this message is output, check how much the system is loaded, and then execute the `jpcvtaskctl sync` command as shown below:

```
>jpcvtaskctl sync
KAVK43004-I The command was successfully executed.
```

When the command is executed successfully, only the notification to the probe or IE probe is sent again, causing the measurement to be paused.

If the command fails, add `-v` to the argument of the `jpcvtaskctl sync` command to show more detailed error information:

```
>jpcvtaskctl sync -v
KAVK43010-E A communication to the service failed. OP=xx, ERRNO=xx,
SERVICE=PROBE, ERRINFO=xx
KAVK43010-E A communication to the service failed. OP=xx, ERRNO=xx,
SERVICE=IEPROBE, ERRINFO=xx
KAVK43003-E An attempt to execute the command has failed.
```

Remove the cause of the error based on the description for the action the operator should take when the message is output in [12.4 Messages](#), and then re-execute the command.

jpcvtest (executes measurement tests)

Format

Format 1

```
jpcvtest -wtfile Web-transaction-file-name -wtname Web-transaction-name [ -t timeout-period
(seconds)] [-s] [-v]
```

Format 2

```
jpcvtest -n measurement-condition-ID [-s] [-v]
```

Function

The functions and usage patterns of each format of the `jpcvtest` command are described below. For details about measurement test usage patterns, see [2.1.3 Web transaction measurement test](#).

Format 1

Based on the Web transaction and timeout period specified as arguments, this command immediately executes a measurement test and outputs measurement results to the standard output.

The Web transaction file name and Web transaction name that are used for a measurement test are directly specified as arguments.

Use this format when conducting a measurement test for Web transactions that are not defined in the measurement condition registration file. The main usage patterns for this format are shown below.

- Verifying whether Web transactions can be measured using a Web transaction file that is created when the product is installed
- Preliminary checking of a new Web transaction file that is created before it is registered in the measurement condition registration file, while production operations are in progress

Format 2

This command immediately executes a measurement test for a Web transaction with the measurement condition ID specified as an argument and outputs measurement results to the standard output.

A measurement test is executed by reading definition information (a Web transaction file name, Web transaction name, and timeout period) related to the measurement condition ID specified as an argument from the measurement condition registration file (`esptask.xml`). If the measurement target with the specified measurement condition ID is not a Web transaction, the measurement result is output as an error. Note that this format cannot be used on a standby node in a cluster environment.

Use this format when conducting a measurement test for an existing Web transaction that is defined in the measurement condition registration file. This format can be used in an environment where Web transactions are measured using PFM - Agent for Service Response, in the following situations:

- To verify whether Web transactions can be measured after Web content or server settings on the monitored server are changed
- To verify whether Web transactions can be measured after the definitions for PFM - Agent for Service Response (such as definitions in a Web transaction file, measurement conditions, passwords, and authentication information in a certificate file) are changed
- To check whether the monitored server is operating when there are no changes to the settings or definitions

There are notes about using this format. See *1* in *Notes* below.

Execution permission

Administrator permissions

Storage folder

installation-folder\agtv\probe\bin

Arguments

-wtfile *Web-transaction-file-name*

Specifies the name of the Web transaction file to be used for a measurement test.

Specify a file with an `.xml` extension that is stored in *installation-folder\agtv\probe\webtrans*. When specifying a file name, include the file's extension, but not its path. File names are not case-sensitive. File names that contain spaces must be enclosed in double quotation marks ("").

-wtname *Web-transaction-name*

Specifies the name of the Web transaction to be subject to a measurement test. Vertical bars (|) cannot be used as part of a Web transaction name. Web transaction names that contain spaces must be enclosed in double quotation marks ("").

Note that the Web transaction name specified here corresponds to the value specified in the following locations:

- For Web Recorder
 New Web transaction name in the Create New Web Transaction window, or **New Web transaction name** in the Save As window
- For Web transaction file
 <TRANSACTION_NAME> tag
- For Measurement condition registration file
 <TRANSACTION_NAME> tag

-t *timeout-period*

Specifies a timeout period for measurement test execution in the range from 1 to 3,600 (seconds). If this argument is not specified, the default value is 30.

Note that the timeout period specified here corresponds to the value of the <TIMEOUT> tag in the measurement condition registration file.

-n *measurement-condition-ID*

Specifies the measurement condition ID registered in the measurement condition registration file.

You can specify as many measurement condition IDs as there are Web transactions (specified in the <WEBTRANS> tag) subject to measurement.

-s

Outputs measurement results for each scope.

-v

Outputs information required for investigating error causes (information other than measurement results, such as HTTP requests and response headers).

This information can be used to investigate causes when an error occurs during a measurement test.

Notes

1. PFM - Agent for Service Response performs a syntax check when the service is started or reloaded. If a syntax error[#] is found in the Web transaction file registered in the measurement condition registration file, other measurements by the probe also stop. This is because the Extensible Service Probe service (for measuring response performance) stops when the PFM - Agent for Service Response service is started or reloaded

For this reason, watch out for syntax errors when executing the `jpcvtest` command in format 2. When you create a new Web transaction file, we recommend that you check for any syntax errors by executing the `jpcvtest` command in format 1 before registering the Web transaction file in the measurement condition registration file. When you modify an existing Web transaction file, we also recommend that you check for any syntax errors by executing a measurement test before starting or reloading the service.

Syntax errors include the following cases: XML tags contain errors, or no password is set even though the user to be authenticated is specified (including cases where a password has not been correctly registered with the `esppasswd` command).

For details about the format of a Web transaction file, see [8.5 Web transaction files](#).

2. Multiple instances of the `jpcvtest` command cannot be executed at the same time. If multiple instances of this command are executed at the same time, the execution results of all the instances except the first one are indicated as an error.
3. If the test measurement by the `jpcvtest` command conflicts with test measurement by the probe, the `jpcvtest` command does not suppress the conflict but follows the specifications on the monitoring target. For example, if there is a restriction that prevents the monitored Web page from being accessed simultaneously, the measurement fails.
4. If you change the definitions for PFM - Agent for Service Response before executing the `jpcvtest` command, back up the definition files to be changed beforehand.
5. If the `jpcvtest` command is executed in format 1, and a message with a measurement condition ID is output, the measurement condition ID is indicated as 0.

Return values

0	Normal termination
1	An error with an argument or definition was found during command execution, or operations could not continue due to a memory shortage. Error details are also output in a message.
2	The measurement test executed by the command resulted in an error. Error examples: <ul style="list-style-type: none">• The monitored server is stopped.• The Web service is stopped.• The resource specified by the URL does not exist (HTTP 404 error).• An authentication error occurs.• A response determination error occurs. Error details are also output in a message.
3	Multiple instances of the command were executed at the same time.

Result report format

- Result report format when the command is executed in format 1

```
KAVK08333-I Web transaction test has started.
```



```

KAVK08334-I Web transaction test has succeeded. ResultCode=0
== Test report =====
Web Transaction Filename: wtdemo.xml ...The Web transaction file name specified by the command argument
Web Transaction Name: wtdemo1 ...The Web transaction name specified by the command argument
Service Type ID: 110 ... Service type ID (fixed as 110)#1
Measurement Start Time: 2014/06/18 19:46:52 ... Measurement start time
Measurement End Time: 2014/06/18 19:46:52 ... Measurement end time
Result Code: 0 ... Result code#2
=====
KAVK08336-I Web transaction test has ended.
KAVK42005-I The command was successfully executed.

```

- Result report format when the command is executed in format 2

```

KAVK08333-I Web transaction test has started.
KAVK08334-I Web transaction test has succeeded. ResultCode=0
== Test report =====
Measurement Condition ID: 100 ...The measurement condition ID specified by the command argument
Service Type ID: 110 ... Service Type ID (fixed as 110)#1
Measurement Start Time: 2014/06/18 19:46:52 ... Measurement start time
Measurement End Time: 2014/06/18 19:46:52 ... Measurement end time
Result Code: 0 ... Result code#2
=====
KAVK08336-I Web transaction test has ended.
KAVK42005-I The command was successfully executed.

```

#1

For details about service type IDs, see [Table 10-12 Service type IDs](#).

#2

For details about result codes, see [Table 10-11 Result code](#).

Example 1 (executing a measurement test)

Three examples of using this command are shown below, based on the definitions in the following Web transaction file (wtdemo.xml):

```

<?xml version="1.0" encoding="Shift_JIS" standalone="no"?>
<!DOCTYPE TRANSACTION_LIST SYSTEM "espwebtrans.dtd">
<TRANSACTION_LIST>
<TRANSACTION>
<TRANSACTION_PARAM>
<TRANSACTION_NAME>wtdemo1</TRANSACTION_NAME>
</TRANSACTION_PARAM>
<STEP>
<TITLE>Web transaction test command demo page</TITLE>
<REQUEST>
<URL>http://testmachine1/~test/jplpfm/SRmemo/wtdemo/wtdemopage1/index.php</URL>
</REQUEST>
</STEP>
<STEP>
<TITLE>page1</TITLE>
<REQUEST>

```

```

<URL>http://testmachine1/~test/jplpfm/SRmemo/wtdemo/wtdemopage1/success.php</URL>
</REQUEST>
</STEP>
<STEP>
<TITLE>Web transaction test command demo page</TITLE>
<REQUEST>
<URL>http://testmachine1/~test/jplpfm/SRmemo/wtdemo/wtdemopage1/index.php</URL>
</REQUEST>
</STEP>
</TRANSACTION>
</TRANSACTION_LIST>

```

In the following command usage example, a measurement test is executed for the Web transaction called *wtdemo1* in the above Web transaction file (*wtdemo.xml*).

```
jpcvtest -wtfile wtdemo.xml -wtname wtdemo1
```

If a measurement test is executed and succeeds, the following result report is output:

```

KAVK08333-I Web transaction test has started.
KAVK08334-I Web transaction test has succeeded. ResultCode=0
== Test report =====
Web Transaction Filename: wtdemo.xml
Web Transaction Name: wtdemo1
Service Type ID: 110
Measurement Start Time: 2014/06/18 19:46:52
Measurement End Time: 2014/06/18 19:46:52
Result Code: 0
=====
KAVK08336-I Web transaction test has ended.
KAVK42005-I The command was successfully executed.

```

If a measurement test is executed, and an error is indicated in the measurement result, an error message is also output as in the following output example. In this example, an HTTP request failed. For details about the descriptions and actions to take for the messages that are output, see [12.4 Messages](#).

```

KAVK08333-I Web transaction test has started.
KAVK08261-E The requested resource was not found. ID=0,Service_type=WEBTRA
NS,URL=testmachine1/~test/jplpfm/SRmemo/wtdemo/wtdemopage1/success.php
KAVK08341-E A HTTP response was failed.ID=0,STATUS_CODE=404
KAVK08335-E Web transaction test has failed. ResultCode=3
== Test report =====
Web Transaction Filename: wtdemo.xml
Web Transaction Name: wtdemo1
Service Type ID: 110
Measurement Start Time: 2014/06/18 19:25:13
Measurement End Time: 2014/06/18 19:25:13
Result Code: 3
=====
KAVK08336-I Web transaction test has ended.
KAVK42004-E An attempt to execute the command has failed.

```

Example 2 (collecting information to check the cause of the error detected by a measurement test)

By executing the command with the `-v` option specified, you can output information that can be used to investigate the cause of the error detected by a measurement test. (This information is any information other than measurement results, such as HTTP requests and response headers.) A command usage example is as follows:

```
jpcvtest -wtfile wtdemo.xml -wtname wtdemo1 -v
```

Based on the case where an HTTP request failed as shown in *Example 1 (executing a measurement test)*, the following section explains how to investigate error causes according to the information output by the `-v` option.

Here, assume that the browser can successfully access the URL (`success.php`) defined in the Web transaction file when the measurement test detects the error that causes the HTTP request to fail.

When the command is executed with the `-v` option specified, the following information is output:

Item	Format	Pad character
Step information	** Step(No. <i>AAAA</i>) ***** STEP ID : <i>BBBB</i>	<i>AAAA</i> : Step number (1,2,3....) <i>BBBB</i> : Step ID If there is no step information, the STEP ID line is omitted.
Resolve address	Resolve address " <i>AAAA</i> "->" <i>BBBB</i> "	<i>AAAA</i> : Host name (IP address if an IP address is specified) <i>BBBB</i> : IP address
HTTP request message	HTTP Request { <i>AAAA</i> }	<i>AAAA</i> : HTTP request message Multiple lines are output. Code <code>\r\n</code> is converted to a line break.
HTTP response header	HTTP Response { <i>AAAA</i> }	<i>AAAA</i> : HTTP response header Multiple lines are output. Code <code>\r\n</code> is converted to a line break.
Step response time	Step response time: <i>AAAA</i> sec.	<i>AAAA</i> : Step response time

The following is an example of command output with the `-v` option specified. HTTP request and response header information is output separately for each step.

```
KAVK08333-I Web transaction test has started.

** Step(No.1) *****
Resolve address "testmachine1"->"172.16.233.12"
HTTP Request {
  GET /~test/jplpfm/SRmemo/wtdemo/wtdemopage1/index.php HTTP/1.0
  Host: testmachine1:80
  Connection: close
  User-Agent: PFM - Agent for Service Response (Windows)
  Accept: */*
}
HTTP Response {
  HTTP/1.1 200 OK
  Date: Wed, 18 Jun 2014 10:30:55 GMT
  Server: Apache/2.0.52 (Red Hat)
  X-Powered-By: PHP/4.3.9
  Content-Length: 548
  Connection: close
  Content-Type: text/html; charset=none
```

```
}
Step response time :0.084 sec

** Step (No.2) *****
Resolve address "testmachine1"->"172.16.233.12"
HTTP Request {
  GET /~test/jp1pfm/SRmemo/wtdemo/wtdemopage1/success.php HTTP/1.0
  Host: testmachine1:80
  Connection: close
  User-Agent: PFM - Agent for Service Response (Windows)
  Accept: */*
}
HTTP Response {
  HTTP/1.1 404 Not Found
  Date: Wed, 18 Jun 2014 10:30:55 GMT
  Server: Apache/2.0.52 (Red Hat)
  X-Powered-By: PHP/4.3.9
  Content-Length: 0
  Connection: close
  Content-Type: text/html; charset=none
}

KAVK08261-E The requested resource was not found. ID=0,Service_type=WEBTRA
NS,URL=testmachine1/~test/jp1pfm/SRmemo/wtdemo/wtdemopage1/success.php
KAVK08341-E A HTTP response was failed. ID=0, STATUS_CODE=404
KAVK08335-E Web transaction test has failed. ResultCode=3
== Test report =====
Web Transaction Filename: wtdemo.xml
Web Transaction Name: wtdemo1
Service Type ID: 110
Measurement Start Time: 2014/06/18 19:30:55
Measurement End Time: 2014/06/18 19:30:55
Result Code: 3
=====
KAVK08336-I Web transaction test has ended.
KAVK42004-E An attempt to execute the command has failed.
```

In the above output example, the first step succeeded with HTTP status code 200 (OK) , while the second step accessed success.php and received status code HTTP404 (Not Found) from the monitored server (testmachine1).

This fact clarifies the following two points:

1. The browser was able to successfully access the URL (success.php) defined in the Web transaction file. The resource for success.php exists on the monitored server.
2. Both the first and second steps sent HTTP request messages to the same monitored server (testmachine1), and the only difference between them is the URLs that they accessed (index.php and success.php). When success.php was accessed, an HTTP404 error occurred. It is very likely that the content of success.php itself could have been the cause of an HTTP404 error.

Now, if we look at the content of success.php (which resulted in an HTTP404 error) on the monitored server, we find that the URL page has the following restriction: the page references the User-Agent section of each HTTP request message sent to the monitored server, and returns an HTTP404 (Not Found) error to requests received from any browsers other than Internet Explorer. (Note that the following content of success.php is just a sample for explaining this usage example.)

The restriction imposed on this page cannot be avoided by using the content of the standard User-Agent settings.

```

<?php
$ua=$_SERVER['HTTP_USER_AGENT']; // Indicates the User-Agent section of each HTTP request message.
// for Internet Explorer(Trident) only
// Returns an HTTP404 error to requests from any browsers other than Internet Explorer.
if (strpos($ua,"Trident"')==false) {
header("HTTP/1.1 404 Not Found");
exit();
}
?>
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
:

```

#

Trident is an HTML rendering engine that is incorporated into Internet Explorer. An *HTML rendering engine* is a program that interprets data written in a Web page description language and computes the layout of text and images that are displayed on the screen.

To make HTTP requests from PFM - Agent for Service Response and avoid the restriction imposed on this page, you need to change the User-Agent settings to match the contents of HTTP requests from Internet Explorer. As shown in the following setting example, you can use a method to set the <USER_AGENT> tag in the Web transaction file. For details about how to set the <USER_AGENT> tag, see [8.5.2\(1\) <TRANSACTION_PARAM> tag](#).

- Example of setting the <USER_AGENT> tag
Set the <USER_AGENT> tag to match the environment that you are using.

```

<?xml version="1.0" encoding="Shift_JIS" standalone="no"?>
<!DOCTYPE TRANSACTION_LIST SYSTEM "espwebtrans.dtd">
<TRANSACTION_LIST>
<TRANSACTION>
<TRANSACTION_PARAM>
<TRANSACTION_NAME>wtdemo1</TRANSACTION_NAME>
<USER_AGENT>Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729; .NET4.0C; .NET4.0E)</USER_AGENT>
</TRANSACTION_PARAM>
:
</TRANSACTION>
</TRANSACTION_LIST>

```

Example 3 (checking measurement test results separately for each scope)

To check measurement results not only for the entire Web transaction but also for individual scopes that are user-defined in Web Recorder, execute the command with the `-s` option specified, as follows:

```
jpcvtest -wtfile wtdemo2.xml -wtname wtdemo2 -s
```

The following output example shows the information output for individual scopes.

The information output under (`scopeALL`) indicates the measurement test results for the entire Web transaction, while the information output under (`scope1`) and (`scope2`) indicates the measurement test results for the individual scopes.

```

KAVK08333-I Web transaction test has started.
KAVK08334-I Web transaction test has succeeded. ResultCode=0

```

```

== Test report =====
Web Transaction Filename: wtdemo2.xml
Web Transaction Name: wtdemo2
Service Type ID: 110
Measurement Start Time: 2014/06/18 20:01:14
Measurement End Time: 2014/06/18 20:01:14
Result Code: 0
-- (scopeALL) -----
Total Response Time: 0.102 ... Total response time (seconds)
Setup Time: 0.027 ... Setup time (seconds)
HTTP Time: 0.073 ... HTTP time (seconds)
DNS Time: 0.002 ... DNS time (seconds)
TCP Connection Time: 0.024 ... TCP connection time (seconds)
Server Processing Time: 0.045 ... Server processing time (seconds)
Data Transfer Time: 0.024 ... Data transfer time (seconds)
Total Amount of Data: 15051 ... Total amount of data (bytes)
Request Count: 15 ... Number of request (counts)
Total Resource Size: 7576 ... Total resource size (bytes)
Throughput: 2525.33 ... Throughput (bits/second)
-- (scope1) -----
Total Response Time: 0.019
Setup Time: 0.009
HTTP Time: 0.01
DNS Time: 0
TCP Connection Time: 0.009
Server Processing Time: 0.006
Data Transfer Time: 0.003
Total Amount of Data: 1993
Request Count: 2
Total Resource Size: 1004
Throughput: 2677.33
-- (scope2) -----
:
-- (scope8) -----
Total Response Time: 0
Setup Time: 0
HTTP Time: 0
DNS Time: 0
TCP Connection Time: 0
Server Processing Time: 0
Data Transfer Time: 0
Total Amount of Data: 0
Request Count: 0
Total Resource Size: 0
Throughput: 0
=====
KAVK08336-I Web transaction test has ended.
KAVK42005-I The command was successfully executed.

```

12

Messages

This chapter describes the format of the PFM - Agent for Service Response messages, lists the locations to which messages are output, shows which messages are output to the Windows event log, and describes the messages in detail.

12.1 Message format

This section explains the format of messages issued by PFM - Agent for Service Response. It also describes the notations used in this manual to explain the messages.

12.1.1 Format of output messages

This section explains the format of the messages issued by PFM - Agent for Service Response. Each message consists of a message ID followed by a message text. The message format is as follows:

```
KAVXnnnnn-Y message-text
```

The message ID is composed of the following elements:

K

Identifies the system.

AVX

Indicates a PFM - Agent message. **F** or **K** is displayed for *X*.

nnnnn

Message number.

Y

Type of message:

- **E**: Error
Error message issued when the system cancels processing.
- **W**: Warning
Error message issued when the system resumes processing after the message has been output.
- **I**: Information
Message in which the system provides the user with information.

The following shows for each PFM - Agent for Service Response message type the corresponding Windows event log type:

-E

- Level: Error
- Description: Error message

-W

- Level: Warning
- Description: Warning message

-I

- Level: Information
- Description: Additional information message

12.1.2 Format of message explanations

This section describes the format used to explain messages in this manual. A portion of a message text that is shown in italics represents a variable; the actual wording in the message will depend on the circumstances. The manual lists the messages in the order of the message IDs. The following illustrates the format of a message explanation:

message-ID

message-text

Explains the message.

(S)

Explains the processing performed by the system.

(O)

Explains the action the operator should take when the message is displayed.

Reference note:

The system administrator who has been contacted by an operator must collect log information as described in [13. Error Handling Procedures](#), and conduct an initial investigation.

When you conduct initial checking to determine the cause of a problem, examine all applicable log information, such as the log information for the OS (Windows event log) and the log information output by PFM - Agent for Service Response. Log information may enable you to understand the details of the problem, take appropriate action, and prevent the problem from recurring in the future. You should also make a record of the operations that led up to the problem, and determine whether or not the problem is likely to recur.

12.2 Message output destinations

This section shows the output destinations of the messages issued by PFM - Agent for Service Response.

In the table below, Y and -- have the following meanings:

Y: Message is output.

--: Message is not output.

Table 12–1: PFM - Agent for Service Response message output destinations

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVF16000-I	Y	--	--	--	Y	--
KAVF16001-E	Y	--	--	--	Y	--
KAVF16002-I	Y	--	--	--	Y	--
KAVF16003-E	Y	--	--	--	Y	--
KAVF16004-I	--	--	--	--	Y	--
KAVF16005-E	--	--	--	--	Y	--
KAVF16006-I	--	--	--	--	Y	--
KAVF16007-E	--	--	--	--	Y	--
KAVF16008-E	--	--	--	--	Y	--
KAVF16009-W	--	--	--	--	Y	--
KAVF16010-E	Y	--	--	--	Y	--
KAVF16011-E	Y	--	--	--	Y	--
KAVF16012-E	Y	--	--	--	Y	--
KAVF16013-E	Y	--	--	--	Y	--
KAVF16014-E	Y	--	--	--	Y	--
KAVF16015-I	--	--	--	--	Y	--
KAVF16017-W	--	--	--	--	Y	--
KAVF16018-W	--	--	--	--	Y	--
KAVF16020-W	--	--	--	--	Y	--
KAVF16021-W	--	--	--	--	Y	--
KAVF16022-W	--	--	--	--	Y	--
KAVF16023-W	--	--	--	--	Y	--
KAVF16024-W	--	--	--	--	Y	--
KAVF16025-I	Y	--	--	--	Y	--
KAVF16026-E	Y	--	--	--	Y	--
KAVF16027-I	Y	--	--	--	Y	--
KAVF16028-E	Y	--	--	--	Y	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVF16029-I	--	--	--	--	Y	--
KAVF16030-E	--	--	--	--	Y	--
KAVF16031-I	--	--	--	--	Y	--
KAVF16032-E	--	--	--	--	Y	--
KAVF16033-W	--	--	--	--	Y	--
KAVF16034-W	--	--	--	--	Y	--
KAVF16035-W	--	--	--	--	Y	--
KAVK04000-E	--	--	--	Y	--	--
KAVK04002-E	--	--	--	Y	--	--
KAVK04003-E	--	--	--	Y	--	--
KAVK04004-E	--	--	--	Y	--	--
KAVK04005-E	--	--	--	Y	--	--
KAVK04006-E	--	--	--	Y	--	--
KAVK04007-I	--	--	Y	--	--	--
KAVK04008-I	--	--	Y	--	--	--
KAVK07001-E	--	--	--	Y	--	--
KAVK07002-E	--	--	--	Y	--	--
KAVK07004-E	--	--	--	Y	--	--
KAVK07005-E	--	--	--	Y	--	--
KAVK07006-E	--	--	--	Y	--	--
KAVK07007-E	--	--	--	Y	--	--
KAVK07008-E	--	--	--	Y	--	--
KAVK07010-I	--	--	Y	--	--	--
KAVK07011-E	--	--	Y	--	--	--
KAVK07100-W	--	--	--	Y	--	--
KAVK07101-E	--	--	--	Y	--	--
KAVK07102-E	--	--	--	Y	--	--
KAVK07103-E	--	--	--	Y	--	--
KAVK07104-E	--	--	--	Y	--	--
KAVK07105-E	--	--	--	Y	--	--
KAVK07106-E	--	--	--	Y	--	--
KAVK07107-E	--	--	--	Y	--	--
KAVK07108-E	--	--	--	Y	--	--
KAVK07109-E	--	--	--	Y	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK07110-E	--	--	--	Y	--	--
KAVK08000-I	Y	Y	--	--	--	--
KAVK08001-E	Y	Y	--	--	--	--
KAVK08002-I	Y	Y	--	--	--	--
KAVK08003-E	Y	Y	--	--	--	--
KAVK08005-E	--	Y	--	Y	--	--
KAVK08006-E	--	Y	--	Y	--	--
KAVK08007-E	--	Y	--	--	--	--
KAVK08008-E	--	Y	--	--	--	--
KAVK08010-E	--	Y	--	--	--	--
KAVK08023-E	--	Y	--	Y	--	--
KAVK08025-E	--	Y	--	Y	--	--
KAVK08026-W	--	Y	--	Y	--	--
KAVK08100-E	--	Y	--	Y	--	--
KAVK08101-E	--	Y	--	Y	--	--
KAVK08102-E	--	Y	--	Y	--	--
KAVK08103-E	--	Y	--	Y	--	--
KAVK08105-E	--	Y	--	--	--	--
KAVK08106-E	--	Y	--	--	--	--
KAVK08110-W	--	Y	--	--	--	--
KAVK08111-E	--	Y	--	Y	--	--
KAVK08112-E	--	Y	--	Y	--	--
KAVK08120-E	--	Y	--	--	--	--
KAVK08122-E	--	Y	--	--	--	--
KAVK08124-E	--	Y	--	--	--	--
KAVK08125-E	--	Y	--	--	--	--
KAVK08131-E	--	Y	--	--	--	--
KAVK08135-E	--	Y	--	Y	--	--
KAVK08137-E	--	Y	--	Y	--	--
KAVK08140-E	--	Y	--	--	--	--
KAVK08142-W	--	Y	--	--	--	--
KAVK08144-W	--	Y	--	--	--	--
KAVK08160-W	--	Y	--	--	--	--
KAVK08170-E	--	Y	--	Y	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK08171-E	--	Y	--	Y	--	--
KAVK08172-E	--	Y	--	Y	--	--
KAVK08173-E	--	Y	--	Y	--	--
KAVK08174-E	--	Y	--	Y	--	--
KAVK08176-E	--	Y	--	Y	--	--
KAVK08177-E	--	Y	--	Y	--	--
KAVK08178-E	--	Y	--	Y	--	--
KAVK08201-E	--	Y	--	Y	--	--
KAVK08202-E	--	Y	--	Y	--	--
KAVK08203-E	--	Y	--	Y	--	--
KAVK08204-E	--	Y	--	Y	--	--
KAVR08205-E	--	Y	Y	--	--	--
KAVK08211-E	--	Y	--	Y	--	--
KAVK08212-E	--	Y	--	--	--	--
KAVK08213-E	--	Y	--	Y	--	--
KAVK08214-E	--	Y	--	Y	--	--
KAVK08215-E	--	Y	--	Y	--	--
KAVK08216-E	--	Y	--	Y	--	--
KAVK08218-E	--	Y	--	--	--	--
KAVK08219-E	--	Y	--	--	--	--
KAVK08220-E	--	Y	--	--	--	--
KAVK08221-E	--	Y	--	--	--	--
KAVK08222-E	--	Y	--	--	--	--
KAVK08229-E	--	Y	--	--	--	--
KAVK08230-E	--	Y	--	--	--	--
KAVK08231-E	--	Y	--	--	--	--
KAVK08238-E	--	Y	--	--	--	--
KAVK08241-E	--	Y	--	--	--	--
KAVK08242-E	--	Y	--	--	--	--
KAVK08243-E	--	Y	--	--	--	--
KAVK08244-E	--	Y	--	--	--	--
KAVK08245-E	--	Y	--	Y	--	--
KAVK08247-E	--	Y	--	Y	--	--
KAVK08249-E	--	Y	--	Y	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK08250-E	--	Y	--	Y	--	--
KAVK08251-E	--	Y	--	Y	--	--
KAVK08252-E	--	Y	--	Y	--	--
KAVK08253-E	--	Y	--	Y	--	--
KAVK08254-E	--	Y	--	Y	--	--
KAVK08255-E	--	Y	--	Y	--	--
KAVK08256-E	--	Y	--	Y	--	--
KAVK08257-E	--	Y	--	Y	--	--
KAVK08258-E	--	Y	--	Y	--	--
KAVK08259-E	--	Y	--	Y	--	--
KAVK08260-E	--	Y	--	Y	--	--
KAVK08261-E	--	Y	--	Y	--	--
KAVK08262-E	--	Y	--	Y	--	--
KAVK08263-E	--	Y	--	Y	--	--
KAVK08264-E	--	Y	--	Y	--	--
KAVK08265-E	--	Y	--	Y	--	--
KAVK08266-E	--	Y	--	Y	--	--
KAVK08267-E	--	Y	--	--	--	--
KAVK08268-E	--	Y	--	Y	--	--
KAVK08269-E	--	Y	--	--	--	--
KAVK08270-W	--	Y	Y	--	--	--
KAVK08271-E	--	Y	--	Y	--	--
KAVK08273-E	--	Y	--	Y	--	--
KAVK08275-E	--	Y	--	--	--	--
KAVK08276-E	--	Y	--	--	--	--
KAVK08277-E	--	Y	--	--	--	--
KAVK08278-E	--	Y	--	--	--	--
KAVK08279-E	--	Y	--	--	--	--
KAVK08280-E	--	Y	--	--	--	--
KAVK08281-E	--	Y	--	--	--	--
KAVK08300-W	--	Y	--	--	--	--
KAVK08301-E	--	Y	--	--	--	--
KAVK08302-E	--	Y	--	Y	--	--
KAVK08303-E	--	Y	--	--	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK08304-E	--	Y	--	--	--	--
KAVK08305-E	--	Y	--	--	--	--
KAVK08310-E	--	Y	--	Y	--	--
KAVK08311-W	--	Y	Y	--	--	--
KAVK08312-E	--	Y	--	Y	--	--
KAVK08313-W	--	Y	Y	--	--	--
KAVK08314-W	--	Y	Y	--	--	--
KAVK08315-W	--	Y	Y	--	--	--
KAVK08316-W	--	Y	Y	--	--	--
KAVK08317-W	--	Y	Y	--	--	--
KAVK08318-W	--	Y	Y	--	--	--
KAVK08319-W	--	Y	Y	--	--	--
KAVK08320-E	--	Y	--	Y	--	--
KAVK08321-E	--	Y	--	Y	--	--
KAVK08322-E	--	Y	--	Y	--	--
KAVK08324-E	--	Y	--	Y	--	--
KAVK08332-E	--	--	--	Y	--	--
KAVK08333-I	--	--	Y	--	--	--
KAVK08334-I	--	--	Y	--	--	--
KAVK08335-E	--	--	--	Y	--	--
KAVK08336-I	--	--	Y	--	--	--
KAVK08337-E	--	--	--	Y	--	--
KAVK08338-E	--	--	--	Y	--	--
KAVK08339-E	--	--	--	Y	--	--
KAVK08340-E	--	--	--	Y	--	--
KAVK08341-E	--	--	--	Y	--	--
KAVK08344-E	--	--	--	Y	--	--
KAVK08345-E	--	Y	--	Y	--	--
KAVK08346-E	--	Y	--	Y	--	--
KAVK08507-E	--	Y	--	--	--	--
KAVK08508-E	--	Y	--	--	--	--
KAVK08509-E	--	Y	--	--	--	--
KAVK08511-E	--	Y	--	--	--	--
KAVK08512-E	--	Y	--	--	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK08513-E	--	Y	--	--	--	--
KAVK08514-E	--	Y	--	--	--	--
KAVK10000-I	Y	Y	--	--	--	--
KAVK10001-E	Y	Y	--	--	--	Y
KAVK10002-E	--	Y	--	--	--	--
KAVK10003-I	Y	Y	--	--	--	--
KAVK10004-E	Y	Y	--	--	--	--
KAVK10005-E	Y	Y	--	--	--	--
KAVK10006-E	Y	Y	--	--	--	--
KAVK10007-E	--	Y	--	--	--	--
KAVK10010-E	--	Y	--	--	--	--
KAVK10020-E	--	Y	--	--	--	--
KAVK10021-E	--	Y	--	--	--	--
KAVK10022-E	--	Y	--	--	--	--
KAVK10023-E	--	Y	--	--	--	--
KAVK10030-E	--	Y	--	--	--	--
KAVK10032-E	--	Y	--	--	--	--
KAVK10033-E	--	Y	--	--	--	--
KAVK10040-E	--	Y	--	--	--	--
KAVK10060-E	--	Y	--	--	--	--
KAVK10061-E	--	Y	--	--	--	--
KAVK10070-E	--	Y	--	--	--	--
KAVK10073-E	--	Y	--	--	--	--
KAVK10080-E	--	Y	--	--	--	--
KAVK10081-W	--	Y	--	--	--	--
KAVK10082-W	--	Y	--	--	--	--
KAVK10100-W	--	Y	--	--	--	--
KAVK10101-E	--	Y	--	--	--	--
KAVK10102-E	--	Y	--	--	--	--
KAVK10103-E	--	Y	--	--	--	--
KAVK10104-E	--	Y	--	--	--	--
KAVK10105-E	--	Y	--	--	--	--
KAVK10106-E	--	Y	--	--	--	--
KAVK10107-E	--	Y	--	--	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK11001-E	--	Y	--	--	--	--
KAVK11003-E	--	Y	--	--	--	--
KAVK11010-I	--	Y	--	--	--	--
KAVK11011-E	--	Y	--	--	--	--
KAVK11020-E	--	Y	--	--	--	--
KAVK11030-E	--	Y	--	--	--	--
KAVK11040-E	--	Y	--	--	--	--
KAVK11041-E	--	Y	--	--	--	--
KAVK11042-E	--	Y	--	--	--	--
KAVK37000-E	--	--	--	--	--	Y
KAVK37001-E	--	--	--	--	--	Y
KAVK37002-E	--	--	--	--	--	Y
KAVK37100-E	--	--	--	--	--	Y
KAVK37101-E	--	--	--	--	--	Y
KAVK37102-E	--	--	--	--	--	Y
KAVK37103-E	--	--	--	--	--	Y
KAVK37104-E	--	--	--	--	--	Y
KAVK37105-E	--	--	--	--	--	Y
KAVK37107-E	--	--	--	--	--	Y
KAVK37109-E	--	--	--	--	--	Y
KAVK37110-E	--	--	--	--	--	Y
KAVK37111-E	--	--	--	--	--	Y
KAVK37113-E	--	--	--	--	--	Y
KAVK37114-E	--	--	--	--	--	Y
KAVK37115-E	--	--	--	--	--	Y
KAVK37116-E	--	--	--	--	--	Y
KAVK37117-E	--	--	--	--	--	Y
KAVK37118-E	--	--	--	--	--	Y
KAVK37120-E	--	--	--	--	--	Y
KAVK37124-E	--	--	--	--	--	Y
KAVK37125-E	--	--	--	--	--	Y
KAVK37127-E	--	--	--	--	--	Y
KAVK37130-E	--	--	--	--	--	Y
KAVK37131-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK37132-E	--	--	--	--	--	Y
KAVK37133-E	--	--	--	--	--	Y
KAVK37134-E	--	--	--	--	--	Y
KAVK37135-E	--	--	--	--	--	Y
KAVK37137-E	--	--	--	--	--	Y
KAVK37138-E	--	--	--	--	--	Y
KAVK37139-E	--	--	--	--	--	Y
KAVK37140-E	--	--	--	--	--	Y
KAVK37141-E	--	--	--	--	--	Y
KAVK37142-E	--	--	--	--	--	Y
KAVK37143-E	--	--	--	--	--	Y
KAVK37144-E	--	--	--	--	--	Y
KAVK37145-E	--	--	--	--	--	Y
KAVK37200-E	--	--	--	--	--	Y
KAVK37201-E	--	--	--	--	--	Y
KAVK37202-E	--	--	--	--	--	Y
KAVK37203-E	--	--	--	--	--	Y
KAVK37204-E	--	--	--	--	--	Y
KAVK37205-E	--	--	--	--	--	Y
KAVK37206-E	--	--	--	--	--	Y
KAVK37207-E	--	--	--	--	--	Y
KAVK37208-E	--	--	--	--	--	Y
KAVK37209-E	--	--	--	--	--	Y
KAVK37210-E	--	--	--	--	--	Y
KAVK37211-E	--	--	--	--	--	Y
KAVK37212-E	--	--	--	--	--	Y
KAVK37213-E	--	--	--	--	--	Y
KAVK37214-E	--	--	--	--	--	Y
KAVK37215-E	--	--	--	--	--	Y
KAVK37216-E	--	--	--	--	--	Y
KAVK37217-E	--	--	--	--	--	Y
KAVK37218-E	--	--	--	--	--	Y
KAVK37219-E	--	--	--	--	--	Y
KAVK37220-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK37221-E	--	--	--	--	--	Y
KAVK37222-E	--	--	--	--	--	Y
KAVK37223-E	--	--	--	--	--	Y
KAVK37224-E	--	--	--	--	--	Y
KAVK37225-E	--	--	--	--	--	Y
KAVK37226-E	--	--	--	--	--	Y
KAVK37227-E	--	--	--	--	--	Y
KAVK37228-E	--	--	--	--	--	Y
KAVK37229-E	--	--	--	--	--	Y
KAVK37230-E	--	--	--	--	--	Y
KAVK37231-E	--	--	--	--	--	Y
KAVK37232-E	--	--	--	--	--	Y
KAVK37233-E	--	--	--	--	--	Y
KAVK37234-E	--	--	--	--	--	Y
KAVK37235-E	--	--	--	--	--	Y
KAVK37236-E	--	--	--	--	--	Y
KAVK37237-E	--	--	--	--	--	Y
KAVK37238-E	--	--	--	--	--	Y
KAVK37239-E	--	--	--	--	--	Y
KAVK37240-E	--	--	--	--	--	Y
KAVK37241-E	--	--	--	--	--	Y
KAVK37242-E	--	--	--	--	--	Y
KAVK37243-E	--	--	--	--	--	Y
KAVK37244-E	--	--	--	--	--	Y
KAVK37300-E	--	--	--	--	--	Y
KAVK37301-E	--	--	--	--	--	Y
KAVK37302-E	--	--	--	--	--	Y
KAVK37303-E	--	--	--	--	--	Y
KAVK37304-E	--	--	--	--	--	Y
KAVK37305-E	--	--	--	--	--	Y
KAVK37306-E	--	--	--	--	--	Y
KAVK37400-W	--	--	--	--	--	Y
KAVK37401-W	--	--	--	--	--	Y
KAVK37402-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK37403-E	--	--	--	--	--	Y
KAVK37404-E	--	--	--	--	--	Y
KAVK37405-E	--	--	--	--	--	Y
KAVK37406-E	--	--	--	--	--	Y
KAVK37407-E	--	--	--	--	--	Y
KAVK37408-E	--	--	--	--	--	Y
KAVK37409-E	--	--	--	--	--	Y
KAVK37410-E	--	--	--	--	--	Y
KAVK37411-E	--	--	--	--	--	Y
KAVK37412-E	--	--	--	--	--	Y
KAVK37413-E	--	--	--	--	--	Y
KAVK37500-E	--	--	--	--	--	Y
KAVK37501-E	--	--	--	--	--	Y
KAVK37502-E	--	--	--	--	--	Y
KAVK37503-E	--	--	--	--	--	Y
KAVK37504-E	--	--	--	--	--	Y
KAVK37505-E	--	--	--	--	--	Y
KAVK37506-E	--	--	--	--	--	Y
KAVK37507-E	--	--	--	--	--	Y
KAVK37508-E	--	--	--	--	--	Y
KAVK37509-E	--	--	--	--	--	Y
KAVK37510-E	--	--	--	--	--	Y
KAVK37511-E	--	--	--	--	--	Y
KAVK37512-E	--	--	--	--	--	Y
KAVK37513-E	--	--	--	--	--	Y
KAVK37514-E	--	--	--	--	--	Y
KAVK37515-E	--	--	--	--	--	Y
KAVK37516-E	--	--	--	--	--	Y
KAVK37517-E	--	--	--	--	--	Y
KAVK37518-E	--	--	--	--	--	Y
KAVK37519-E	--	--	--	--	--	Y
KAVK37520-E	--	--	--	--	--	Y
KAVK37521-E	--	--	--	--	--	Y
KAVK37522-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK37523-E	--	--	--	--	--	Y
KAVK37524-E	--	--	--	--	--	Y
KAVK37525-E	--	--	--	--	--	Y
KAVK37526-E	--	--	--	--	--	Y
KAVK37527-E	--	--	--	--	--	Y
KAVK37528-E	--	--	--	--	--	Y
KAVK37602-E	--	--	--	--	--	Y
KAVK37603-E	--	--	--	--	--	Y
KAVK37604-E	--	--	--	--	--	Y
KAVK37605-E	--	--	--	--	--	Y
KAVK37606-E	--	--	--	--	--	Y
KAVK37700-E	--	--	--	--	--	Y
KAVK37701-E	--	--	--	--	--	Y
KAVK37702-E	--	--	--	--	--	Y
KAVK37703-E	--	--	--	--	--	Y
KAVK37704-E	--	--	--	--	--	Y
KAVK37705-E	--	--	--	--	--	Y
KAVK37706-E	--	--	--	--	--	Y
KAVK37707-E	--	--	--	--	--	Y
KAVK37708-E	--	--	--	--	--	Y
KAVK37709-E	--	--	--	--	--	Y
KAVK37711-E	--	--	--	--	--	Y
KAVK37712-E	--	--	--	--	--	Y
KAVK37713-E	--	--	--	--	--	Y
KAVK37714-E	--	--	--	--	--	Y
KAVK37715-E	--	--	--	--	--	Y
KAVK37718-E	--	--	--	--	--	Y
KAVK37719-E	--	--	--	--	--	Y
KAVK37720-E	--	--	--	--	--	Y
KAVK37721-E	--	--	--	--	--	Y
KAVK37722-E	--	--	--	--	--	Y
KAVK37723-E	--	--	--	--	--	Y
KAVK37724-E	--	--	--	--	--	Y
KAVK37725-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK37726-E	--	--	--	--	--	Y
KAVK37727-E	--	--	--	--	--	Y
KAVK37728-E	--	--	--	--	--	Y
KAVK37729-E	--	--	--	--	--	Y
KAVK37730-E	--	--	--	--	--	Y
KAVK37731-E	--	--	--	--	--	Y
KAVK37732-E	--	--	--	--	--	Y
KAVK37733-E	--	--	--	--	--	Y
KAVK37734-E	--	--	--	--	--	Y
KAVK37800-I	--	--	--	--	--	Y
KAVK37801-I	--	--	--	--	--	Y
KAVK37802-I	--	--	--	--	--	Y
KAVK37803-I	--	--	--	--	--	Y
KAVK37804-I	--	--	--	--	--	Y
KAVK37805-I	--	--	--	--	--	Y
KAVK37806-I	--	--	--	--	--	Y
KAVK37807-I	--	--	--	--	--	Y
KAVK37808-I	--	--	--	--	--	Y
KAVK37809-I	--	--	--	--	--	Y
KAVK37850-E	--	--	--	--	--	Y
KAVK37851-E	--	--	--	--	--	Y
KAVK37852-E	--	--	--	--	--	Y
KAVK37853-E	--	--	--	--	--	Y
KAVK37854-E	--	--	--	--	--	Y
KAVK37855-E	--	--	--	--	--	Y
KAVK37856-E	--	--	--	--	--	Y
KAVK37857-E	--	--	--	--	--	Y
KAVK37858-E	--	--	--	--	--	Y
KAVK37859-E	--	--	--	--	--	Y
KAVK37860-E	--	--	--	--	--	Y
KAVK37861-E	--	--	--	--	--	Y
KAVK37862-E	--	--	--	--	--	Y
KAVK37863-E	--	--	--	--	--	Y
KAVK37864-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK37865-E	--	--	--	--	--	Y
KAVK37866-E	--	--	--	--	--	Y
KAVK37867-E	--	--	--	--	--	Y
KAVK37868-W	--	--	--	--	--	Y
KAVK37869-E	--	--	--	--	--	Y
KAVK37870-E	--	--	--	--	--	Y
KAVK37873-E	--	--	--	--	--	Y
KAVK37874-E	--	--	--	--	--	Y
KAVK37875-E	--	--	--	--	--	Y
KAVK37876-E	--	--	--	--	--	Y
KAVK37877-E	--	Y	--	--	--	--
KAVK38001-E	--	--	--	--	--	Y
KAVK38002-E	--	--	--	--	--	Y
KAVK38003-E	--	--	--	--	--	Y
KAVK38004-E	--	--	--	--	--	Y
KAVK38100-E	--	--	--	--	--	Y
KAVK38101-E	--	--	--	--	--	Y
KAVK38102-E	--	--	--	--	--	Y
KAVK38103-E	--	--	--	--	--	Y
KAVK38104-E	--	--	--	--	--	Y
KAVK38108-E	--	--	--	--	--	Y
KAVK38113-E	--	--	--	--	--	Y
KAVK38115-W	--	--	--	--	--	Y
KAVK38116-E	--	--	--	--	--	Y
KAVK38117-E	--	--	--	--	--	Y
KAVK38118-E	--	--	--	--	--	Y
KAVK38119-W	--	--	--	--	--	Y
KAVK38120-I	--	--	--	--	--	Y
KAVK38121-E	--	--	--	--	--	Y
KAVK38122-E	--	--	--	--	--	Y
KAVK38123-E	--	--	--	--	--	Y
KAVK38124-E	--	--	--	--	--	Y
KAVK38200-E	--	--	--	--	--	Y
KAVK38300-E	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK38302-W	--	--	--	--	--	Y
KAVK38303-W	--	--	--	--	--	Y
KAVK38304-W	--	--	--	--	--	Y
KAVK38500-E	--	--	--	--	--	Y
KAVK38501-E	--	--	--	--	--	Y
KAVK38502-E	--	--	--	--	--	Y
KAVK38504-E	--	--	--	--	--	Y
KAVK38505-E	--	--	--	--	--	Y
KAVK38506-E	--	--	--	--	--	Y
KAVK38507-E	--	--	--	--	--	Y
KAVK38508-E	--	--	--	--	--	Y
KAVK38601-E	--	--	--	--	--	Y
KAVK38602-E	--	--	--	--	--	Y
KAVK38603-E	--	--	--	--	--	Y
KAVK38604-E	--	--	--	--	--	Y
KAVK38605-E	--	--	--	--	--	Y
KAVK38700-E	--	--	--	--	--	Y
KAVK38752-E	--	--	--	--	--	Y
KAVK38753-E	--	--	--	--	--	Y
KAVK38754-E	--	--	--	--	--	Y
KAVK38755-E	--	--	--	--	--	Y
KAVK38756-E	--	--	--	--	--	Y
KAVK38757-E	--	--	--	--	--	Y
KAVK38758-E	--	--	--	--	--	Y
KAVK38759-E	--	--	--	--	--	Y
KAVK38800-I	--	--	--	--	--	Y
KAVK38801-I	--	--	--	--	--	Y
KAVK38803-I	--	--	--	--	--	Y
KAVK38804-I	--	--	--	--	--	Y
KAVK38805-I	--	--	--	--	--	Y
KAVK38806-I	--	--	--	--	--	Y
KAVK38807-I	--	--	--	--	--	Y
KAVK38808-I	--	--	--	--	--	Y
KAVK38809-W	--	--	--	--	--	Y

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK38810-I	--	--	--	--	--	Y
KAVK38811-I	--	--	--	--	--	Y
KAVK38812-E	--	--	--	--	--	Y
KAVK38813-E	--	--	--	--	--	Y
KAVK38814-I	--	--	--	--	--	Y
KAVK38815-E	--	--	--	--	--	Y
KAVK38816-E	--	--	--	--	--	Y
KAVK38817-E	--	Y	--	--	--	--
KAVK41000-E	--	Y	--	Y	--	--
KAVK41001-E	--	Y	--	Y	--	--
KAVK41002-E	--	Y	--	Y	--	--
KAVK41003-E	--	Y	--	Y	--	--
KAVK41004-E	--	Y	--	Y	--	--
KAVK41005-E	--	Y	--	Y	--	--
KAVK41006-E	--	Y	--	Y	--	--
KAVK41007-I	--	Y	--	Y	--	--
KAVK41008-I	--	Y	--	Y	--	--
KAVK42000-E	--	--	--	Y	--	--
KAVK42002-E	--	--	--	Y	--	--
KAVK42003-E	--	--	--	Y	--	--
KAVK42004-E	--	--	--	Y	--	--
KAVK42005-I	--	--	--	Y	--	--
KAVK42006-E	--	--	--	Y	--	--
KAVK42007-E	--	--	--	Y	--	--
KAVK43000-E	--	--	--	Y	--	--
KAVK43001-E	--	--	--	Y	--	--
KAVK43002-E	--	--	--	Y	--	--
KAVK43003-E	--	--	--	Y	--	--
KAVK43004-I	--	--	Y	--	--	--
KAVK43005-E	--	--	--	Y	--	--
KAVK43006-E	--	--	--	Y	--	--
KAVK43007-E	--	--	--	Y	--	--
KAVK43008-E	--	Y	--	Y	--	--
KAVK43009-W	--	--	--	Y	--	--

Message ID	Output destination					
	Windows event log	Integrated trace log	Standard output	Standard error output	Common message log	Dialog box
KAVK43010-E	--	--	--	Y	--	--
KAVK43011-E	--	--	--	Y	--	--
KAVK43015-E	--	--	--	Y	--	--
KAVK43016-E	--	Y	--	Y	--	--
KAVK43017-E	--	Y	--	--	--	--
KAVK43018-I	--	--	Y	--	--	--
KAVK43019-W	--	--	Y	--	--	--
KAVK43020-W	--	--	Y	--	--	--
KAVK43021-E	--	--	--	Y	--	--
KAVK43023-E	--	--	--	Y	--	--
KAVK43024-E	--	--	--	Y	--	--
KAVK43025-E	--	--	--	Y	--	--
KAVK43026-E	--	Y	--	--	--	--

12.3 List of messages output to the Windows event log

This section lists the messages that PFM - Agent for Service Response outputs to the Windows event log.

The Windows event log is displayed in the application log in the Event Viewer window.

Reference note:

To open the Event Viewer window, from the Windows **Start** menu, choose **Administrative Tools**, and then **Event Viewer**.

For any event issued by PFM - Agent for Service Response, the identifier `PFM-ServiceResponse` is displayed in the **Source** column of the Event Viewer window.

The table below lists the messages that PFM - Agent for Service Response outputs to the Windows event log.

Table 12–2: Messages output to the Windows event log

Message ID	Windows event log	
	Event ID	Type
KAVF16000-I	16000	Information
KAVF16001-E	16001	Error
KAVF16002-I	16002	Information
KAVF16003-E	16003	Error
KAVF16010-E	16010	Error
KAVF16011-E	16011	Error
KAVF16012-E	16012	Error
KAVF16013-E	16013	Error
KAVF16014-E	16014	Error
KAVF16025-I	16025	Information
KAVF16026-E	16026	Error
KAVF16027-I	16027	Information
KAVF16028-E	16028	Error
KAVK08000-I#	1	Information
KAVK08001-E#	2	Error
KAVK08002-I#	3	Information
KAVK08003-E#	4	Error
KAVK10000-I#	1	Information
KAVK10001-E#	2	Error
KAVK10003-I#	4	Information
KAVK10004-E#	5	Error
KAVK10005-E#	6	Error

Message ID	Windows event log	
	Event ID	Type
KAVK10006-E#	7	Error

#

If you set `Y` to the value of the `printlog_flag` in the [System Log] section of the Probe action condition definition file (`esp.conf`), they are output to the Windows event log. For details about the Probe action condition definition file, see [8.2 Probe action condition definition file \(esp.conf\)](#).

12.4 Messages

This section explains the messages issued by PFM - Agent for Service Response and the actions to be taken.

KAVF16000-I

Agent Collector has started. (*host=host-name, service=host-name<SR>*)

The Agent Collector has started.

(S)

Starts the Agent Collector processing.

KAVF16001-E

An attempt to start Agent Collector has failed. (*host=host-name, service=host-name<SR>*)

Startup of the Agent Collector failed.

(S)

Terminates the Agent Collector processing.

(O)

Check the immediately preceding message that has been output to the common message log, and take appropriate action according to that message.

KAVF16002-I

Agent Collector has stopped. (*host=host-name, service=host-name<SR>*)

The Agent Collector has stopped.

(S)

Terminates the Agent Collector processing.

KAVF16003-E

Agent Collector stopped abnormally. (*host=host-name, service=host-name<SR>*)

The Agent Collector stopped abnormally.

(S)

Terminates the Agent Collector processing.

(O)

Check the common message log to determine the cause.

KAVF16004-I

Probe Daemon was started.

A probe has started.

(S)

Starts the Probe Daemon processing.

KAVF16005-E

An attempt to start Probe Daemon has failed.

Startup of a probe failed.

(S)

Continues the Agent Collector processing.

(O)

The definition file may be invalid. Check the integrated trace log and, if necessary, revise the definition file.

KAVF16006-I

Probe Daemon was stopped.

A probe has stopped.

(S)

Continues the Agent Collector processing.

KAVF16007-E

An attempt to stop Probe Daemon has failed.

An attempt to stop a probe failed.

(S)

Continues the Agent Collector processing.

(O)

The load of the Probe Daemon may be heavy. Check the measurement interval.



Important

Even when Probe Daemon has stopped, this error might be output because the OS is busy due to shutdown. However, the processing to stop Probe Daemon continues.

KAVF16008-E

Reception of a signal interrupted service processing. (*signal=signal-number*)

The Agent Collector service has been suspended because a signal was accepted.

(S)

Stops the Agent Collector service.

KAVF16009-W

Reception of a signal caused the service to stop. (*signal=signal-number*)

The Agent Collector service is being stopped because a signal was accepted.

(S)

Stops the Agent Collector service.

KAVF16010-E

An attempt to initialize a service failed. (`rc=maintenance-code`)

Service initialization processing failed.

(S)

Cancels the service start processing.

(O)

Collect maintenance data and then contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*.

KAVF16011-E

You cannot start the service because it is already running.

An attempt to start the service failed because it is already running.

(S)

Stops the service.

(O)

Use the `jpctool service list (jpcctrl list)` command to check the service start status.

KAVF16012-E

Data could not be collected.

The system was unable to collect data.

(S)

Continues the process of the Agent Collector.

(O)

Check if the Probe Daemon or the IE Probe Daemon is running. If the cause is unknown, collect maintenance data and then contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*.

KAVF16013-E

Memory is insufficient.

Memory allocation failed due to a memory shortage.

(S)

- When this error occurs during the start processing:
Stops the Agent Collector service.
- When this error occurs after start processing has been completed (during operations):

The Agent Collector service attempts to continue its processing. Acquisition of the performance data that was to be acquired at this time fails.

(O)

Terminate any application that is not in use, or increase the memory.

KAVF16014-E

An attempt to create a pipe has failed. (*maintenance-code*)

An attempt to create a pipe failed.

(S)

Cancels data acquisition processing.

(O)

Take appropriate action according to the value displayed in the message.

KAVF16015-I

There is no measurement data.

No measurement has been performed since the Probe Daemon or the IE Probe Daemon started.

(S)

Continues subsequent processing.

(O)

The Probe Daemon or the IE Probe Daemon settings may be incorrect. Check and, if necessary, revise the settings.

KAVF16017-W

The acquired data is incorrect.

The data to be acquired from the Probe Daemon or the IE Probe Daemon is invalid.

(S)

Continues subsequent processing.

The system does not acquire the performance data that was to be acquired at this time.

(O)

Probe Daemon or the IE Probe Daemon operation may be invalid. If this message is displayed repeatedly, collect maintenance data and then contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*.

KAVF16018-W

Probe Daemon has already stopped.

The Probe Daemon has already stopped.

(S)

Resumes the service stop processing.

(O)

If this message is displayed repeatedly, collect maintenance data and then contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*.

This message is also displayed if the Probe Daemon service is stopped manually before the Agent Collector service is stopped.

KAVF16020-W

The measurement condition was not updated because an invalid property exists. (`task ID=measurement-condition-ID, property=property-name`)

The measurement condition was not updated because an invalid property exists.

(S)

Continues subsequent processing.

(O)

An invalid property exists. Check whether the required property is entered or the values you entered for each property is within the range of allowed values, and re-enter those properties.

KAVF16021-W

The measurement condition could not be created because an invalid property exists. (`property=property-name`)

The measurement condition could not be created because an invalid property exists.

(S)

Continues subsequent processing.

(O)

An invalid property exists. If the invalid property is the New Task ID, check whether the task ID is within the range from 1 to 65535 and does not overlap the currently defined task IDs, and re-enter the New Task ID. If the invalid property is New Task Protocol, select the protocol you use from the list.

KAVF16022-W

A measurement condition registration file could not be read.

A measurement condition registration file could not be read, because an invalid specification exists.

(S)

Measurement condition registration function is disabled in the monitoring console.

(O)

The measurement condition registration file has invalid specification. Check the measurement condition registration file for any specification format error, the measurement condition ID in the measurement condition registration file is duplicated in another measurement condition ID in the same file.

KAVF16023-W

The number of registered measurement conditions exceeds the max number displayable in the monitoring console.

The number of registered measurement conditions exceeds the max number displayable in the monitoring console.

(S)

The 501st and later measurement conditions are not displayed in the monitoring console. Moreover, the 501st and later measurement conditions cannot be deleted, edited, and added.

(O)

If you update the measurement conditions not displayed in the monitoring console, stop the Agent Collector service and directly edit the measurement condition registration file.

KAVF16024-W

The measurement condition registration file contains a measurement condition that has invalid properties. (task ID=*measurement-condition-ID*, property=*property-name*)

The measurement condition registration file contains a measurement condition that has invalid properties.

(S)

Continues subsequent processing.

(O)

The measurement condition registration file contains a measurement condition that has invalid properties. In the monitoring console, check whether the required property is entered or the values you entered for each property is within the range of allowed values, and re-enter those properties.

KAVF16025-I

Processing to reload the Probe daemon has ended.

Processing to reload the Probe daemon has ended.

(S)

Starts the Probe Daemon processing according to the measurement condition registration file contains.

KAVF16026-E

Processing to reload the Probe daemon has failed.

Processing to reload the Probe daemon has failed.

(S)

Continues the process of the Agent Collector.

(O)

The definition file may be invalid. Check the integrated trace log and, if necessary, revise the definition file.

KAVF16027-I

Processing to reload the IE Probe daemon has ended.

Processing to reload the IE Probe daemon has ended.

(S)

Starts the IE Probe Daemon processing according to the measurement condition registration file contains.

KAVF16028-E

Processing to reload the IE Probe daemon has failed.

Processing to reload the IE Probe daemon has failed.

- (S) Continues the process of the Agent Collector.
- (O) The definition file may be invalid. Check the integrated trace log and, if necessary, revise the definition file.

KAVF16029-I

IE Probe Daemon was started.

An IE probe has started.

- (S) Starts the IE Probe Daemon processing.

KAVF16030-E

An attempt to start IE Probe Daemon has failed.

Startup of an IE probe failed.

- (S) Continues the process of the Agent Collector.
- (O) The definition file may be invalid. Check the integrated trace log and, if necessary, revise the definition file.

KAVF16031-I

IE Probe Daemon was stopped.

An IE probe has stopped.

- (S) Continues the process of the Agent Collector.

KAVF16032-E

An attempt to stop IE Probe Daemon has failed.

An attempt to stop an IE probe failed.

- (S) Continues the process of the Agent Collector.
- (O) The load of the IE Probe Daemon may be heavy. Check the measurement interval.

Important

Even when IE Probe Daemon has stopped, this error might be output because the OS is busy due to shutdown. However, the processing to stop IE Probe Daemon continues.

KAVF16033-W

IE Probe Daemon has already stopped.

The IE Probe Daemon has already stopped.

(S)

Resumes the service stop processing.

(O)

If this message is displayed repeatedly, collect maintenance data and then contact the system administrator. For details about how to collect maintenance data, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*.

This message is also displayed if the IE Probe Daemon service is stopped manually before the Agent Collector service is stopped.

KAVF16034-I

Probe Daemon is starting.

The probe is now starting.

(S)

Continues Agent Collector processing.

(O)

Starting the probe is taking a long time.

Select **Administrative Tools**, then **Services**, and then check whether the probe has started in the Services dialog box. If the probe has not started, check the integrated trace log, and then follow the instructions for the output error message.

KAVF16035-I

IE Probe Daemon is starting.

The IE probe is now starting.

(S)

Continues Agent Collector processing.

(O)

Starting the IE probe is taking a long time.

Select **Administrative Tools**, then **Services**, and then check whether the IE probe has started in the Services dialog box. If the IE probe has not started, check the integrated trace log, and then follow the instructions for the output error message.

KAVK04000-E

An invalid option exists.

An invalid option was specified in the command arguments.

(S)

Terminates the command.

(O)

Specify the arguments correctly and then re-execute the command.

KAVK04002-E

An internal error occurred.

An internal error occurred. Processing cannot be continued.

(S)

Terminates the command.

(O)

Contact the system administrator.

KAVK04003-E

An error occurred in communication with *process-name*, *error-code*, *detail-error-code*

A communication error occurred in the daemon.

(S)

Terminates the command.

(O)

Make sure that there is no shortage in the system resources.

If re-execution does not recover the system, contact the system administrator.

KAVK04004-E

A system call error occurred in communication with *process-name*, *system-call-name*, *error-number*, *error-string*

A system call error occurred during communication with the daemon.

(S)

Terminates the command.

(O)

Make sure that there is no shortage in the system resources.

If re-execution does not recover the system, contact the system administrator.

KAVK04005-E

An attempt to connect with *process-name* has failed.

An attempt to establish connection with the daemon failed.

(S)

Terminates the command.

(O)

Make sure that the daemon process is running.

KAVK04006-E

process-name did not return a response.

A timeout occurred because the daemon did not respond to the request.

(S)

Terminates the command.

(O)

Check the daemon for any error.

If the problem cannot be resolved, contact the system administrator.

KAVK04007-I

process-name is active.

The daemon is running.

(S)

Terminates the command.

KAVK04008-I

process-name is inactive.

The daemon is not running.

(S)

Terminates the command.

(O)

Take appropriate action according to the error message for the applicable process.

KAVK07001-E

An attempt to read the password registration file has failed.

An attempt to access the password registration file failed.

The password registration file does not exist, or cannot open the password registration file, because access permissions have not been granted.

(S)

Terminates the command.

(O)

Make sure that the file has been placed in the specified folder. Check the file access permissions.

KAVK07002-E

An attempt to write to the password registration file has failed.

An attempt to write data to the password file failed.

(S)

Terminates the command.

(O)

Check the access permissions for the password file.

KAVK07004-E

An unexpected error occurred.

An unexpected error occurred.

(S)

Terminates the command.

(O)

Contact the system administrator.

KAVK07005-E

An installation path could not be acquired.

The location where the installation was installed could not be detected.

(S)

Terminates the command.

(O)

Contact the system administrator.

KAVK07006-E

An attempt to reserve memory has failed.

A memory shortage occurred during processing.

(S)

Terminates the command.

(O)

Terminate an unneeded application and then re-execute.
Either increase memory or increase the virtual memory space.

KAVK07007-E

The specification of an option is invalid.

A specified command option is invalid.

(S)

Terminates the command.

(O)

Check the option format and then re-execute the command.

KAVK07008-E

A running `esppasswd` exists.

Another process is executing `esppasswd`.

(S)

Terminates the command.

(O)

Re-execute the command after the current `esppasswd` has terminated.

KAVK07010-I

The execution of the command has succeeded.

Command execution was successful.

(S)

Terminates the command.

KAVK07011-E

An attempt to execute the command has failed.

Command execution failed.

(S)

Terminates the command.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK07100-W

The password is not registered.

The password has not been registered, but an attempt was made to display a list of keys.

(S)

Terminates the command.

KAVK07101-E

A password key is invalid.

Adding a password: The same password key already exists.

Changing or deleting a password: The specified password key does not exist.

(S)

Terminates the command.

(O)

Check the password key that has already been registered, and then re-enter the command.

KAVK07102-E

The password does not match the password entered first. Check and enter the password.

The second password entered does not match the first password.

(S)

Terminates the command.

(O)

Check the password and enter the correct password.

KAVK07103-E

Enter a password within 40 characters.

The entered password is longer than 40 bytes.

(S)

Terminates the command.

(O)

Enter a password that is no longer than 40 characters.

KAVK07104-E

Enter a password within 64 characters.

The entered password is longer than 64 bytes.

(S)

Terminates the command.

(O)

Enter a password that is no longer than 64 characters.

KAVK07105-E

An attempt to delete the backup file of a password file has failed.

An attempt to delete the backup file failed.

(S)

Terminates the command.

(O)

Make sure that no error has occurred in the file system.

If the problem cannot be resolved, contact the system administrator.

KAVK07106-E

An attempt to rename the backup file of a password file has failed.

An attempt to rename the backup file failed.

(S)

Terminates the command.

(O)

Make sure that no error has occurred in the file system.

If the problem cannot be resolved, contact the system administrator.

KAVK07107-E

An attempt to generate the backup file of a password file has failed.

An attempt to generate the backup file failed.

(S)

Terminates the command.

(O)

Make sure that no error has occurred in the file system.

If the problem cannot be resolved, contact the system administrator.

KAVK07108-E

An attempt to output the password key file has failed.

An attempt to output the backup file failed.

(S)

Terminates the command.

(O)

Check the access permissions for the specified file.

KAVK07109-E

An invalid character was used in the password.

An invalid character was used in the password.

(S)

Terminates the command.

(O)

Specify the password using alphanumeric characters and symbols.

KAVK07110-E

Enter a password within 1023 characters.

The entered password is longer than 1023 bytes.

(S)

Terminates the command.

(O)

Enter a password that is no longer than 1023 characters.

KAVK08000-I

esprobed was started.

esprobed was started.

(S)

Starts esprobed.

KAVK08001-E

Starting of esprobed has failed.

An attempt to start esprobed failed.

(S)

Does not start esprobed.

(O)

Make sure that the Probe action condition definition file has been stored in the specified folder. If start processing still fails, contact the system administrator.

KAVK08002-I

esprobed was stopped.

esprobed terminated normally.

(S)

Terminates esprobed normally.

KAVK08003-E

esprobed abnormally ended.

esprobed terminated abnormally.

(S)

Terminates esprobed abnormally.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK08005-E

An unexpected error occurred.

An internal error occurred in the program.

(S)

Terminates esprobed.

(O)

Contact the system administrator.

KAVK08006-E

The installation path could not be acquired.

The location where the product was installed could not be detected.

(S)

Terminates esprobed.

(O)

Contact the system administrator.

KAVK08007-E

An attempt to reserve memory has failed.

Memory allocation failed during processing.

(S)

Terminates esprobed.

(O)

Terminate an unneeded application and then re-execute. Increase memory or virtual memory space.

KAVK08008-E

The capacity of the disk is insufficient.

There is not enough disk space.

(S)

Terminates esprobed.

(O)

Delete an unneeded file and then re-execute the command, or add more disk space.

KAVK08010-E

The abnormal termination of SCM was detected.

Abnormal termination of SCM was detected.

(S)

Terminates esprobed.

(O)

Make sure that there is no shortage in the system resources. If the problem cannot be resolved, contact the system administrator.

KAVK08023-E

The format of a definition in the measurement condition registration file is invalid. *INFO=error-detail*

The format of a definition in the measurement condition registration file is invalid.

(S)

Terminates esprobed.

(O)

Check the measurement condition registration file for any specification format error.

KAVK08025-E

The format of a definition in the file is invalid. *FILE=file-name, INFO=error-detail*

The format of a definition in the file is invalid.

(S)

Terminates esprobed.

(O)

Check the file for any specification format error.

KAVK08026-W

Additional communication error information: *ID=task-ID, SERVICETYPE=service-type, ERRNO=error-number, ERRINFO=error-detail*

Additional communication error information, which is output together with the communication error message.

(S)

Continues subsequent processing.

(O)

Make sure that the connection information such as the host name and port number is correct. If it is correct, check the following:

If *ERRNO=10060*:

Make sure that monitored devices, including relay devices, are running or that they are reachable.

If *ERRNO=10061*:

Make sure that the monitored service is available (the communication port is listening to connections).

If *ERRNO=0*:

If the monitored devices, including relay devices, are under normal load conditions, check whether the measurement condition registration file has a valid timeout value.

KAVK08100-E

An attempt to open the Probe action condition definition file has failed.

An attempt to access the Probe action condition definition file failed.

(S)

Terminates esprobed.

(O)

Make sure that the Probe action condition definition file has been stored in the specified folder. Check the access permissions for the Probe action condition definition file.

KAVK08101-E

Information could not be acquired from the Probe action condition definition file.

An attempt to read the settings from the Probe action condition definition file failed.

(S)

Terminates esprobed.

(O)

Check the Probe action condition definition file for any specification format error.

KAVK08102-E

The content of a definition in the Probe action condition definition file is invalid. *section: key*

Settings in the Probe action condition definition file are invalid.

(S)

Terminates esprobed.

(O)

Correct the settings in the Probe action condition definition file and then re-execute the command.

KAVK08103-E

There is not necessary directory on the shared disk in the cluster operation. Necessary directory=*necessary-directory*

The directory required for cluster operation was not found.

(S)

Terminates esprobed.

(O)

Check the following:

- Whether the content of a definition in the Probe action condition definition file is correct
- Whether the shared disk is in use
- Whether there is not necessary directory on the shared disk

KAVK08105-E

Information could not be acquired from the command registration file.

Definitions in the command registration file could not be read.

(S)

Terminates esprobed.

(O)

Make sure that the command registration file has not been corrupted. Check the access permissions for the command registration file.

KAVK08106-E

The content of a definition in the command registration file is invalid. *user-defined-service-ID*

Definitions in the command registration file are invalid.

(S)

Terminates esprobed.

(O)

Correct the contents of the command registration file, and then re-execute the command.

KAVK08110-W

esprobed will be ended because measuring conditions do not exist.

The measurement condition registration file does not exist or does not contain measurement conditions.

(S)

Terminates esprobed.

(O)

Make sure that the measurement condition registration file exists. Register at least one measurement condition in the file.

KAVK08111-E

The content of a definition in the measurement condition registration file is invalid. *ID=measurement-condition-ID, TAG=tag-name*

Definitions in the measurement condition registration file are invalid.

(S)

Terminates esprobed.

(O)

Correct the contents of the measurement condition registration file, and then re-execute the command.

KAVK08112-E

The format of a definition in the measurement condition registration file is invalid. *error-detail*

The format of the measurement condition registration file is invalid.

- (S) Terminates esprobed.
- (O) Correct the contents of the measurement condition registration file, and then re-execute the command.

KAVK08120-E

Authentication with the SCM has failed.

SCM authentication failed.

- (S) Terminates esprobed.
- (O) Make sure that there is no shortage in the system resources. If the problem cannot be resolved, contact the system administrator.

KAVK08122-E

An attempt to initialize communication has failed.

An attempt to initialize communication failed.

- (S) Terminates esprobed.
- (O) Correct the settings in the Probe action condition definition file and then re-execute the command.

KAVK08124-E

A system call error occurred in communication. *system-call-name, error-number, error-string*

A system call error occurred during communication.

- (S) Terminates esprobed.
- (O) If this message is displayed repeatedly, check and, if necessary, revise the network environment. If the error cannot be recovered, contact the system administrator.

KAVK08125-E

An unexpected error occurred in communication. *error-code, detail-error-code*

An unexpected error occurred during communication.

- (S) Terminates esprobed.

(O)

If this message is displayed repeatedly, check and, if necessary, revise the network environment. If the error cannot be recovered, contact the system administrator.

KAVK08131-E

The addition of measuring conditions has failed. ID=*measurement-condition-ID*

An attempt to add a measurement condition failed.

(S)

Terminates esprobed.

(O)

Check the *KAVKnnnnn* message that was output immediately before this message and take the action indicated in it.

KAVK08135-E

The measuring condition ID is invalid. ID=*measurement-condition-ID*

An invalid measurement condition ID was specified in the measurement condition registration file. The specified value is outside the valid range, or a duplicate value may have been specified.

(S)

Terminates esprobed.

(O)

Correct the measurement condition ID and then re-execute the command.

KAVK08137-E

A password has not been set up. ID=*object-ID*

The password required for the specified measurement condition cannot be acquired from the password file.

(S)

Continues subsequent processing. However, the measurement condition for which the password could not be acquired will be ignored.

(O)

Use the password utility to register the password and then re-execute the command.

If this error occurs even though the password was already registered using the password utility, use the `esppasswd -l` command to obtain a key list, and make sure that the password identifier, authentication target, and user name are correct.

If an error occurs during HTTP(S) Web authentication, check the following issues related to the URL to be authenticated that is specified by the `esppasswd` command and the URL specified in the measurement condition registration file:

- Have the URL to be authenticated and the URL specified in the measurement condition registration file been registered without including a protocol identifier (`http://` or `https://`)?
- Does the URL to be authenticated match the URL specified in the measurement condition registration file?

KAVK08140-E

The report output has failed. ID=*measurement-condition-ID*

Report file output processing failed.

(S)

Continues subsequent processing.

(O)

Check the following:

- Whether there is an output directory for the report file, and whether access permissions have been granted
- Whether the report file is in use by the other process
- Whether there is enough disk space
- Whether there is no problem in the network status

KAVK08142-W

The file size of a report file reached the maximum report file size. ID=*measurement-condition-ID*

A backup file was created because the report file reached its maximum size.

(S)

Continues subsequent processing.

(O)

Back up the report file as required; otherwise, reports will be lost the next time the report file reaches its maximum size.

KAVK08144-W

The backup file of a report file was overwritten. ID=*measurement-condition-ID*

The backup file for the existing report file was overwritten.

(S)

Continues subsequent processing.

(O)

Back up the report file as required; otherwise, reports will be lost again the next time the report file reaches its maximum size.

KAVK08160-W

Measurement was started after having passed more than the measurement interval since measurement demand time. ID=*measurement-condition-ID*

Actual measurement was started after the measurement interval from the measurement start time elapsed.

(S)

Continues subsequent processing.

(O)

Check and, if necessary, revise the settings to eliminate delay in the actual measurement time by taking an appropriate action. Appropriate actions include increasing the maximum number of measurement conditions for the probe, reducing the number of measurement conditions, or increasing the measurement interval.

KAVK08170-E

The reading of a Web transaction file has failed.

A read error occurred in the Web transaction file.

(S)

Terminates esprobed.

(O)

Make sure that access permissions have been granted for the Web transaction file storage directory.
Make sure that the definitions are correct in the Web transaction file.

KAVK08171-E

There is no Web transaction. `ID=measurement-condition-ID, File=Web-transaction-file-name, Web transaction=Web-transaction-name`

The indicated Web transaction specified in the measurement condition does not exist. One of the following causes may apply:

- The Web transaction file specified in the measurement condition registration file does not exist.
- The absolute path to the Web transaction file is specified in the measurement condition registration file.
- The Web transaction specified in the measurement condition registration file does not exist.

(S)

Terminates esprobed.

(O)

Make sure that the specified Web transaction is correct.
Make sure that the specified Web transaction has been defined.

KAVK08172-E

The format of a definition in the Web transaction file is invalid. `File=Web-transaction-file-name, error-detail`

The format of the Web transaction file is invalid.

(S)

Terminates esprobed.

(O)

Correct the contents of the Web transaction file and then re-execute the command.

Also, make sure that the following situation does not apply:

- The encoding declaration (`encoding=`) specified in the XML declaration (`<?XML . . . ?>`) in the Web transaction file is not consistent with the character encoding actually used in the file.

KAVK08173-E

The content of a definition in the Web transaction file is invalid. `File=Web-transaction-file-name`, `TAG=tag-name`

Definitions in the Web transaction file are invalid.

(S)

Terminates esprobed.

(O)

Correct the contents of the Web transaction file and then re-execute the command.

KAVK08174-E

A password has not been set up. `File=Web-transaction-file-name`, `TAG=tag-name`

An attempt was made to acquire the password required for measurement of Web transactions from the password file, but the attempt failed.

(S)

Terminates esprobed.

(O)

Define the password in the Web transaction file or use the password utility to register the password, and then re-execute the command.

If this error occurs even though the password was already registered using the password utility, use the `esppasswd -l` command to obtain a key list, and make sure that the password identifier, authentication target, and user name are correct.

If an error occurs during HTTP(S) Web authentication, check the following issue related to the URL to be authenticated that is specified by the `esppasswd` command:

- Has the URL to be authenticated been registered without including a protocol identifier (`http://` or `https://`)?

KAVK08176-E

A variable string is not included in URL, message body or Cookie. `File=Web-transaction-file-name`, `Web transaction=Web-transaction-name`

The variable character string specified in the `<VARIABLE_PART>` in the Web transaction file was not found in the character string defined for the URL, message body or Cookie.

(S)

Terminates esprobed.

(O)

Make sure that the variable character string is defined correctly.

KAVK08177-E

There is no specified step identifier. `File=Web-transaction-file-name`, `Web transaction=Web-transaction-name`

The step identifier specified in the <TARGET_STEP_ID> tag in the Web transaction file was not defined in the preceding steps that were defined.

(S)

Terminates esprobed.

(O)

Make sure that the step identifier is defined correctly.

KAVK08178-E

A variable string is duplicated. File=*Web-transaction-file-name*, Web transaction=*Web-transaction-name*

The variable character string specified in the <VARIABLE_PART> tag in the Web transaction file is duplicated in another <VARIABLE_PART> tag in the same step.

(S)

Terminates esprobed.

(O)

Make sure that the variable character string is defined correctly.

KAVK08201-E

An attempt to reserve memory has failed. ID=*measurement-condition-ID*, Service_type=*service-type*

Memory allocation failed.

(S)

Terminates measurement.

(O)

Terminate an unneeded application and then re-execute. Add more memory or increase the virtual memory space.

KAVK08202-E

An unexpected error occurred. ID=*measurement-condition-ID*, Service_type=*service-type*

An unexpected error occurred.

(S)

Terminates measurement.

(O)

If this message is displayed repeatedly, contact the system administrator.

KAVK08203-E

Generation of a socket has failed. ID=*measurement-condition-ID*, Service_type=*service-type*

Generation of a socket failed.

(S)

Terminates measurement.

(O)

Terminate an unneeded application and then re-execute.

KAVK08204-E

The DNS name resolution has failed. ID=*measurement-condition-ID*, Service_type=*service-type*

DNS name resolution failed.

(S)

Terminates measurement.

(O)

Make sure that the DNS server is running normally.

KAVK08205-I

TLS/SSL library output error information. ERRINFO=*error-information*

TLS/SSL library output error information.

(S)

Terminates measurement.

(O)

Take appropriate action as indicated in the error message that is output before or after this message.

KAVK08211-E

An attempt to establish a TCP connection for measurement has failed. ID=*measurement-condition-ID*, Service_type=*service-type*

Establishment of a TCP connection failed.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is running normally, and that there is no problem in the network status between the measurement-target server and the probe.

KAVK08212-E

An attempt to shut down the TCP connection for measurement has failed. ID=*measurement-condition-ID*, Service_type=*service-type*

Release of a TCP connection failed.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is running normally, and that there is no problem in the network status between the measurement-target server and the probe.

KAVK08213-E

An attempt to send data during measurement has failed. ID=*measurement-condition-ID*,
Service_type=*service-type*

Data transmission failed.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is running normally, and that there is no problem in the network status between the measurement-target server and the probe.

KAVK08214-E

An attempt to receive data during measurement has failed. ID=*measurement-condition-ID*,
Service_type=*service-type*

Data reception failed.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is running normally, and that there is no problem in the network status between the measurement-target server and the probe.

KAVK08215-E

A measurement timeout occurred. ID=*measurement-condition-ID*, Service_type=*service-type*

A measurement timeout occurred.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is running normally, and that there is no problem in the network status between the measurement-target server and the probe.

If there is no problem with the measurement-target server and the network status, make sure that the timeout period is appropriate.

KAVK08216-E

Since the connection is already disconnected, data transmission cannot be performed. ID=*measurement-condition-ID*, Service_type=*service-type*

Data cannot be transferred because the connection has already been lost.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is running normally, and that there is no problem in the network status between the measurement-target server and the probe.

KAVK08218-E

The specified user of the destination mail address in SMTP does not exist locally. ID=*measurement-condition-ID*, Mail_address=*destination-email-address*

The specified user was not found in the local system.

(S)

Terminates measurement.

(O)

Make sure that the destination email address is correct.

KAVK08219-E

The SMTP service is not available. ID=*measurement-condition-ID*

The SMTP service is not available.

(S)

Terminates measurement.

(O)

Make sure that no error has occurred at the measurement-target server.

KAVK08220-E

Execution of the command was stopped on the SMTP server. ID=*measurement-condition-ID*

Command execution was cancelled at the SMTP server.

(S)

Terminates measurement.

(O)

Make sure that no error has occurred at the measurement-target server.

KAVK08221-E

The specified receipt mail address for SMTP probe is invalid. ID=*measurement-condition-ID*, Mail_address=*destination-email-address*

The domain specified by the destination email address does not accept email.

(S)

Terminates measurement.

(O)

Make sure that the destination email address is correct.

KAVK08222-E

The mail transmission by SMTP has failed. ID=*measurement-condition-ID*

Email send processing by SMTP failed.

(S)

Terminates measurement.

(O)

Make sure that no error has occurred at the measurement-target server.

KAVK08229-E

The mail receiving by POP3 has failed. ID=*measurement-condition-ID*

Email receive processing by POP3 failed.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server's inbox is accessible. Also, make sure that no error has occurred at the measurement-target server.

KAVK08230-E

The mail receiving by IMAP4 has failed. ID=*measurement-condition-ID*

Email receive processing by IMAP4 failed.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server's inbox is accessible. Also, make sure that no error has occurred at the measurement-target server.

KAVK08231-E

The file transmission by FTP has failed. ID=*measurement-condition-ID*, File=*file-name*

File transfer processing by FTP failed.

(S)

Terminates measurement.

(O)

Make sure that no error has occurred at the measurement-target server.

KAVK08238-E

The DHCP server does not have an assignable IP address. ID=*measurement-condition-ID*

The specified DHCP server does not have an assignable IP address.

(S)

Terminates measurement.

(O)

There may be a shortage in the IP address resources managed by the DHCP server. If this message is displayed repeatedly, make sure that the DHCP server is running correctly.

KAVK08241-E

A DNS server error occurred. *ID=measurement-condition-ID, Server=DNS-server-IP-address*

A DNS server error occurred.

(S)

Terminates measurement.

(O)

Make sure that no error has occurred at the measurement-target server, and check that the name of the host to be searched is correct.

KAVK08242-E

The domain name is not registered in the DNS server. *ID=measurement-condition-ID, Query=name-of-host-to-be-searched*

The specified host name has not been registered in the DNS server.

(S)

Terminates measurement.

(O)

Make sure that the name of the host to be searched is correct.

KAVK08243-E

The requested operation is not supported on the DNS server. *ID=measurement-condition-ID*

The DNS server does not support the requested operation.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is correct.

KAVK08244-E

The request was refused by the policy setup of a DNS server. *ID=measurement-condition-ID*

The request was refused by the DNS server's policy settings.

(S)

Terminates measurement.

(O)

Make sure that the measurement-target server is correct.

KAVK08245-E

An SSL handshake has failed. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

An SSL handshake has failed.

(S)

Terminates measurement.

(O)

Make sure that access to the specified URL via HTTPS is possible.

KAVK08247-E

There is no root certificate of the Certificate Authority that signed the server certificate. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

There is no root certificate of the Certificate Authority that signed the server certificate.

(S)

Terminates measurement.

(O)

Install the root certificate and then re-execute.

KAVK08249-E

The server certificate is invalid. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The server certificate is invalid.

(S)

Terminates measurement.

(O)

Check the HTTP server's server certificate.

KAVK08250-E

The validity period is not in the server certificate. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The validity period is not in the server certificate.

(S)

Terminates measurement.

(O)

Check the HTTP server's server certificate.

KAVK08251-E

The public key for the server certificate can not be decrypted. ID=*measurement-condition-ID*,
Service_type=*service-type*, URL=*URL*

The public key for the server certificate cannot be decrypted.

(S)

Terminates measurement.

(O)

Check the HTTP server's server certificate.

KAVK08252-E

The signature of the server certificate can not be verified. ID=*measurement-condition-ID*,
Service_type=*service-type*, URL=*URL*

The signature of the server certificate cannot be verified.

(S)

Terminates measurement.

(O)

Check the HTTP server's server certificate.

KAVK08253-E

A self-signed certificate was found in the chain. ID=*measurement-condition-ID*, Service_type=*service-type*,
URL=*URL*

Authentication failed because the certificates required for server authentication contain an unreliable self-signed certificate.

(S)

Terminates measurement.

(O)

Check the HTTP server's server certificate.

KAVK08254-E

The certificate chain exceeds the maximum verification depth. ID=*measurement-condition-ID*,
Service_type=*service-type*, URL=*URL*

Authentication failed because the certificate chain was too long.

(S)

Terminates measurement.

(O)

Check the HTTP server's server certificate.

KAVK08255-E

The client certificate is invalid. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The client certificate is invalid.

(S)

Terminates measurement.

(O)

Check the client certificate.

KAVK08256-E

The private key for the client certificate is invalid. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The password for the client certificate is invalid.

(S)

Terminates measurement.

(O)

Use the correct password for the client certificate.

KAVK08257-E

An authentication is required. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

Authentication is required to access the specified resource.

(S)

Terminates measurement.

(O)

Register the Web authentication user name and password in the measurement condition or Web transaction.

KAVK08258-E

A proxy authentication is required. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

A proxy authentication is required.

(S)

Terminates measurement.

(O)

Register the proxy user name and password in the measurement condition or Web transaction.

KAVK08259-E

A timeout has occurred. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

A timeout occurred at the HTTP server.

(S)
Terminates measurement.

(O)
Check the HTTP server or network status.

KAVK08260-E

The requested method is not allowed. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The method specified for the resource is not permitted.

(S)
Terminates measurement.

(O)
Make sure that the URL or method is correct.

KAVK08261-E

The requested resource was not found. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The specified resource was not found on the server.

(S)
Terminates measurement.

(O)

- Make sure that the URL is correct.
- If a Web transaction is being monitored, on the **Request Info** page in the Set Web Transaction Conditions window, select **Do not do for Acquire embedded resource** for the Web transaction.
Note, however, that embedded resources for other Web pages will no longer be acquired.
- If an HTTP or HTTPS service is being monitored, specify 1 for the depth of the embedded resources and frames to be acquired.
Note, however, that the pages displayed in the resources and frames that are embedded in the page at the specified URL will no longer be acquired.
- If an HTML resource can be updated, delete any double hyphens (--) in HTML comments (the part enclosed in <!-- and -->).
Note, however, that if -- is a meaningful character string, the display of the Web page will be affected.

KAVK08262-E

The user does not have permission for the requested operation. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The user does not have the permissions necessary to access the specified resource.

(S)
Terminates measurement.

(O)

Check the HTTP server settings.

If client authentication is performed, make sure that the client certificate is correct.

KAVK08263-E

A requested resource is invalid. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The specified resource is not available.

(S)

Terminates measurement.

(O)

Check the resource status.

KAVK08264-E

The requested URL is too long. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The server cannot accept the URL because it is too long.

(S)

Terminates measurement.

(O)

Specify a shorter URL.

KAVK08265-E

The entity is too long. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The server cannot accept the entity because it is too long.

(S)

Terminates measurement.

(O)

Specify a shorter message body.

KAVK08266-E

An internal server error has occurred. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

An error occurred at the HTTP server.

(S)

Terminates measurement.

(O)

Check the HTTP server or proxy server status.

KAVK08267-E

The reading or writing of the cookie file has failed. ID=*measurement-condition-ID*, Service_type=*service-type*, File=*file-name*

A read or write error occurred in the cookie file. The message displays the measurement condition ID and service type.

(S)

Terminates measurement.

(O)

Make sure that the cookie file exists and that the user has access permission.

KAVK08268-E

The client certificate is not matching to the private key. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

The client certificate and its password do not match.

(S)

Terminates measurement.

(O)

Make sure that the client certificate and its password are correct.

KAVK08269-E

An invalid cookie file was found. ID=*measurement-condition-ID*, Service_type=*service-type*, File=*file-name*

The format of the cookie file is invalid.

(S)

Terminates measurement.

(O)

Delete the cookie file.

KAVK08270-W

An invalid cookie header was received. ID=*measurement-condition-ID*, Service_type=*service-type*, Cookie=*cookie-header*

A cookie header with an invalid format was received. The cookie is not saved.

(S)

Continues measurement.

KAVK08271-E

An error occurred in the processing which set the client certificate. ID=*measurement-condition-ID*, Service_type=*service-type*, URL=*URL*

An error occurred when the client certificate was registered.

(S)

Terminates measurement.

(O)

Make sure that there is no shortage in the system resources. If the problem cannot be resolved, contact the system administrator.

KAVK08273-E

The specified URL is invalid. *ID=measurement-condition-ID, Service_type=service-type, URL=URL*

The specified URL has an invalid format.

(S)

Terminates measurement.

(O)

Specify the URL in the correct format.

KAVK08275-E

The creation of the new process for the user-defined command has failed. There are too many processes.
ID=measurement-condition-ID, User_defined_command=user-defined-command-name

There are too many active processes to execute the user-defined command.

(S)

Terminates measurement.

(O)

Terminate an application that is not in use.

KAVK08276-E

The opening of the user-defined command file has failed. *ID=measurement-condition-ID, User_defined_command=user-defined-command-name*

The user does not have the permissions to execute the specified user-defined command.

(S)

Terminates measurement.

(O)

Make sure that the user-defined command is executable.

KAVK08277-E

The user-defined command file was not found. *ID=measurement-condition-ID, User_defined_command=user-defined-command-name*

The specified user-defined command was not found.

(S)
Terminates measurement.

(O)
Make sure that the user-defined command exists.

KAVK08278-E

The user-defined command execution has failed. ID=*measurement-condition-ID*,
User_defined_command=*user-defined-command-name*

The specified user-defined command is not executable.

(S)
Terminates measurement.

(O)
Make sure that the user-defined command is executable.

KAVK08279-E

The user-defined command has failed. ID=*measurement-condition-ID*, User_defined_command=*user-defined-command-name*

The specified user-defined command terminated abnormally.

(S)
Terminates measurement.

(O)
Make sure that the user-defined command runs normally.

KAVK08280-E

The output of the user-defined command is invalid. ID=*measurement-condition-ID*,
User_defined_command=*user-defined-command-name*

Output of the specified user-defined command is invalid.

(S)
Terminates measurement.

(O)
Check the output of the user-defined command.

KAVK08281-E

The DNS resolution of the target hostname has failed. ID=*measurement-condition-ID*, Service_type=*service-type*, Query=*name-of-host-to-be-searched*

The corresponding IP address cannot be acquired because the specified search target is not a host name.

(S)
Terminates measurement.

(O)

Make sure that the name of the host to be searched is correct.

KAVK08300-W

An attempt to set up the timer precision has failed.

An attempt to set up the precision of the timer used for response time measurement failed. The measurement precision may become 5 to 10 milliseconds.

(S)

Continues measurement.

KAVK08301-E

The authentication has failed. *ID=measurement-condition-ID, Service_type=service-type, User=user-name*

Authentication failed.

(S)

Terminates measurement.

(O)

Check and, if necessary, revise the entered measurement condition. The user name or password provided by the measurement condition may be invalid.

KAVK08302-E

The server returned an unexpected response. *ID=measurement-condition-ID, Service_type=service-type, Server=server-name-or-IP-address-or-URL*

The server returned an unexpected response.

(S)

Terminates measurement.

(O)

The measurement target may not be an RFC-compliant server. Make sure that the measurement-target server is RFC-compliant.

Specifically, check the HTTP header of the monitored server for any of the following possible causes:

- The HTTP header sent from the Web server is not in a format that is separated by `:` as shown below:

```
Accept-Ranges: bytes
Content-Length: 3462
```

- No `Content-Type` is found.
- The value of `Content-Length` is not a number.

KAVK08303-E

The reading or writing of the file for measurement of FTP has failed. *ID=measurement-condition-ID, File=file-name*

A read or write error occurred in the file for FTP measurement.

- (S) Terminates measurement.
- (O) Make sure that the user has the permissions to access the specified file, and that the specified file exists.

KAVK08304-E

The host information acquisition of a local machine has failed. *ID=measurement-condition-ID, Service_type=service-type*

Acquisition of host information for the local machine failed.

- (S) Terminates measurement.
- (O) The correct IP address or host name may not have been set for the local machine. If this is the case, set the appropriate IP address.

KAVK08305-E

The file for measurement of FTP is not found. *ID=measurement-condition-ID, File=file-name*

The specified file for measurement of the FTP was not found.

- (S) Terminates measurement.
- (O) Make sure that the specified file exists.

KAVK08310-E

It was not consistent to response pattern. *ID=measurement-condition-ID, URL=URL*

The contents of the acquired HTML file do not match the specified response determination information.

- (S) Terminates measurement.
- (O) Check the HTTP server or network status.

KAVK08311-W

The measurement is continued though the acquisition of an embedded resource has failed. *ID=measurement-condition-ID, Service_type=service-type, URL=URL*

Acquisition of embedded resources failed, but measurement will continue in accordance with the settings in the Probe action condition definition file (*esp.conf*).

(S)

Continues measurement.

(O)

Check the `KAVKnnnnn-Z` message that was output immediately before this message and take the action indicated in it.

`nnnnn` indicates a message serial number. `Z` indicates a message type.

KAVK08312-E

The output of HTML has failed. `ID=measurement-condition-ID, Step_id=step-ID`

Output of the acquired HTML file failed.

(S)

Continues measurement.

(O)

Check the following:

- Whether there is enough disk space
- Whether there is an output directory for the HTML file, and whether access permissions have been granted
- Whether the step identifier is duplicated in another Web transaction

KAVK08313-W

The element including substitute string does not exist. `ID=measurement-condition-ID, Element_name=element-name`

An element containing the specified substitute character string was not found in the acquired HTML.

(S)

Replaces the variable character string with the null character, and then continues measurement.

(O)

Check the following:

- Whether the step identifier specified in the `<TARGET_STEP_ID>` tag is correct
- Whether the element containing the substitute character string specified in the `<TARGET_ELEMENT>` tag is correct
- Whether an unexpected result was sent in the measurement of the Web transaction

KAVK08314-W

The HTML including substitute string does not exist. `ID=measurement-condition-ID, Step_id=step-ID`

The HTML with the step identifier specified in the `<TARGET_STEP_ID>` tag was not found.

(S)

Continues measurement without replacing the variable character string.

(O)

Check to see if the response from the step with the step identifier specified in the <TARGET_STEP_ID> tag was HTML.

KAVK08315-W

The content of element including substitute string is empty. ID=*measurement-condition-ID*,
Element_name=*element-name*

The element containing the specified substitute character string was the null element.

(S)

Replaces the variable character string with the null character and continues measurement.

(O)

Check the following:

- Whether the step identifier specified in the <TARGET_STEP_ID> tag is correct
- Whether the element containing the substitute character string specified in the <TARGET_ELEMENT> tag is correct
- Whether the substitute character string specified in the <SUBSTITUTE_TYPE> tag is at the correct location

KAVK08316-W

The attribute of element including substitute string does not exist. ID=*measurement-condition-ID*,
Element_name=*element-name*, Attribute_name=*attribute-name*

The attribute name specified in the <TYPE_ATTRIBUTE> tag was not found in the element that contains the specified substitute character string.

(S)

Replaces the variable character string with the null character and continues measurement.

(O)

Check the following:

- Whether the step identifier specified in the <TARGET_STEP_ID> tag is correct
- Whether the element containing the substitute character string specified in the <TARGET_ELEMENT> tag is correct
- Whether the substitute character string specified in the <SUBSTITUTE_TYPE> tag is at the correct location

KAVK08317-W

The HTTP header including substitute string does not exist. ID=*measurement-condition-ID*,
Header_name=*HTTP-header-name*

The HTTP header does not include the substitute character string you specified.

(S)

Replaces the variable character string with the null character and continues measurement.

(O)

Check the following:

- Whether the step identifier specified in the <TARGET_STEP_ID> tag is correct
- Whether the HTTP header containing the substitute character string specified in the <TARGET_HEADER> tag is correct
- Whether an unexpected result was sent in the measurement of the Web transaction

KAVK08318-W

The content of HTTP header including substitute string is empty. ID=*measurement-condition-ID*, Header_name=*HTTP-header-name*

The content of HTTP header including substitute string is empty.

- (S)
Replaces the variable character string with the null character and continues measurement.
- (O)
Check the following:
- Whether the step identifier specified in the <TARGET_STEP_ID> tag is correct
 - Whether the content of HTTP header containing the substitute character string specified in the <TARGET_HEADER> tag is correct

KAVK08319-W

Execution of the command that generates substitute string has failed. ID=*measurement-condition-ID*, Command=*substitution-string-generation-command-name*

Execution of the command that generates substitute character string has failed.

- (S)
Replaces the variable character string with the null character and continues measurement.
- (O)
Check the following:
- Whether the specified command exits
 - Whether the commandline specified in the <TARGET_COMMAND_LINE> tag is correct
 - Whether the arguments are specified correctly in the <TARGET_COMMAND_ARG> tag
 - Whether the specified command outputs the substitute character string in the StandardOutput
 - Whether the return-code (exit-code) by executing the specified command is 0

KAVK08320-E

The output of HTTP header has failed. ID=*measurement-condition-ID*, Step_id=*step-ID*

The output of HTTP header has failed.

- (S)
Continues measurement.
- (O)
Check the following:

- Whether there is enough disk space
- Whether there is an output directory for the HTML file, and whether access permissions have been granted
- Whether the step identifier is duplicated in another Web transaction

KAVK08321-E

A timeout has occurred during execution of the command that generates substitute string. ID=*measurement-condition-ID*, Command=*substitution-string-generation-command-name*

A timeout has occurred during execution of the command that generates substitute character string. This is because the command that generates substitute character string is being executed when the timeout occurs or the command does not end.

(S)

Terminates measurement.

(O)

Check the following:

- Whether the command that generates substitute character string is executed with the correct arguments
- Whether the result of the command that generates substitute character string is executed is correct
- Whether the timeout is short

KAVK08322-E

An attempt to open the measurement condition registration file has failed. INFO=*error-detail*

An attempt to open the measurement condition registration file has failed.

(S)

Terminates esprobed.

(O)

Make sure that the measurement condition registration file exists. Check the access permissions for the measurement condition registration file.

KAVK08324-E

An attempt to open the file has failed. FILE=*file-name*, INFO=*error-detail*

An attempt to open the file has failed.

(S)

Terminates esprobed.

(O)

Make sure that the file exists. Check the access permissions for the file.

KAVK08332-E

The specification of an option is invalid. INFO=*error-detail*

The specification of an option is invalid.

The following values are set to INFO:

- -n: -n option is invalid.
- -s: -s option is invalid.
- -v: -v option is invalid.
- -wtfile: -wtfile option is invalid.
- -wtname: -wtname option is invalid.
- -t: -t option is invalid.
- UNKNOWN: An unknown option or parameter is specified.
- FORMAT ERROR: Required options are missing, or options that cannot coexist are specified.

(S)

Terminates the command.

(O)

Check the option format and then re-execute the command.

KAVK08333-I

Web transaction test has started.

Web transaction test has started.

(S)

Web transaction test has started.

(O)

This is not an error. No action is required.

KAVK08334-I

Web transaction test has succeeded. `ResultCode=result-code`

Web transaction test has succeeded.

(S)

Web transaction test has ended.

(O)

This is not an error. No action is required.

KAVK08335-E

Web transaction test has failed. `ResultCode=result-code`

Web transaction test has failed.

(S)

Web transaction test has ended.

(O)

See the message that was displayed before this message.

KAVK08336-I

Web transaction test has ended.

Web transaction test has ended.

(S)

Web transaction test has ended.

(O)

This is not an error. No action is required.

KAVK08337-E

Specified measuring conditions do not exist. ID=*measurement-condition-ID*

Specified measuring conditions do not exist.

(S)

Web transaction test has ended.

(O)

Make sure that the measurement conditions for the Web transaction with the specified measurement condition ID exist in the measurement condition registration file.

KAVK08338-E

Error occurred during measurement test. ID=*measurement-condition-ID*, STEP_INFO=*step-ID* (0 if a step ID cannot be acquired) (*step-serial-number*)

An error occurred during a Web transaction measurement test.

(S)

Continues or cancels processing.

(O)

See the message that was displayed before this message.

KAVK08339-E

XPKE_EXCEPTION occurred. CODE=*error-code*, MESSAGE=*error-message*

XPKE_EXCEPTION occurred.

(S)

Web transaction test has ended.

(O)

Eliminate the cause of the error by referring to the contents of the error message.

KAVK08340-E

Socket API error. SOCKET_ERRNO=*socket-error-NO*. (*detailed-error-number-of-Winsock-API*),
OPERATION=*socket-API-name*

Socket API error.

(S)

Web transaction test has ended.

(O)

If TCP connection fails (the KAVK08211-E message is displayed), see the socket error number (SOCKET_ERRNO), and eliminate the cause of the error as described below.

If the value of SOCKET_ERRNO is 10060:

This value indicates that an attempt to connect to the monitored server failed and timed out. Possible causes are shown below. Check the monitoring destination information settings, network, and monitored server.

- The IP address is incorrect (or if a host name is specified, it cannot be correctly resolved to an IP address).
- The OS of the monitored server is not running.
- The network is disconnected or faulty.
- Communications are blocked by a firewall (for example, proxy settings are insufficient in a network where communications pass through proxy servers).

If the value of SOCKET_ERRNO is 10061:

This value indicates that a connection rejection message is received from the monitored server. Possible causes are shown below. Check the monitoring destination information settings and the monitored server.

- The Web service on the monitored server is not running.
- The port number is incorrect.

If the value of SOCKET_ERRNO is not 10060 or 10061:

Make sure that the monitored server (and the Web service) are running normally, or check for any problems with the status of the network between the monitored server and the probe.

If TCP connections did not fail, make sure that the monitored server (and the Web service) are running normally, or check for any problems with the status of the network between the monitored server and the probe.

KAVK08341-E

A HTTP response was failed. ID=*measurement-condition-ID*, STATUS_CODE=*HTTP-status-code*

A HTTP response was failed.

(S)

Web transaction test has ended.

(O)

Take appropriate action according to the HTTP status code indicated in the message to eliminate the cause of the error.

KAVK08344-E

The result report output has failed.

The result report output has failed.

(S)

Web transaction test has ended.

(O)

Contact the system administrator.

KAVK08345-E

Loading a dynamic link library has failed. *LIBFILE=library-file, ERRNO=failure-information*

Loading a dynamic link library failed.

(S)

Terminates esprobed.

(O)

Make sure that a dynamic link library exists and that access permissions have been granted. Then, eliminate the cause.

KAVK08346-E

Retrieving an address of a function or variable from a dynamic link library has failed. *LIBFILE=library-file, PROCNAME=function-or-variable-name, ERRNO=failure-information*

Retrieving an address of a function or variable from a dynamic link library failed.

(S)

Terminates esprobed.

(O)

Make sure that the dynamic link library is correct, and then eliminate the cause of the error.

KAVK08507-E

Starting of jpcviesvc has failed.

Starting of jpcviesvc has failed.

(S)

Continues the process of the Agent Collector.

(O)

Check the Probe action condition definition file for any specification format error.

Check the daemon for any error.

If the problem cannot be resolved, contact the system administrator.

KAVK08508-E

jpcviesvc abnormally ended.

jpcviesvc abnormally ended.

(S)

Continues the process of the Agent Collector.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

If the problem cannot be resolved, contact the system administrator.

KAVK08509-E

The content of a definition in the Probe action condition definition file is invalid. *key*

The content of a definition in the Probe action condition definition file is invalid.

(S)

Continues the process of the Agent Collector.

(O)

Correct the contents of the Probe action condition definition file, and then retry.

KAVK08511-E

`jpcviesvc` has been already started.

`jpcviesvc` has been already started.

(S)

Terminates `jpcviesvc`.

(O)

`jpcviesvc` has been already started. If you restart `jpcviesvc`, terminate `jpcviesvc` first and then re-execute it.

KAVK08512-E

A prerequisite program is not installed.

A prerequisite program for the IE Probe Daemon is not installed.

(S)

Terminates `jpcviesvc`.

(O)

If you take measurements of the IE scenario, install in advance the prerequisite program for the IE probe Daemon (i.e. .NET Framework 3.5).

KAVK08513-E

An internal error occurred. *error-detail*

An internal error occurred.

(S)

Terminates `jpcviesvc`.

(O)

Contact the system administrator.

KAVK08514-E

Win32 API error occurred. *API=API-function-name, ERRNO=error-code*

Win32 API function returns an error.

(S)

Terminates jpcviesvc.

(O)

Contact the system administrator.

KAVK10000-I

jpcviemd was started.

jpcviemd was started.

(S)

jpcviemd was started.

KAVK10001-E

Starting of jpcviemd has failed.

Starting of jpcviemd has failed.

(S)

Starting of jpcviemd has failed.

(O)

Make sure that the Probe action condition definition file has been placed in the specified folder.

KAVK10002-E

jpcviemd has already started.

jpcviemd has already started.

(S)

Terminates jpcviemd.

(O)

jpcviemd has been already started. If you restart jpcviemd, terminate jpcviemd first and then re-execute it.

KAVK10003-I

jpcviemd was stopped.

jpcviemd was stopped.

(S)

jpcviemd was stopped.

KAVK10004-E

jpcviemd abnormally ended.

jpcviemd abnormally ended.

(S)

jpcviemd abnormally ended.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK10005-E

Abnormal termination of jpcvieprobed was detected.

Abnormal termination of jpcvieprobed was detected.

(S)

Continues subsequent processing.

(O)

Check the message that was output by the jpcvieprobed.

KAVK10006-E

A failure to start jpcvieprobed was detected.

A failure to start jpcvieprobed was detected.

(S)

Continues subsequent processing.

(O)

Check the message that was output by the jpcvieprobed.

KAVK10007-E

An attempt to restart jpcvieprobed failed. `PID=process-ID`

An attempt to restart jpcvieprobed failed.

(S)

Continues subsequent processing.

(O)

Check the status of the process that was displayed by the `PID`.

KAVK10010-E

A prerequisite program is not installed.

A prerequisite program for the IE Probe Daemon is not installed.

(S)

Terminates jpcviemd.

(O)

If you take measurements of the IE scenario, install in advance the prerequisite program for the IE probe Daemon (.NET Framework 2.0).

KAVK10020-E

An attempt to open the Probe action condition definition file has failed.

An attempt to open the Probe action condition definition file has failed.

(S)

Terminates jpcviemd.

(O)

Make sure that the Probe action condition definition file has been placed in the specified folder. Check the file access permissions.

KAVK10021-E

Information could not be acquired from the Probe action condition definition file.

Information could not be acquired from the Probe action condition definition file.

(S)

Terminates jpcviemd.

(O)

Check the format of the Probe action condition definition file is correct.

KAVK10022-E

The content of a definition in the Probe action condition definition file is invalid.*section: key*

The content of a definition in the Probe action condition definition file is invalid.

(S)

Terminates jpcviemd.

(O)

Correct the contents of the Probe action condition definition file, and then retry.

KAVK10023-E

The specified directory is not on the shared disk. (*directory=specified-directory-on-shared-disk*)

The specified directory, required when PFM - Agent Option for Service Response operates in a cluster system, is not on the shared disk.

(S)

Terminates jpcviemd.

(O)

Check the following:

- Whether the content of a definition in the Probe action condition definition file is correct
- Whether the shared disk is in use
- Whether there is not necessary directory on the shared disk

KAVK10030-E

An attempt to open the measurement condition registration file has failed.

An attempt to open the measurement condition registration file has failed.

(S)

Terminates jpcviemd.

(O)

Make sure that the measurement condition registration file has been placed in the specified folder. Check the file access permissions.

KAVK10032-E

The format of a definition in the measurement condition registration file is invalid. (*error-detail*)

The format of a definition in the measurement condition registration file is invalid.

(S)

Terminates jpcviemd.

(O)

Check the measurement condition registration file for any specification format error.

KAVK10033-E

The content of a definition in the measurement condition registration file is invalid. (*ID=measurement-condition-ID, TAG=tag-name*)

The content of a definition in the measurement condition registration file is invalid.

(S)

Terminates jpcviemd.

(O)

Correct the contents of the measurement condition registration file, and then retry or reload the file.

If the tag name is `INTERVAL`, make sure that the value for **Interval** is greater than the value for **Timeout**.

KAVK10040-E

An attempt to open the IE scenario file has failed.

An attempt to open the IE scenario file has failed.

(S)

Terminates jpcviemd.

(O)

Check the following:

- Whether the IE scenario file has been placed in the specified folder.
- Whether the access permissions on the IE scenario file are sufficient.
- Whether the absolute path to the IE scenario file is not specified in the measurement condition registration file (or a correct path is specified).

KAVK10060-E

An attempt to reserve memory has failed.

An attempt to reserve memory has failed.

(S)

Terminates jpcviemd.

(O)

Terminate any application that is not in use, or increase the memory or the virtual memory.

KAVK10061-E

The capacity of the disk is insufficient.

The capacity of the disk is insufficient.

(S)

Terminates jpcviemd.

(O)

Delete the unnecessary files and then re-execute, or add more disks.

KAVK10070-E

An internal error occurred. (*error-detail*)

An internal error occurred.

(S)

Terminates jpcviemd.

(O)

Contact the system administrator.

KAVK10073-E

An unexpected error occurred in communication. (*error-code, detail-error-code*)

An unexpected error occurred in communication.

(S)

Terminates jpcviemd.

(O)

If this message is repeatedly output, check whether problems exist in the network environment.

KAVK10080-E

The report output has failed. (*ID=measurement-condition-ID*)

The report output has failed.

(S)

Continues subsequent processing.

(O)

Check the following:

- Whether there is an output directory for the report file, and whether access permissions have been granted
- Whether the report file is in use by the other process
- Whether there is enough disk space
- Whether there is no problem in the network status

KAVK10081-W

The file size of a report file reached the maximum report file size. (*ID=measurement-condition-ID*)

Made a backup file because the file size of a report file reached maximum report file size.

(S)

Continues subsequent processing.

(O)

Back up the report file as required; otherwise, reports will be lost the next time the report file reaches its maximum size.

KAVK10082-W

The backup file of a report file was overwritten. (*ID=measurement-condition-ID*)

The backup file of a report file was overwritten.

(S)

Continues subsequent processing.

(O)

Back up the report file as required; otherwise, reports will be lost the next time the report file reaches its maximum size.

KAVK10100-W

Measurement started after the period from the measurement start time exceeded the measurement interval.
(ID=*measurement-condition-ID*)

Measurement started after the period from the measurement start time exceeded the measurement interval.

(S)

Continues subsequent processing.

(O)

Check and, if necessary, revise the settings to eliminate delay in the actual measurement time by taking an appropriate action. Appropriate actions include increasing the maximum number of measurement conditions for the IE probe, reducing the number of measurement conditions, or increasing the measurement interval.

KAVK10101-E

IE scenario cannot be measured because all jpcvieprobed are unavaibale.

IE scenario cannot be measured because all jpcvieprobed do not respond or do not start successfully.

(S)

Continues subsequent processing.

(O)

Restart the IE Probe.

KAVK10102-E

An attempt to receive the measured data has failed. ID=*measurement-condition-ID*

An attempt to receive the measured data has failed.

(S)

Continues subsequent processing.

(O)

If this message is output frequently, check the system status.

KAVK10103-E

Authentication with the SCM has failed.

Authentication with the SCM has failed.

(S)

Terminates jpcviemd.

(O)

Make sure that there is no shortage in the system resources. If the problem cannot be resolved, contact the system administrator.

KAVK10104-E

An attempt to initialize communication has failed.

An attempt to initialize communication has failed.

(S)

Terminates jpcviemd.

(O)

Make sure that there is no shortage in the system resources. If the problem cannot be resolved, contact the system administrator.

KAVK10105-E

A system call error occurred in communication. *system-call-name, error-number, error-string*

A system call error occurred in communication.

(S)

Terminates jpcviemd.

(O)

If this message is output repeatedly, check whether problems exist in the network environment. If the problem cannot be resolved, contact the system administrator.

KAVK10106-E

The abnormal termination of SCM was detected.

The abnormal termination of SCM was detected.

(S)

Terminates jpcviemd.

(O)

Make sure that there is no shortage in the system resources. If the problem cannot be resolved, contact the system administrator.

KAVK10107-E

It was not possible to enable the parameters of the Probe action condition definition file. *Parameters=parameter-information*

It was not possible to enable the parameters of the Probe action condition definition file.

(S)

Continues subsequent processing.

(O)

Check the *KAVKnnnnn-Z* message that was output immediately before this message and take the action indicated in it.

nnnnn indicates a message serial number. *Z* indicates a message type.

KAVK11001-E

Starting of jpcvieprobed has failed.

Starting of jpcvieprobed has failed.

(S)

Starting of jpcvieprobed has failed.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK11003-E

jpcvieprobed abnormally ended.

jpcvieprobed abnormally ended.

(S)

jpcvieprobed abnormally ended.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK11010-I

Normal termination of jpcviemd was detected.

Normal termination of jpcviemd was detected.

(S)

Terminates jpcvieprobed.

KAVK11011-E

Abnormal termination of jpcviemd was detected.

Abnormal termination of jpcviemd was detected.

(S)

Terminates jpcvieprobed.

(O)

Check the message that was output by the jpcviemd.

KAVK11020-E

An attempt to reserve memory has failed.

An attempt to reserve memory has failed.

(S)

Terminates jpcvieprobed.

(O)

Terminate any application that is not in use, or increase the memory or the virtual memory.

KAVK11030-E

An internal error occurred.

An internal error occurred.

(S)

Terminates jpcvieprobed.

(O)

Contact the system administrator.

KAVK11040-E

An attempt to initialize communication has failed.

An attempt to initialize communication has failed.

(S)

Terminates jpcvieprobed.

(O)

If this message is repeatedly output, check whether problems exist in the network environment.

KAVK11041-E

A system call error occurred in communication. (*system-call-name, error-number, error-string*)

A system call error occurred in communication.

(S)

Terminates jpcvieprobed.

(O)

If this message is repeatedly output, check whether problems exist in the network environment.

KAVK11042-E

An unexpected error occurred in communication. (*error-code, detail-error-code*)

An unexpected error occurred in communication.

(S)

Terminates jpcvieprobed.

(O)

If this message is repeatedly output, check whether problems exist in the network environment.

KAVK37000-E

An attempt to start Web Recorder has failed.

An attempt to start Web Recorder failed.

(S)

Does not start Web Recorder.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK37001-E

Web Recorder has ended abnormally.

Web Recorder terminated abnormally.

(S)

Terminates Web Recorder.

(O)

Check the `KAVKnnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK37002-E

An attempt to initialize the logging function has failed.

The Hitachi Network Objectplaza Trace Library (HNTRLib2) cannot be used.

(S)

Terminates Web Recorder.

(O)

Contact the system administrator.

KAVK37100-E

The definition of the Web Recorder action condition definition file is invalid. (*section-name* section: *key-name*)

The Web Recorder action condition definition file contains invalid information.

(S)

Resumes processing using the default values.

(O)

Check the file for a specification error. Check to see whether or not the use of default values is appropriate.

KAVK37101-E

An attempt to read the Web Recorder action condition definition file has failed.

The Web Recorder action condition definition file was not found.

The file cannot be opened due to a lack of required permissions.

(S)

Resumes processing using the default values.

- (O)
Make sure that the Web Recorder action condition definition file has been placed in the specified folder.
Check the access permissions for the Web Recorder action condition definition file.

KAVK37102-E

An attempt to read the Web transaction data has failed. (file name: *file-name*)

An attempt to read Web transaction information from the Web transaction file failed.

- (S)
Stops reading the Web transaction and performs other processing.

KAVK37103-E

An irreparable error occurred while processing Web transaction data. The Web transaction data is lost.

An irreparable error occurred while processing the read Web transaction information.

- (S)
Discards the read Web transaction information and restores the application to its initial status.

- (O)
Make sure that there is no shortage in the system resources.

KAVK37104-E

The save directory for Web transaction files does not exist.

The directory storing the Web transaction file was not found.

- (S)
Stops reading the Web transaction and performs other processing.

- (O)
Make sure that the Web transaction storage directory is in the specified folder.

KAVK37105-E

An attempt to acquire the list of Web transaction names has failed. (file name: *Web-transaction-file-name*)

An attempt to acquire a list of Web transaction names from the specified file failed.

- (S)
Stops reading the file and performs other processing.
- (O)
Check the *KAVKnnnnn* message displayed before this message; check that there is no error in the Web transaction file names in the specified file.

KAVK37107-E

An attempt to acquire the list of Web transaction file names has failed.

An attempt to acquire a list of Web transaction files failed.

(S)

Stops acquiring a list of Web transaction files and performs other processing.

(O)

Make sure that the Web transaction storage directory is in the specified folder.

KAVK37109-E

A system call error occurred.

A system call error occurred.

(S)

Cancels the file manipulation and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37110-E

You do not have the access permissions necessary for the selected directory. (directory name: *directory-name*)

The user does not have the permissions to access the specified directory.

(S)

Stops reading the file and performs other processing.

(O)

Check the access permissions for the specified directory.

KAVK37111-E

You do not have the access permissions necessary for the selected file. (file name: *file-name*)

The user does not have the permissions to access the specified file.

(S)

Cancels the file manipulation and performs other processing.

(O)

Check the access permissions for the specified file.

KAVK37113-E

No Web transaction name is selected.

No Web transaction name is specified.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the Web transaction name.

KAVK37114-E

No Web transaction file name is selected.

The name of the Web transaction file is missing.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the name of the Web transaction file.

KAVK37115-E

The specified file is not xml.

The specified Web transaction file is not in XML format.

(S)

Closing the message dialog box returns to the original window.

(O)

For a Web transaction file, specify a file in XML format.

KAVK37116-E

An attempt to acquire the Web transaction file name has failed.

An attempt to acquire a Web transaction file name in the Web transaction storage directory failed.

(S)

Performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37117-E

An attempt to acquire the Web transaction name has failed.

An attempt to acquire a Web transaction name from the Web transaction file failed.

(S)

Performs other processing.

(O)

Make sure that no more than one Web transaction with the same Web transaction name is defined in the Web transaction file.

KAVK37118-E

The specified file was not found. (*file name: file-name*)

During a write operation, a required temporary write file was not found in the temporary file storage directory.

(S)

Cancels the file write operation and performs other processing.

(O)

Check to see if a file in the temporary file storage directory was being used during the write operation to the Web transaction file.

KAVK37120-E

The object to be deleted was not found.

The specified Web transaction file does not contain the Web transaction definition to be deleted.

(S)

Cancels the Web transaction deletion processing and performs other processing.

(O)

Check to see if the specified Web transaction file contains the Web transaction to be deleted.

KAVK37124-E

The disk is full.

Available disk capacity is less than the size of the file to be written.

(S)

Cancels the Web transaction write operation and performs other processing.

(O)

Increase the available disk capacity.

KAVK37125-E

The specified Web transaction data does not exist.

The specified Web transaction definition was not found in the specified Web transaction file.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that the Web transaction to be read has been defined in the Web transaction file.

KAVK37127-E

An attempt to display the file name has failed.

The attempt to display Web transaction file names in the list of Web transaction files failed.

(S)

Performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37130-E

An attempt to display the list of Web transaction names has failed.

The attempt to display a list of Web transaction names failed.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that there is no shortage in the system resources.

KAVK37131-E

An attempt to create a Web transaction has failed.

The attempt to create new Web transaction information failed.

(S)

Cancels the creation processing and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37132-E

The specified file does not exist. (file name : *file-name*)

The specified file was not found.

The specified directory was not found.

There is no help file.

(S)

Cancels the file read or write operation and performs other processing.

(O)

Make sure that the specified file exists in the specified directory.

KAVK37133-E

An attempt to save the specified Web transaction has failed. (file name : *file-name*)

The attempt to save Web transaction information failed due to a write error.

(S)

Cancels the save operation on the Web transaction information and performs other processing.

(O)

Check the KAVKnnnnn message that was output immediately before this message and take the action indicated in it.

KAVK37134-E

An attempt to delete the specified Web transaction has failed.

The attempt to delete a Web transaction from the Web transaction file failed.

(S)

Cancels deletion of the Web transaction information and performs other processing.

(O)

Check the KAVKnnnnn message that was output immediately before this message and take the action indicated in it.

If this message was not immediately preceded by another message, make sure that there is no shortage in the system resources.

KAVK37135-E

No Web transaction files exist.

There is no Web transaction file in the Web transaction storage directory.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that the Web transaction storage directory contains Web transaction files.

KAVK37137-E

An invalid character is specified in the file name.

The file name contains an invalid character.

(S)

Closing the message dialog box returns to the original window.

(O)

Correct the invalid characters in the file name.

KAVK37138-E

The specified Web transaction name is already in use.

When a new Web transaction was created, the name of an existing Web transaction was specified as the new Web transaction name.

(S)

Closing the message dialog box returns to the original window.

(O)

Each Web transaction name must be unique within the same Web transaction definition file.

KAVK37139-E

The step definition does not exist.

An attempt was made to save a Web transaction, but no step information was defined.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that the step information has been defined.

KAVK37140-E

The scope definition is invalid.

An attempt was made to save a Web transaction, but the scope definition was insufficient or invalid.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that the scope definition is correct.

KAVK37141-E

The size of the Web transaction name has exceeded *permitted-maximum-length-in-bytes* bytes.

The specified Web transaction name exceeded the permitted maximum length in bytes.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the Web transaction name so that its length is within the permitted range.

KAVK37142-E

The size of the Web transaction file name has exceeded *permitted-maximum-length-in-bytes* bytes.

The specified Web transaction file name exceeded the permitted maximum length in bytes.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the Web transaction file name so that its length is within the permitted range.

KAVK37143-E

An attempt to open the version dialog box has failed.

An attempt to open the version dialog box failed. The files needed for opening the version dialog box may have been damaged.

(S)

Performs other processing without displaying the version dialog box.

(O)

Make sure that no error has occurred in the file system.

KAVK37144-E

No valid Web transaction file exists.

There is no Web transaction file that can be read. This is applicable when all Web transaction files in the Web transaction file storage directory are invalid.

(S)

Returns to the original window without opening the Select Web Transaction window.

(O)

Make sure that the Web transaction files are correct in the Web transaction file storage directory.

KAVK37145-E

An invalid character is specified in the Web transaction name.

The specified Web transaction name contains an invalid character string.

(S)

Closing the message dialog box returns to the original window.

(O)

Correct any invalid characters in the Web transaction name.

KAVK37200-E

The xml declaration does not exist on the first line.

There is no XML declaration on the first line in the specified XML file.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the required XML declaration statement on the first line in the XML file.

KAVK37201-E

The xml declaration is not closed.

The XML declaration statement is not closed in the specified XML file.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Make sure that the XML declaration statement is closed in the XML file.

KAVK37202-E

The version attribute does not exist in the xml declaration.

The version attribute is missing in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Make sure that the XML declaration statement contains the version attribute.

KAVK37203-E

Each item in the xml declaration must be separated with a space.

The items are not delimited by the space character in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Separate the items with the space character in the XML declaration statement.

KAVK37204-E

The version attribute specified in the xml declaration is invalid.

The specified version attribute is invalid in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the correct version attribute in the XML declaration statement.

KAVK37205-E

The version number in the xml declaration is invalid.

The version number is invalid in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the correct number for the version attribute in the XML declaration statement.

KAVK37206-E

The encoding attribute does not exist in the xml declaration.

The encoding attribute is missing in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Make sure that the XML declaration statement contains the encoding attribute.

KAVK37207-E

The encoding attribute specified in the xml declaration is invalid.

The specified encoding attribute is invalid in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the correct encoding attribute in the XML declaration statement.

KAVK37208-E

The standalone attribute does not exist in the xml declaration.

The standalone attribute is missing in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Make sure that the XML declaration statement contains the standalone attribute.

KAVK37209-E

The specified standalone attribute is invalid in the xml declaration.

The specified standalone attribute is invalid in the XML declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the correct standalone attribute in the XML declaration statement.

KAVK37210-E

The xml document declaration does not exist on the second line.

There is no document type declaration statement on the second line in the XML file.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Make sure that the XML file contains the XML declaration statement on the second line.

KAVK37211-E

The xml document declaration is not closed.

The document type declaration statement is not closed.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Make sure that the document type declaration statement is closed.

KAVK37212-E

item does not exist in the xml document declaration.

A required item is missing in the document type declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the indicated item in the document type declaration statement.

KAVK37213-E

Each item in the xml document declaration must be separated with a space.

The items are not delimited by the space character in the document type declaration statement.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Separate the items with the space character in the document type declaration statement.

KAVK37214-E

The start tag for the transaction list (*start-tag-for-transaction-list*) does not exist.

The start tag for the transaction list is missing in the XML file.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the start tag for the transaction list.

KAVK37215-E

The end tag for the transaction list (*end-tag-for-transaction-list*) does not exist.

The end tag for the transaction list is missing in the XML file.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the termination tag for the transaction list.

KAVK37216-E

The comment is not closed.

The comment is not closed in the XML file.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Close the comment correctly.

KAVK37217-E

An invalid string (--) exists in the comment.

The comment in the XML file contains an invalid character string (--).

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Do not use -- in comments.

KAVK37218-E

An invalid string (*invalid-character-string*) exists.

An invalid character string was detected.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Correct the invalid character string.

KAVK37219-E

The content of this tag (*start-tag*) does not exist.

The tag is missing required contents.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the missing contents in the tag.

KAVK37220-E

The content of this tag (*start-tag*) must be empty.

The tag must be empty, but instead a value was specified for it.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Delete the contents of the tag.

KAVK37221-E

The start tag (*start-tag*) does not exist.

The required start tag is missing.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the start tag.

KAVK37222-E

The end tag (*end-tag*) does not exist.

The required end tag is missing.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set the end tag.

KAVK37223-E

An invalid character (&) exists in the xml.

An ampersand (&) is used illegally in a data field in the XML document.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Replace the illegal & with &#x26;

KAVK37224-E

An invalid character (*invalid-character*) exists in the xml.

A data field in the XML document contains an invalid character.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

See [8.1.1 About specification in XML format](#), then replace the invalid character with the appropriate character string.

KAVK37225-E

The size of the content of this tag (*start-tag*) has exceeded *permitted-maximum-length-in-bytes* bytes.

The contents of the indicated tag exceed the permitted length in bytes.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set no more than the permitted number of characters in the tag.

KAVK37226-E

The value of the content of this tag (*start-tag*) is invalid. Specify a value between *permitted-minimum-length-in-bytes* and *permitted-maximum-length-in-bytes*.

The value specified in the tag is outside the permitted range.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set a value that is within the permitted range for this tag.

KAVK37227-E

The value of the content of this tag (*start-tag*) is not a real number.

The value specified in the tag is not an integer.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Set an integer in the tag.

KAVK37228-E

This tag (*start-tag*) cannot be processed.

There is an invalid tag that cannot be processed.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Delete the invalid tag.

KAVK37229-E

The specified scope name in this tag is invalid (*start-tag*).

The scope name specified in the tag is invalid.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Specify the correct scope name.

KAVK37230-E

The specified scope number in this tag is invalid (*start-tag*). Specify a scope number between *minimum-scope-number* and *maximum-scope-number*.

The scope number specified in the tag is invalid.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Specify the correct scope name, or set a scope number that is within the permitted range.

KAVK37231-E

The specified start scope already exists. (`scope number: scope-number`)

The start scope specified in the tag has already been defined.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Check and, if necessary, revise the definition of the start scope.

KAVK37232-E

The corresponding start scope is not defined. (`scope number: scope-number`)

No start scope that corresponds to the specified end scope has been defined.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Check and, if necessary, revise the scope definition.

KAVK37233-E

The specified end scope already exists. (`scope number: scope-number`)

The end scope specified in the tag has already been defined.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Check and, if necessary, revise the definition of the end scope.

KAVK37234-E

A semicolon (;) must not be used in a Cookie.

The <COOKIE> tag contains a semicolon (;).

(S)

Cancel the XML file read or write operation and perform other processing.

(O)

Delete the semicolon in the <COOKIE> tag.

KAVK37235-E

The data specified for the COOKIE tag is invalid.

The cookie specification is invalid.

(S)

Cancel the XML file read or write operation and perform other processing.

(O)

Correct the cookie specification.

KAVK37236-E

The data specified for the RESPONSE_PATTERN tag is invalid. (*error-detail*)

The <RESPONSE_PATTERN> tag contains invalid information.

(S)

Cancel the XML file read or write operation and perform other processing.

(O)

Correct the contents of the <RESPONSE_PATTERN> tag according to the information provided in parentheses in the message.

KAVK37237-E

An attempt to analyze the specified xml file has failed. (*file-name*)

An attempt to analyze the specified XML file failed.

(S)

Cancel the XML file read or write operation and perform other processing.

(O)

Check the KAVKnnnnn message that was output immediately before this message and take the action indicated in it.

KAVK37238-E

There are too many cookie tags.

There are too many <COOKIE> tags.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Check the specified <COOKIE> tag and reduce the number of <COOKIE> tags.

KAVK37239-E

The URL protocol identifier in the URL tag is invalid.

The URL protocol identifier is invalid in the <URL> tag.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Correct the URL protocol identifier in the <URL> tag.

KAVK37240-E

The corresponding end scope is not defined. (*scope number: scope-number*)

There is no end scope that corresponds to the specified start scope.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Check and, if necessary, revise the scope definition.

KAVK37241-E

This empty tag (*empty-tag*) must not be used.

An empty tag was specified illegally.

(S)

Cancels the XML file read or write operation and performs other processing.

(O)

Delete the empty tag and specify the tag correctly.

KAVK37242-E

A variable string is duplicated.

The variable character string specified in <VARIABLE_PART> tag in the specified Web transaction file duplicates the variable character string specified in another <VARIABLE_PART> tag defined in the same step.

(S)

Cancels the XML file read or write operation.

(O)

Review the variable character string so that the variable cannot be duplicated.

KAVK37243-E

There is no specified step identifier.

The step identifier specified in <TARGET_STEP_ID> tag in the specified Web transaction file is not defined in the step preceding this step.

(S)

Cancels the XML file read or write operation.

(O)

Specify the step identifier which is defined in the step preceding this step.

KAVK37244-E

A variable string is not included in URL, message body or cookie.

A variable character string specified in <VARIABLE_PART> tag in the specified Web transaction file is not included in URL, message body, or cookie.

(S)

Cancels the XML file read or write operation.

(O)

Specify the variable character string which is included in URL, message body, or cookie.

KAVK37300-E

Memory is insufficient.

Memory allocation failed during processing.

(S)

Terminates Web Recorder.

(O)

Terminate any unneeded applications, and then re-execute the command.

KAVK37301-E

An attempt to create a popup menu of a URL list has failed.

An attempt to create a pop-up menu of URLs failed.

(O)

Check to see if the pop-up menu of URLs is necessary. Also, make sure that there is no shortage in the system resources.

KAVK37302-E

An attempt to create a list to display the list of Web transaction names has failed.

An attempt to create a list for displaying Web transaction names failed.

(S)

When the message dialog box is closed, the system returns to the original window without opening the Select Web Transaction window.

(O)

Make sure that there is no shortage in the system resources.

KAVK37303-E

An attempt to display the list of available start scopes has failed.

An attempt to display a list of start scopes available for the specified step failed.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that there is no shortage in the system resources.

KAVK37304-E

An attempt to show the list of available end scopes has failed.

An attempt to display a list of end scopes available for the specified step failed.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that there is no shortage in the system resources.

KAVK37305-E

There are no available start scopes.

There was no available start scope for the specified step when an attempt was made to add a start scope.

(S)

Closing the message dialog box returns to the original window.

(O)

Check and, if necessary, revise the scope definition.

Delete the definition of an unneeded start scope.

KAVK37306-E

There are no available end scopes.

There was no available end scope for the specified step when an attempt was made to add an end scope.

(S)

Closing the message dialog box returns to the original window.

(O)

Check and, if necessary, revise the scope definition.

Make sure that the start scope corresponding to the set end scope has been defined correctly.

KAVK37400-W

Closing of the IE window on the main window will be canceled because it cannot be closed.

A page was opened in an IE window inside the Web Recorder (main) window. An attempt to close the IE window on that page was cancelled.

(S)

Cancels the IE window close operation and performs other processing.

(O)

Continue the operation as is because the IE window inside the Web Recorder (main) window cannot be closed.

KAVK37401-W

Closing of the IE window will be canceled. If you want to close this IE window, use the close button on the top right-hand corner.

A page was opened in a new IE window. An attempt to close the IE window on that page was cancelled.

(S)

Cancels the IE window close operation and performs other processing.

(O)

To close the new IE window, use the **Close** button in the upper right corner.

KAVK37402-E

The data from the IE window could not be acquired.

An attempt to acquire data that is collected automatically from the IE window failed.

(S)

Cancels acquisition of data from the IE window and performs other processing.

(O)

Check the *KAVKnnnnn* message that was output immediately before this message and take the action indicated in it.

KAVK37403-E

The size of the input value of the URL has exceeded *permitted-maximum-length-in-bytes* bytes.

The URL acquired automatically from the IE window exceeds the permitted length in bytes.

(S)

If this message was displayed during an IE window operation, the system cancels acquisition of data from the IE window and performs other processing.

(O)

Check and, if necessary, revise the target URL or entered URL.

KAVK37404-E

The URL that was input is invalid.

The URL acquired automatically from the IE window is invalid.

- (S) Cancels acquisition of data from the IE window and performs other processing.
- (O) Check and, if necessary, revise the target URL.

KAVK37405-E

No URL has been input.

The URL acquired automatically from the IE window is empty.

No URL has been set in the Properties window.

- (S) If this message was displayed during an IE window operation, the system cancels automatic data collection from the IE window, then performs other processing.
If this message was displayed in the Properties window, closing the message dialog box returns to the original window.
- (O) Make sure that the URL gets entered.

KAVK37406-E

The size of the input value of the frame name has exceeded *permitted-maximum-length-in-bytes* bytes.

The frame name acquired automatically from the IE window exceeds the permitted length in bytes.

- (S) Cancels acquisition of data from the IE window and performs other processing.
- (O) Check and, if necessary, revise the frame name in the target page, or the entered frame name.

KAVK37407-E

The frame name that was input is invalid.

The frame name acquired automatically from the IE window is invalid.

- (S) Cancels acquisition of data from the IE window and performs other processing.
- (O) Check and, if necessary, revise the target frame name. If necessary, enter the frame name by editing the step information.

KAVK37408-E

The size of the input value of the post data has exceeded *permitted-maximum-length-in-bytes* bytes.

The message body acquired automatically from the IE window exceeds the permitted length in bytes.

(S)

Cancels data processing from the IE window and performs other processing.

(O)

Check and, if necessary, revise the message body of the request sent from the IE window.

KAVK37409-E

The post data that was input is invalid.

The message body acquired automatically from the IE window is invalid.

(S)

Cancels data processing from the IE window and performs other processing.

(O)

Check and, if necessary, revise the message body of the request sent from the IE window.

KAVK37410-E

The size of the input value of the content type has exceeded *permitted-maximum-length-in-bytes* bytes.

The content type acquired automatically from the IE window exceeds the permitted length in bytes.

(S)

Cancels data processing from the IE window and performs other processing.

(O)

Check and, if necessary, revise the content type in the request sent from the IE window.

KAVK37411-E

An invalid content type was input.

The content type acquired automatically from the IE window is invalid.

(S)

Cancels data processing from the IE window and performs other processing.

(O)

Check and, if necessary, revise the content type in the request sent from the IE window.

KAVK37412-E

No separator (boundary) is input.

The content type acquired automatically from the IE window is in multi-part format with no boundary.

(S)

If this message was displayed during an IE window operation, the system cancels automatic data collection from the IE window.

(O)

Check and, if necessary, revise the boundary of the content type for the request that is sent from the IE window.

KAVK37413-E

The size of the input value of the separator (boundary) has exceeded *permitted-maximum-length-in-bytes* bytes.

The content type acquired automatically from the IE window is in multi-part format and its boundary exceeds the permitted length in bytes.

(S)

If this message was displayed during an IE window operation, the system cancels automatic data collection from the IE window.

(O)

Check and, if necessary, revise the boundary of the content type for the request that is sent from the IE window.

KAVK37500-E

An attempt to insert the step has failed.

An attempt to insert step information failed.

(S)

Cancels the step information insertion processing, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37501-E

An attempt to add the step has failed.

An attempt to add step information failed.

(S)

Cancels the step information addition processing and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37502-E

An attempt to edit the step has failed.

An attempt to edit step information failed.

(S)

Cancels the step information editing and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37503-E

An attempt to create the step has failed.

An attempt to create new step information failed.

(S)

Cancels the step information insertion or addition processing, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37504-E

An irreparable error occurred in the processing for adding the step. Active data will be lost.

An attempt to add step information failed, resulting in inconsistency between the information displayed in the list of URLs and the information that is retained internally.

(S)

Cancels the step information addition processing, clears the data in the Web Recorder (main) window as well as the internal data, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37505-E

An irreparable error occurred in the processing for deleting the step. Active data will be lost.

An attempt to delete step information failed, resulting in inconsistency between the information displayed in the list of URLs and the information that is retained internally.

(S)

Cancels the step information deletion processing, clears the data in the Web Recorder (main) window as well as the internal data, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37506-E

An irreparable error occurred in the processing for editing the step. Active data will be lost.

An attempt to edit step information failed, resulting in inconsistency between the information displayed in the URL list and the information that is retained internally.

(S)

Cancels the step information editing, clears data in the Web Recorder (main) window as well as the internal data, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37507-E

An attempt to add the start scope has failed.

An attempt to add start scope information failed.

(S)

Cancels addition of the start scope information and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37508-E

An attempt to add the end scope has failed.

An attempt to add end scope information failed.

(S)

Cancels the addition of the end scope information and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37509-E

An attempt to delete the start scope has failed.

An attempt to delete start scope information failed.

(S)

Cancels the start scope deletion processing and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37510-E

An attempt to delete the end scope has failed.

An attempt to delete end scope information failed.

(S)

Cancels the end scope deletion processing and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37511-E

An attempt to delete the corresponding scope has failed.

An attempt to delete scope information corresponding to the deleted scope failed.

- (S) Cancels deletion of the scope information corresponding to the deleted scope, and performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37512-E

An irreparable error occurred in the processing for adding the start scope. Active data will be lost.

An attempt to add start scope information failed, resulting in inconsistency between the information displayed in the list of URLs and the information that is retained internally.

- (S) Cancels addition of the start scope information, clears data in the Web Recorder (main) window as well as the internal data, and then performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37513-E

An irreparable error occurred in the processing for adding the end scope. Active data will be lost.

An attempt to add end scope information failed, resulting in inconsistency between the information displayed in the list of URLs and the information that is retained internally.

- (S) Cancels addition of the end scope information, clears data in the Web Recorder (main) window as well as the internal data, and then performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37514-E

An irreparable error occurred in the processing for deleting the start scope. Active data will be lost.

An attempt to delete start scope information failed, resulting in inconsistency between the information displayed in the list of URLs and the information that is retained internally.

- (S) Cancels deletion of the start scope information, clears data in the Web Recorder (main) window as well as the internal data, and then performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37515-E

An irreparable error occurred in the processing for deleting the end scope. Active data will be lost.

An attempt to delete end scope information failed, resulting in inconsistency between the information displayed in the list of URLs and the information that is retained internally.

(S)

Cancels deletion of the end scope information, clears data in the Web Recorder (main) window as well as the internal data, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37516-E

An irreparable error occurred in the processing for deleting the corresponding scope. Active data will be lost.

An attempt to delete the scope information for the deleted scope has failed, causing an inconsistency between the display of the URL list and internal information.

(S)

Cancels deletion of the scope information that corresponds to the deleted scope, clears data in the Web Recorder (main) window as well as the internal data, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37517-E

A scope is selected in the URL list. A step must be selected.

A command for processing a step was executed, but a scope was selected in the list of URLs.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a URL is selected in the list of URLs.

KAVK37518-E

A step is selected in the URL list. A scope must be selected.

A command for processing a scope was executed, but a step was selected in the list of URLs.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a scope is selected in the list of URLs.

KAVK37519-E

No item is selected in the URL list. A scope must be selected.

A command for processing a scope was executed, but nothing was selected in the list of URLs.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a scope is selected in the list of URLs.

KAVK37520-E

No item is selected in the URL list. A step must be selected.

A command for processing a step was executed, but nothing was selected in the list of URLs.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a step is selected in the list of URLs.

KAVK37521-E

A scope must be selected in the URL list.

A command for processing a scope was executed, but an invalid location was selected in the list of URLs.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a scope is selected in the list of URLs.

KAVK37522-E

A step must be selected in the URL list.

A command for processing a step was executed, but an invalid location was selected in the list of URLs.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a step is selected in the list of URLs.

KAVK37523-E

The step data does not exist.

The Properties window was called, but the selected step information was empty.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a step is selected in the list of URLs.

KAVK37524-E

The separator (boundary) is not input.

In the Properties window, on the **Request Info** page, **POST** was specified for the method, **Multipart** was selected for the content type, but no boundary was entered.

(S)

Closing the message dialog box returns to the original window.

(O)

Verify the items that were selected for the method and content type.

Make sure that the separators have been entered.

KAVK37525-E

The content-type is not input.

In the Properties window, on the **Request Info** page, **POST** was specified for the method, **Other** was selected for the content type, but nothing was entered in any other edit box.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the items selected for the method and content type.

Make sure that other required information has been entered.

KAVK37526-E

The message-body is not input.

In the Properties window, on the **Request Info** page, **POST** was specified for the method, but no message body was entered.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the items selected for the method and content type.

Make sure that the message body has been entered.

KAVK37527-E

The Web authentication user name is not input.

In the Properties window, on the **Web Authentication** page, **Web authentication** check box was selected, but no Web authentication user name was entered.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the selection of **Web authentication** check box.

Make sure that the Web authentication user name is entered.

KAVK37528-E

The URL protocol identifier is invalid.

In the Properties window, on the **Page Info** page, an invalid protocol identifier was specified for the URL entered in **URL**.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the protocol identifier of the entered URL.

KAVK37602-E

The host name is not input.

In the Set Web Transaction Conditions window, on the **Default Proxy** page, **Use proxy** check box was selected, but no proxy host name has been entered.

In the Properties window, on the **Proxy** page, **Use this setting value** was selected, but no proxy host name has been entered.

(S)

Closing the message dialog box returns to the original window.

(O)

In the case of the Set Web Transaction Conditions window, on the **Default Proxy** page, make sure that **Use proxy** check box is selected and a proxy host name is entered.

In the case of the Properties window, on the **Proxy** page, check the selected proxy settings and make sure that the proxy host name is entered.

KAVK37603-E

The port number is invalid. Specify a port number between 1 and 65535.

In the Set Web Transaction Conditions window, on the **Default Proxy** page, the proxy port number is invalid.

In the Properties window, on the **Proxy** page, the proxy port number is invalid.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the proxy port number setting.

KAVK37604-E

The proxy user name is not input.

In the Set Web Transaction Conditions window or in the Properties window, on the **Default Proxy** page or on the **Proxy** page, **Proxy authentication** check box was selected, but no proxy user name has been entered.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that **Proxy authentication** check box is selected and that a proxy user name has been entered.

KAVK37605-E

The client certificate file name is not input.

In the Set Web Transaction Conditions window, on the **SSL authentication** page, **Client authentication** check box was selected, but no client certificate file name has been entered.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that **Client authentication** check box is selected and a client certificate file name has been entered.

KAVK37606-E

The port number is not input.

In the Set Web Transaction Conditions window or the Properties window, on the **Default Proxy** page or on the **Proxy** page, no proxy port number has been entered.

- (S) Closing the message dialog box returns to the original window.
- (O) In the case of the Set Web Transaction Conditions window, on the **Default Proxy** page, make sure that **Use proxy** check box has been selected and a proxy port number has been entered.
In the case of the Properties window, on the **Proxy** page, check the selected proxy settings and make sure that a proxy port number has been entered.

KAVK37700-E

An attempt to parse response determination information has failed.

An attempt to analyze response determination information failed.

- (S) When the message dialog box is closed, the system displays the **Response Determination** page.
- (O) Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK37701-E

An error occurred during response determination information processing.

An attempt to display response determination information failed.

(S)
When the message dialog box is closed, the system displays the **Response Determination** page.

(O)
Make sure that there is no shortage in the system resources.

KAVK37702-E

An invalid character exists in the operator position.

In the response determination information, an invalid character is specified at the location where an operator should be specified.

(S)
Cancels analysis of response determination information and performs other processing.

(O)
Check and, if necessary, revise the operator in the response determination information.

KAVK37703-E

The number of closed braces [}] is insufficient.

In the response determination information, there are not enough right curly brackets [}] or there are too many left curly brackets [{].

(S)
Cancels analysis of response determination information and performs other processing.

(O)
Check and, if necessary, revise the specification of curly brackets [{ }] in the response determination information.

KAVK37704-E

An invalid character or an invalid white space exists.

The response determination information contains an invalid character or space.

(S)
Cancels analysis of response determination information and performs other processing.

(O)
Make sure that the response determination information contains no invalid characters or spaces.

KAVK37705-E

There are too many closed parentheses [)].

In the response determination information, there are too many right parentheses [)] or not enough left parentheses [(].

(S)
Cancels analysis of response determination information and performs other processing.

(O)
Check and, if necessary, revise the specification of parentheses [()] in the response determination information.

KAVK37706-E

The number of closed parentheses [)] is insufficient.

In the response determination information, there are not enough right parentheses [)] or too many left parentheses [(].

(S)

Cancels analysis of response determination information and performs other processing.

(O)

Check and, if necessary, revise the specification of parentheses[()] in the response determination information.

KAVK37707-E

The number of terms in the logical expression is insufficient.

There are not enough items in the response determination information.

(S)

Cancels analysis of response determination information and performs other processing.

(O)

Check and, if necessary, revise the response determination information.

KAVK37708-E

An attempt to create response determination information has failed.

An attempt to create response determination information from a list of response determination conditions failed.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the *KAVKnnnnn* message that was output immediately before this message and take the action indicated in it.

KAVK37709-E

This item can not be deleted.

An attempt was made to delete an item that cannot be deleted from the list of response determination conditions.

Alternatively, the first line of the list of response determination conditions was selected, and then the Delete button was clicked.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that the first row is not selected in the list of response determination conditions.

KAVK37711-E

An irreparable error occurred during processing for deleting an item in the list. All items in the list will be lost.

An attempt to delete an item from the list of response determination conditions failed, resulting in an invalid display of the list.

- (S) Cancels item deletion processing on the list of response determination conditions, clears the list of response determination conditions, and then performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37712-E

An irreparable error occurred during processing for changing an item in the list. All items in the list will be lost.

An attempt to change an item in the list of response determination conditions failed, resulting in an invalid display of the list.

- (S) Cancels item change processing on the list of response determination conditions, clears the list of response determination conditions, then performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37713-E

An irreparable error occurred during processing for an item in the list. All items in the list will be lost.

An attempt to manipulate an item in the list of response determination conditions failed, resulting in an invalid display of the list.

- (S) Cancels item manipulation on the list of response determination conditions, clears the list, and then performs other processing.
- (O) Make sure that there is no shortage in the system resources.

KAVK37714-E

No item in the list is selected.

The **Modify** or **Move** button was pressed, but no item was selected in the list of response determination conditions.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that an item to be manipulated is selected in the list of response determination conditions.

KAVK37715-E

This item can not be changed.

An attempt was made to change a prohibited item in the list of response determination conditions.

The first row was selected and then the **Modify** or **Move** button was pressed.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that an item to be manipulated is selected in the list of response determination conditions.

KAVK37718-E

The rank of this item cannot be raised any further.

In the list of response determination conditions, an attempt was made to raise the rank of an item that cannot be raised any higher.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that the correct item whose rank is to be raised is selected in the list of response determination conditions.

KAVK37719-E

The rank of this item cannot be lowered any further.

In the list of response determination conditions, an attempt was made to lower the rank of an item that cannot be lowered any more.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that the correct item whose rank is to be lowered is selected in the list of response determination conditions.

KAVK37720-E

The string of a condition is not input.

The **Add** or the **Modify** button was pressed, but no character string was entered for the condition.

- (S) Closing the message dialog box returns to the original window.
- (O) Make sure that a character string is entered for the condition.

KAVK37721-E

The conjunction of a condition is not selected.

The **Add** or the **Modify** button was pressed, but no conjunction was selected for the condition.

- (S) Closing the message dialog box returns to the original window.

(O)

Make sure that a conjunction for the condition is selected.

KAVK37722-E

The judgment of a condition is not selected.

The **Add** or the **Modify** button was pressed, but no determination was selected for the condition.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that a determination for the condition is selected.

KAVK37723-E

An invalid parenthesis exists.

In the response determination information, a single item is enclosed in parentheses (()).

(S)

Cancels analysis of the response determination information and performs other processing.

(O)

Make sure that no single item is enclosed in parentheses in the response determination information.

KAVK37724-E

An attempt to add a condition to the list has failed.

An attempt to add an item to the list of response determination conditions failed.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that there is no shortage in the system resources.

KAVK37725-E

An attempt to delete a condition from the list has failed.

An attempt to delete an item from the list of response determination conditions failed.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that there is no shortage in the system resources.

KAVK37726-E

An irreparable error occurred in the processing for deleting a condition in the list. All items in the list will be lost.

An attempt to delete an item in the list of response determination conditions failed, resulting in an invalid display of the list.

(S) Cancels item deletion on the list of response determination conditions, clears the list, and then performs other processing.

(O) Make sure that there is no shortage in the system resources.

KAVK37727-E

An attempt to change a condition in the list has failed.

An attempt to change an item in the list of response determination conditions failed.

(S) Closing the message dialog box returns to the original window.

(O) Make sure that there is no shortage in the system resources.

KAVK37728-E

An attempt to process a condition in the list has failed.

An attempt to manipulate an item in the list of response determination conditions failed.

(S) Closing the message dialog box returns to the original window.

(O) Make sure that there is no shortage in the system resources.

KAVK37729-E

An irreparable error occurred in the processing for a condition in the list. All items in the list will be lost.

An attempt to manipulate an item in the list of response determination conditions failed, resulting in an invalid display of the list.

(S) Cancels item manipulation on the list of response determination conditions, clears the list, and then performs other processing.

(O) Make sure that there is no shortage in the system resources.

KAVK37730-E

An irreparable error occurred in the processing for changing a condition in the list. All items in the list will be lost.

An attempt to change an item in the list of response determination conditions failed, resulting in an invalid display of the list.

(S)

Cancels changing the item in the list of response determination conditions, clears the list, and then performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK37731-E

The size of the input value of the response determination information has exceeded *permitted-maximum-value* bytes.

The response determination information exceeded the permitted size in bytes.

(S)

Closing the message dialog box returns to the original window.

(O)

Eliminate items from the list of response determination conditions.

KAVK37732-E

An empty string is specified.

A null character string was specified for a condition in the response determination information.

(S)

Cancels analysis of the response determination information and performs other processing.

(O)

Make sure that a null character string is not specified.

KAVK37733-E

This item of the list cannot be moved there.

An attempt was made to move up the second row of the list of response determination conditions, or an attempt was made to move down the last row.

(S)

Closing the message dialog box returns to the original window.

(O)

Make sure that the item to be moved up or down is selected from the list of response determination conditions.

KAVK37734-E

A specified string includes a curly bracket ({,}).

An attempt was made to add or change a condition, but the character string for the condition contains curly brackets ({,}).

(S)

Closing the message dialog box returns to the original window.

(O)

Delete the curly brackets because a character string for a condition cannot contain curly brackets.

KAVK37800-I

The specified Web transaction name already exists. Do you want to overwrite it?

Asks whether or not the existing file is to be overwritten when a Web transaction with the specified name has already been defined in the target Web transaction file.

(S)

When the **Yes** button is selected, the system overwrites the Web transaction.

When the **No** button is selected, the system cancels the overwrite processing.

KAVK37801-I

The selected step will be deleted. Do you want to continue?

Asks whether or not the selected step information is to be deleted.

(S)

When the **Yes** button is selected, the system deletes the selected step information.

When the **No** button is selected, the system cancels the step deletion processing.

KAVK37802-I

The scope (`START(END) SCOPE scope-number`) will be deleted.

Reports that scope information will be deleted.

(S)

When the dialog box is closed, the system resumes processing.

KAVK37803-I

The scope (`START(END) SCOPE scope-number`) will be deleted. Do you want to continue?

Asks for confirmation that the scope information is to be deleted.

(S)

When the **Yes** button is selected, the system deletes the specified scope information.

When the **No** button is selected, the system cancels the scope deletion processing.

KAVK37804-I

Do you want to delete the corresponding scope?

Asks for confirmation that the scope information corresponding to the deleted scope information is to be deleted.

(S)

When the **Yes** button is selected, the system deletes the corresponding scope information.

When the **No** button is selected, the system cancels deletion of the corresponding scope information.

KAVK37805-I

END(*START*) *scope-name* corresponding to *START*(END) *scope-name* does not exist.

Reports that there is no corresponding scope.

(S)

When the dialog box is closed, the system resumes processing.

KAVK37806-I

END *scope-name* exists before *START* *scope-name*. Correct this problem.

Reports that the start and end scopes have been reversed.

(S)

When the dialog box is closed, the system resumes processing.

KAVK37807-I

The processing for checking the scope has finished.

Reports that scope checking has been completed.

(S)

When the dialog box is closed, the system returns to the original window.

KAVK37808-I

Web transaction data being edited now will be deleted from the Web transaction file. Do you want to continue?

Asks for confirmation that the Web transaction that is currently being edited is to be deleted from the Web transaction file.

(S)

When the **Yes** button is selected, the system deletes from the Web transaction file the current Web transaction that is being edited.

When the **No** button is selected, the system cancels deletion of the Web transaction.

KAVK37809-I

Web transaction data being edited now will be discarded. Do you want to continue?

Asks for confirmation that the processing is to be continued and that the Web transaction currently being edited is to be discarded.

(S)

When the **Yes** button is selected, the system resumes processing.

When the **No** button is selected, the system cancels processing and returns to the original window.

KAVK37850-E

The variable string at the time of the record is not input.

When you click the **OK** or **Apply** button in the Conditions of Variable String window or switch tabs, the **Variable string at the time of the record** is not specified.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Variable string at the time of the record**.

KAVK37851-E

The command is not input.

After you select the **From Command** in the Conditions of Variable String window, you click the **OK** or **Apply** button or switch tabs without specifying the **Command**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Command**.

KAVK37852-E

The step ID is not selected.

When you click the **OK** button in the Conditions of Substitute String window, you do not select the **Step ID**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Step ID**.

KAVK37853-E

The element name is not input.

After you select the **From HTML** in the Conditions of Substitute String window, you click the **OK** button without specifying the **Element name**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Element name**.

KAVK37854-E

The attribute name is not input.

In the Conditions of Substitute String window after you select the **From HTML** and **Attribute** in the **Where to include substitute string** section, you click the **OK** button without specifying the **Attribute name**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Attribute name**.

KAVK37855-E

The HTTP header name is not input.

After you select the **From HTTP header** in the Conditions of Substitute String window, you click the **OK** button without specifying the **Header name**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Header name**.

KAVK37856-E

The string just before and/or string just after is not input.

After you select the **String to exclude from substitute string** check box in the Conditions of Substitute String window, you click the **OK** button without specifying the **String just before** and/or **String just after**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **String just before** and/or **String just after**.

KAVK37857-E

The attribute value or element content is not input.

When you click the **OK** button in the Filtering Conditions window, you do not specify the **Attribute** or **Content**.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Attribute** or **Content**.

KAVK37858-E

The substitute target is not set.

When you click the **OK** or **Apply** button in the Conditions of Variable String window, you do not specify substitute strings.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify substitute strings.

KAVK37859-E

A variable string is duplicated.

When you click the **OK** or **Apply** button or switch the tabs in the Conditions of Variable String window, the variable string specified in the **Variable string at the time of the record** is already set.

(S)

Closing the message dialog box returns to the original window.

(O)

The variable string specified in the **Variable string at the time of the record** must be unique.

KAVK37860-E

A variable string is not included in URL, message body or cookie.

When you click the **OK** or **Apply** button in the Conditions of Variable String window, the variable string specified in the **Variable string at the time of the record** is not included in recorded URL, message body or cookie.

(S)

Closing the message dialog box returns to the original window.

(O)

The variable string specified in the **Variable string at the time of the record** must be included in recorded URL, message body or cookie.

KAVK37861-E

The prefix of step ID is not specified.

After you select the **Give a step ID automatically** check box in the Create New Web Transaction windows, you click the **OK** button without specifying the **Prefix** of step ID.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Prefix**.

KAVK37862-E

An invalid character exists in step ID.

- When you click the **OK** or **Apply** button or switch tabs in the **Page Info** page in the Properties window, an invalid character is included in the specified step ID.
- When you click the **OK** button in the Select Web Transaction window, an invalid character is included in the step ID in the specified Web transaction.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the step ID using alphanumeric characters, hyphen, underscore, and space.

KAVK37863-E

An invalid character exists in prefix of step ID.

When you select the **Give a step ID automatically** check box and then click the **OK** button in the Create New Web Transaction window, the **Prefix** includes invalid character.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Prefix** using alphanumeric characters, hyphen, underscore, and space.

KAVK37864-E

A variable string does not exist.

When you click the **Import** button in the Conditions of Variable String window, you do not specify any variable strings.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify variable strings.

KAVK37865-E

A substitute string does not exist.

When you click the **Import** button in the Conditions of Substitute String window, you do not specify any substitute strings.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify substitute strings.

KAVK37866-E

A step ID does not exist.

When you click the **Add** button in the **Substitute String** page in the Conditions of Variable String window, you do not specify any step IDs in the Web transaction.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify step IDs.

KAVK37867-E

The step ID does not exist in the Web transaction.

- When you click the **Save** or **Save As** button from **File** menu in the Web transaction (main) window, the step ID specified in the Conditions of Substitute String window does not exist in the Web transaction.
- When you click the **OK** button in the Select Web Transaction window, the step ID specified in the Conditions of Substitute String window does not exist in the Web transaction.

- (S) Closing the message dialog box returns to the original window.
- (O) Specify the step ID that exists in the Web transaction in the Conditions of Substitute String window.

KAVK37868-W

Output the acquired HTML and HTTP header in a file. check box is selected, but there is no step information to be output. Do you want to continue?

When you select the **Output the acquired HTML and HTTP header in a file. check box** in the Set Web Transaction Conditions window and choose **Save** or **Save As** from **File** menu in the Web transaction (main) window, no step ID exists in the specified Web transaction.

- (S) If you click the **Yes** button, the system stores the Web transaction information to a file.
If you click the **No** button, the system cancels to store the Web transaction information and returns to the original window.
- (O) Specify the step ID in the step where the acquired HTML and HTTP header is to be output.

KAVK37869-E

A step ID is duplicated.

When you enter a step ID and then click the **OK** button or **Apply** button or switch tabs in the **Page Info** page in the Properties window, the same step ID is set in other step.

- (S) Closing the message dialog box returns to the original window.
- (O) Specify a unique step ID.

KAVK37870-E

An invalid character exists in attribute name.

- When you select the **From HTML**, select the **Attribute in the Where to include substitute string** section, and click the **OK** button in the Conditions of Substitute String window, an invalid character exists in the **Attribute name**.
- When you click the **OK** button in the Select Web Transaction window, an invalid character exists in the attribute name.

(S)

Closing the message dialog box returns to the original window.

(O)

Do not use the invalid character to specify attribute name. Do not use an equal sign (=) to specify the **Attribute name**.

KAVK37873-E

The format of attribute is invalid.

- When you select the **Attribute** and click the **OK** button in the Filtering Conditions window, the format of the specified attribute is invalid.
- When you click the **OK** button in the Select Web Transaction window, the format of the specified attribute is invalid.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the **Attribute** in the *element-name=element-value* format.

KAVK37874-E

The tag which is necessary for a (*tag-name*) tag is not specified.

When you click the **OK** button in the Select Web Transaction window, the tag which is necessary for this tag is not specified.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the tag which is necessary for this tag.

KAVK37875-E

The value to specify the nth element to use as a substitute string when there are multiple matched elements is invalid. Specify the value in the range from 1 to 1023.

When you click the **OK** button in the Conditions of Substitute String window, the specified value of the **When there are multiple matched elements, Use nth match** is invalid.

(S)

Closing the message dialog box returns to the original window.

(O)

Check the value of the **When there are multiple matched elements, Use nth match**.

KAVK37876-E

An error occurred while navigating of the page.

An error occurred while navigating of the page.

(S)

Closing the message dialog box returns to the original window.

(O)

Check whether the specified URL is correct.

KAVK37877-E

It was not possible to enable the parameters of the Web Recorder action condition definition file.

Parameters=parameter-information

It was not possible to enable the parameters of the Web Recorder action condition definition file.

(S)

Continues subsequent processing.

(O)

Check the *KAVKnnnnn-Z* message that was output immediately before this message and take the action indicated in it.

nnnnn indicates a message serial number. *Z* indicates a message type.

KAVK38001-E

An attempt to start IE Recorder has failed.

An attempt to start IE Recorder has failed.

(S)

Does not start IE Recorder.

(O)

Check the *KAVKnnnnn* message that was output immediately before this message and take the action indicated in it.

KAVK38002-E

IE Recorder has ended abnormally.

IE Recorder has ended abnormally.

(S)

Terminates IE Recorder.

(O)

Check the *KAVKnnnnn* message that was output immediately before this message and take the action indicated in it.

KAVK38003-E

An attempt to initialize the Hitachi Network Objectplaza Trace Library (HNTRLib2) has failed.

The Hitachi Network Objectplaza Trace Library (HNTRLib2) is not available.

(S)
Terminates IE Recorder.

(O)
Contact the system administrator.

KAVK38004-E

IE Recorder is already running.

The multiple instance of the IE Recorder cannot be open.

(S)
Does not start IE Recorder.

(O)
Use the already running IE Recorder.

KAVK38100-E

The definition of the IE Recorder action condition definition file is invalid. (`section=section-name, key=key-name`)

The definition of the IE Recorder action condition definition file is invalid.

(S)
Uses the default value to continue processing.

(O)
Check whether the definition of the IE Recorder action condition definition file is invalid. Moreover, check whether using the default value does not prevent the performance monitoring.

KAVK38101-E

An attempt to read the IE Recorder action condition definition file has failed.

The IE Recorder action condition definition file is not found, or is not opened due to the file access permission.

(S)
Uses the default value to continue processing.

(O)
Make sure that the IE Recorder action condition definition file has been placed in the specified folder. Check the file access permissions.

KAVK38102-E

An attempt to read the IE scenario file has failed. (`file name=file-name`)

IE scenario data cannot be read from the IE scenario file.

(S)
Cancels reading the IE Scenario file but continues to proceed other processing.

(O)

Check the IE Scenario file access permissions.

KAVK38103-E

An attempt to write the IE scenario file has failed. (*file name=file-name*)

IE scenario data cannot be written to the IE scenario file.

(S)

Cancels writing the IE Scenario file but continues to proceed other processing.

(O)

Check the IE Scenario file access permissions. Moreover, check whether the IE scenario file is read-only.

KAVK38104-E

An irreparable error occurred while processing IE scenario data. The IE scenario data was lost.

An irreparable error occurred while processing IE scenario data.

(S)

Discards the IE scenario data and the IE Recorder returns to its initial state.

(O)

Make sure that there is no shortage in the system resources.

KAVK38108-E

You do not have access permissions for the selected file. (*file name=file-name*)

You do not have access permissions for the selected file.

(S)

Cancels the file operation and performs other processing.

(O)

Check the specified file access permissions.

KAVK38113-E

An attempt to save the specified IE scenario file has failed. (*file name=file-name*)

An attempt to save the specified IE scenario file has failed because an error occurred during the writing process.

(S)

Cancels the IE Scenario file save operation and performs other processing.

(O)

Check the *KAVKnnnnn* message that was output immediately before this message and take the action indicated in it.

KAVK38115-W

The IE scenario file name must be no more than *permitted-maximum-length-in-bytes* characters.

The specified IE scenario file name exceeded the permitted maximum length in bytes characters.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the IE scenario file name so that its length is within the permitted range.

KAVK38116-E

An attempt to open the version dialog box has failed.

An attempt to open the version dialog box has failed. The files needed for opening the version dialog box may have been damaged.

(S)

Cancels to open the version dialog box and performs other processing.

(O)

Check whether an error occurred in the file system.

KAVK38117-E

Measurement conditions could not be registered because Agent Collector is running.

Measurement conditions could not be registered in the measurement condition registration file because Agent Collector is running.

(S)

Closing the message dialog box returns to the original window.

(O)

When you register the measurement conditions in the measurement condition registration file, stop the Agent Collector service. If you cannot stop the Agent Collector service, register measurement conditions on the Web Console.

KAVK38118-E

The measurement condition registration file could not be opened because Agent Collector is running.

The measurement condition registration file could not be opened because Agent Collector is running.

(S)

Closing the message dialog box returns to the original window.

(O)

When you operate the measurement condition registration file, stop the Agent Collector service.

KAVK38119-W

This IE scenario file will not be measured if it is saved in this folder. Do you want to continue?

If you save the IE scenario file in the folders other than `iescena` folder, the IE scenario file will not be measured.

(S)

If you click the **Yes** button, the system stores the IE scenario file in the folder.

If you click the **No** button, returns to the original window.

(O)

Check the destination folder to save the IE scenario file.

KAVK38120-I

The measurement condition has been registered successfully.

The measurement condition has been registered successfully.

(S)

Closing the message dialog box returns to the original window.

KAVK38121-E

Registration of measurement conditions has failed.

Registration of measurement condition has failed.

(S)

Cancels the simplified registration of measurement condition.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

Check whether the IE recorder can access `installation-folder\agtv\probe\tmp` folder.

KAVK38122-E

The measurement condition registration file could not be opened.

The measurement condition registration file could not be opened.

(S)

Cancels opening the measurement condition registration file.

(O)

Check the specified file access permissions. Moreover, check whether you can use the notepad.

KAVK38123-E

An attempt to load the measurement condition registration file has failed.

An attempt to load the measurement condition registration file has failed.

(S)

Cancels the simplified registration of measurement condition.

(O)

Check the measurement condition registration file for any specification format error.
Check the file access permissions.

KAVK38124-E

A measurement condition registration file was not found.

A measurement condition registration file was not found.

(S)

Cancel the simplified registration of measurement condition, and cancel editing the measurement condition registration file.

(O)

Create a measurement condition registration file correctly.

KAVK38200-E

The IE scenario file is invalid.

The IE scenario file has invalid data.

(S)

Initialize the IE Recorder.

(O)

Use the IE Recorder to recreate the IE scenario file.

KAVK38300-E

Reservation of memory has failed.

Reservation of memory has failed.

(S)

Terminate the IE Recorder.

(O)

Terminate an unneeded application and then re-execute.

KAVK38302-W

The scope name includes an invalid character. A comma or double quotation mark cannot be specified.

A comma or double quotation mark cannot be specified for the scope name.

(S)

Closing the message dialog box returns to the original window.

(O)

Delete the comma and/or double quotation mark from the scope name.

KAVK38303-W

The scope name exceeded *permitted-maximum-length-in-bytes* bytes.

The scope name exceeds the permitted maximum length in bytes.

(S)

Closing the message dialog box returns to the original window.

(O)

Specify the scope name so that its length is within the permitted range.

KAVK38304-W

The scope name is not specified.

The null character is specified for the scope name.

(S)

Closing the message dialog box returns to the original window.

(O)

Check whether the null character is specified for the scope name.

KAVK38500-E

An irreparable error occurred while operation information was being deleted. Active data was lost.

The deletion of the IE scenario data has failed.

(S)

Cancels deleting the IE scenario, clears the data in the IE Recorder (main) window as well as the internal data, and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK38501-E

An attempt to set the start scope has failed.

An attempt to set the start scope has failed.

(S)

Cancels setting the start scope and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK38502-E

An attempt to set the end scope has failed.

An attempt to set the end scope has failed.

(S)
Cancels setting the end scope and performs other processing.

(O)
Make sure that there is no shortage in the system resources.

KAVK38504-E

An irreparable error occurred during processing to set the start scope. Active data was lost.

Setting the start scope has failed.

(S)
Cancels setting the start scope, clears the data in the IE Recorder (main) window as well as the internal data, and performs other processing.

(O)
Make sure that there is no shortage in the system resources.

KAVK38505-E

An irreparable error occurred during processing to set the end scope. Active data was lost.

Setting the end scope has failed.

(S)
Cancels setting the end scope, clears the data in the IE Recorder (main) window as well as the internal data, and performs other processing.

(O)
Make sure that there is no shortage in the system resources.

KAVK38506-E

An irreparable error occurred during processing to delete scope settings. Active data was lost.

Deleting the scope setting has failed.

(S)
Cancels deleting the scope setting, clears the data in the IE Recorder (main) window as well as the internal data, and performs other processing.

(O)
Make sure that there is no shortage in the system resources.

KAVK38507-E

An attempt to get operation settings data has failed. Active data was lost.

An attempt to get operation settings data has failed.

(S)
Cancels getting the operation settings, clears the data in the IE Recorder (main) window as well as the internal data, and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK38508-E

An attempt to set scope information has failed. Active data was lost.

An attempt to set scope information has failed.

(S)

Clears the data in the IE Recorder (main) window as well as the internal data, and performs other processing.

(O)

Make sure that there is no shortage in the system resources.

KAVK38601-E

The Internet Options window of Internet Explorer could not be opened.

An error occurred when the Internet Options window of the Internet Explorer was opened.

(S)

Closing the message dialog box returns to the original window.

(O)

Check whether you can open the Internet Options window of the Internet Explorer.

KAVK38602-E

An error occurred while recording operations. Recording will be canceled.

An error occurred while recording operations.

(S)

Cancels recording operations.

(O)

Perform the same operation as the IE scenario in the Internet Explorer to check whether the Web page is displayed correctly.

KAVK38603-E

An error occurred while replaying operations. Replaying will be canceled.

An error occurred while replaying operations.

(S)

Cancels replaying operations.

(O)

Perform the same operation as the IE scenario in the Internet Explorer to check whether the Web page is displayed correctly.

KAVK38604-E

An attempt to display HTML source code has failed.

An attempt to display HTML source code has failed.

(S)

Cancels displaying HTML source code.

(O)

Check whether *installation-folder\agtv\probe\tmp* folder exists. Check also whether the HTML file of the currently displaying Web page exists. If not, the HTML source code cannot be displayed.

KAVK38605-E

An attempt to record selecting operations has failed.

The information necessary for the selecting data from the list cannot be recorded.

(S)

Cancels the recording operations.

(O)

Check whether the recording target Web page has the operations cannot be replayed. For details about the operations cannot be replayed, see [5.2.3\(3\) Notes on recording and replaying the IE scenarios](#).

KAVK38700-E

The response pattern conditions were not satisfied.

The contents of acquired HTML files were not satisfied the response determination information.

(S)

Cancels replaying the IE scenario.

(O)

Check the status of the HTTP server and whether the IE scenario can be replayed by using the IE Recorder.

KAVK38752-E

There is no tag that will be operated on specified position.

There is no tag that will be operated on the specified position.

(S)

Cancels replaying the IE scenario.

(O)

Check whether the measurement target Web page is different from that when recording the IE scenario. Although the target Web page is displayed same as the IE scenario, the position of the tags in the HTML source code may be different. Check whether the tag that be operated exists on the position specified in the **filtering conditions** in the HTML source code. If the target Web page is the same when recording the IE scenario, see [5.2.4\(4\) How to handle the error There is no tag that will be operated although the Web page does not change](#).

KAVK38753-E

There is no tag that will be operated.

There is no tag that will be operated.

(S)

Cancels replaying the IE scenario.

(O)

Check whether the measurement target Web page is different from that when recording the IE scenario.

Although the target Web page is displayed same as the IE scenario, the position of the tags in the HTML source code may be different. Check whether the tag that be operated exists on the position specified in the **filtering conditions** in the HTML source code. If the target Web page is the same when recording the IE scenario, see [5.2.4\(4\) How to handle the error There is no tag that will be operated although the Web page does not change.](#)

KAVK38754-E

There is no frame that will be operated.

There is no frame that will be operated.

(S)

Cancels replaying the IE scenario.

(O)

Check whether the structure (or specification) of the measurement target Web page is different from that when recording the IE scenario.

KAVK38755-E

There is no tab that will be operated.

There is no tab (or browser) that will be operated.

(S)

Cancels replaying the IE scenario.

(O)

Check whether the structure (or specification) of the measurement target Web page is different from that when recording the IE scenario.

KAVK38756-E

A popup dialog box which is not recorded while replaying the IE scenario appears.

A popup dialog box which is not recorded while replaying the IE scenario appears.

(S)

Cancels replaying the IE scenario.

(O)

Check whether the structure (or specification) of the measurement target Web page is different from that when recording the IE scenario.

KAVK38757-E

An error occurred in the Web page transition while replaying the IE scenario. (`detail code=error-code`)

An error occurred in the Web page transition while replaying the IE scenario. If the error code is numeric value for hex which begins with 0x, an internal error occurred. If the error code is numeric value for 3 digits, it shows the HTTP-status error code.

(S)

Cancels replaying the IE scenario.

(O)

Check whether the structure (or specification) of the measurement target Web page is different from that when recording the IE scenario.

KAVK38758-E

An error occurred in the Web page transition while recording the IE scenario. (`detail code=error-code`)

An error occurred in the Web page transition while recording the IE scenario. If the error code is numeric value for hex which begins with 0x, an internal error occurred. If the error code is numeric value for 3 digits, it shows the HTTP-status error code.

(S)

Cancels recording the IE scenario.

(O)

Check the following:

1. Whether the recorded operations perform that the Web page is displayed correctly.
2. Whether an error occurred in the measurement target Web page. (Note that some errors that are not displayed during operating in the Internet Explorer are displayed in the IE Recorder. The IE Recorder cannot record this operations.)

For details about how to check, see [5.2.4\(3\) How to check the user operations when navigation errors occur](#).

KAVK38759-E

An unexpected error occurred. (`detail code=error-code`)

An unexpected error occurred.

(S)

Cancels replaying or recording the IE scenario.

(O)

Contact the system administrator.

KAVK38800-I

The selected operation information will be deleted. Do you want to continue?

Confirms whether to delete the selected operation information.

(S)

If you click the **Yes** button, the system deletes the selected operation information.

If you click the **No** button, the system cancels deleting the selected operation information.

KAVK38801-I

Scope (*scope-name*) settings will be deleted. Do you want to continue?

Confirms whether to delete the scope settings.

(S)

If you click the **Yes** button, the system deletes the scope settings.

If you click the **No** button, the system cancels deleting the scope settings.

KAVK38803-I

An end scope does not exist for a start scope. Do you want to set the final operation as the end scope? (*scope name=scope-name*)

An end scope does not exist corresponding for a start scope. Confirms whether to set the final operation as the end scope.

(S)

If you click the **Yes** button, the system sets the final operation as the end scope.

If you click the **No** button, the system cancels the save or save-as processing.

KAVK38804-I

A start scope does not exist for an end scope. Do you want to set the first operation as the start scope? (*scope name=scope-name*)

A start scope does not exist corresponding for an end scope. Confirms whether to set the first operation as the start scope.

(S)

If you click the **Yes** button, the system sets the first operation as the start scope.

If you click the **No** button, the system cancels the save or save-as processing.

KAVK38805-I

Operation information after the selection will be deleted. Do you want to continue?

Confirms whether to delete the operation information after the selection.

(S)

If you click the **Yes** button, the system deletes the operation information after the selection.

If you click the **No** button, the system cancels deleting the operation information.

KAVK38806-I

All tabs will close. Do you want to continue?

If the multiple tabs open when replaying the IE scenario, confirms whether to open only one tab and close all others.

(S)

If you click the **Yes** button, the system opens only one tab and closes all others.

If you click the **No** button, the system cancels replaying the IE scenario.

KAVK38807-I

The end scope is before the start scope. Do you want to swap the start scope and end scope? (`scope ID=scope-ID`)

The end scope is before the start scope. Confirms whether to swap the start scope and end scope.

(S)

If you click the **Yes** button, the system swaps the start scope and end scope.

If you click the **No** button, the system does not set the start scope.

KAVK38808-I

The start scope is after the end scope. Do you want to swap the start scope and end scope? (`scope ID=scope-ID`)

The start scope is after the end scope. Confirms whether to swap the start scope and end scope.

(S)

If you click the **Yes** button, the system swaps the start scope and end scope.

If you click the **No** button, the system does not set the start scope.

KAVK38809-W

Different passwords were entered. Please enter the same password in both text boxes.

The value of **New password** and **Confirm new password** is different.

(S)

When the dialog box is closed, the system resumes processing.

(O)

Enter the same password in both **New password** and **Confirm new password**.

KAVK38810-I

The IE scenario file has been changed. Do you want to save the file? (`file name=file-name`)

Confirms whether to save the changes to the file.

(S)

If you click the **Yes** button, the system saves the changes to the file.

If you click the **No** button, the system does not save the changes to the file.

If you click the **Cancel** button, returns to the IE Recorder (main) window.

KAVK38811-I

The IE scenario will be replayed once. Do you want to continue?

Confirms whether to replay the IE scenario once.

(S)

If you click the **Yes** button, the system replays the IE scenario.

If you click the **No** button, returns to the IE Recorder (main) window.

KAVK38812-E

The start scope has not been set. Please complete the scope settings. (`scope name=scope-name`)

The start scope has not been set.

(S)

If you click the **OK** button, the system cancels the measurement test and returns to the IE Recorder (main) window.

(O)

Set the start scope, and complete the scope settings.

KAVK38813-E

The end scope has not been set. Please complete the scope settings. (`scope name=scope-name`)

The end scope has not been set.

(S)

If you click the **OK** button, the system cancels the measurement test and returns to the IE Recorder (main) window.

(O)

Set the end scope, and complete the scope settings.

KAVK38814-I

The IE scenario file has been changed. Do you want to save the file?

Confirms whether to save the changes to the file.

(S)

If you click the **Yes** button, the system saves the changes to the file.

If you click the **No** button, the system does not save the changes to the file.

If you click the **Cancel** button, returns to the IE Recorder (main) window.

KAVK38815-E

An attempt to get information from browser has failed.

An attempt to get information of the dialog box data from the browser has failed.

(S)

If you click the **OK** button, returns to the IE Recorder (main) window.

(O)

Redo a series of operations in progress.

KAVK38816-E

The file name is invalid.

The specified file name is invalid.

- (S) If you click the **OK** button, the system does not save the file and returns to the IE Recorder (main) window.
- (O) Specify the name of the file, including the file name extension (.xml).

KAVK38817-E

It was not possible to enable the parameters of the IE Recorder action condition definition file.
Parameters=parameter-information

It was not possible to enable the parameters of the IE Recorder action condition definition file.

- (S) Continues subsequent processing.
- (O) Check the *KAVKnnnnn-Z* message that was output immediately before this message and take the action indicated in it.
nnnnn indicates a message serial number. *Z* indicates a message type.

KAVK41000-E

Insufficient memory occurred.

Insufficient memory occurred. Processing cannot be continued.

- (S) Terminates the command.
- (O) Terminate any application that is not in use, or increase memory.

KAVK41001-E

System call error occurred. *API=system-call-name, ERRNO=error-number*

System call error occurred.

- (S) Terminates the command.
- (O) Contact the system administrator.

KAVK41002-E

An internal error occurred.

An internal error occurred. Processing cannot be continued.

(S)

Terminates the command.

(O)

Contact the system administrator.

KAVK41003-E

An attempt to acquire the logical host name failed.

An attempt to acquire the logical host name failed.

(S)

Terminates the command.

(O)

Make sure that there is no shortage of system resources.

If re-execution does not recover the system, contact the system administrator.

KAVK41004-E

An attempt to copy the file has failed. `File=file-that-could-not-be-copied` (Blank if the file name cannot be acquired)

An attempt to copy the file has failed.

(S)

Terminates the command.

(O)

Make sure that there is no shortage of system resources.

If re-execution does not recover the system, contact the system administrator.

KAVK41005-E

An attempt to acquire the environment directory failed.

An attempt to acquire the environment directory failed.

(S)

Terminates the command.

(O)

Make sure that there is no shortage of system resources.

If re-execution does not recover the system, contact the system administrator.

KAVK41006-E

An attempt to acquire the environment directory failed. `Directory=directory-that-could-not-be-created` (Blank if the directory name cannot be acquired)

An attempt to acquire the environment directory failed.

(S)

Terminates the command.

(O)

Check the path to the displayed directory, and make sure that the directory can be created.

If re-execution does not recover the system, contact the system administrator.

KAVK41007-I

Did not restore files because there is not the directory. `Directory=directory-containing-backup-of-definition-files`

The definition files for Performance Management - Agent Option for Service Response were not restored because the backup directory for these files does not exist.

(S)

Terminates the command.

(O)

This is not an error. No action is required.

KAVK41008-I

Did not backup files because there is not the directory. `Directory=shared-disk-directory-containing-definition-file`

The definition files for Performance Management - Agent Option for Service Response were not backed up because the directory for these files does not exist on the shared disk.

(S)

Terminates the command.

(O)

This is not an error. No action is required.

KAVK42000-E

Insufficient memory occurred.

Insufficient memory occurred. Processing cannot be continued.

(S)

Terminates the command.

(O)

Close any applications that are not being used, or expand the memory.

KAVK42002-E

An internal error occurred.

An internal error occurred. Processing cannot be continued.

(S)
Terminates the command.

(O)
Contact the system administrator.

KAVK42003-E

An installation path could not be acquired.

The location where the product was installed could not be found.

(S)
Terminates the command.

(O)
Contact the system administrator.

KAVK42004-E

An attempt to execute the command has failed.

An attempt to execute the command has failed.

(S)
Terminates the command.

(O)
See the *KAVKnnnnn* message that was displayed before this message, and take appropriate action.

KAVK42005-I

The command was successfully executed.

The command was successfully executed.

(S)
Terminates the command.

(O)
This is not an error. No action is required.

KAVK42006-E

Win32 API error. *API=API-function-name*, *ERRNO=error-code*

The Win32 API returned an error.

(S)
Terminates the command.

(O)
Contact the system administrator.

KAVK42007-E

The command is already running.

The command is already running.

(S)

Terminates the command.

(O)

The command is already running. Stop the command and then restart it.

KAVK43000-E

Insufficient memory occurred.

Insufficient memory occurred. Processing cannot be continued.

(S)

Terminates the command.

(O)

Terminate any application that is not in use, or increase memory.

KAVK43001-E

An internal error occurred.

An internal error occurred. Processing cannot be continued.

(S)

Terminates the command.

(O)

Contact the system administrator.

KAVK43002-E

An installation path could not be acquired.

The location where the product was installed could not be found.

(S)

Terminates the command.

(O)

Contact the system administrator.

KAVK43003-E

An attempt to execute the command has failed.

An attempt to execute the command has failed.

(S)

Terminates the command.

(O)

Check the `KAVKnnnnn` message that was output immediately before this message and take the action indicated in it.

KAVK43004-I

The command was successfully executed.

The command was successfully executed.

(S)

Terminates the command.

(O)

This is not an error. No action is required.

KAVK43005-E

The command is already running.

The command is already running.

(S)

Terminates the command.

(O)

The command is already running. Stop the command and then restart it.

KAVK43006-E

The specified sub-command does not exist.

The specified sub-command does not exist.

(S)

Terminates the command.

(O)

Check whether the command is correct in the command line, and then re-execute the command.

KAVK43007-E

The specification of an option is invalid. `INFO=error-detail`

The specified option is invalid.

(S)

Terminates the command.

(O)

Check whether the command is correct in the command line, and then re-execute the command.

KAVK43008-E

An internal file operation failed. *OP=operation*, *ERRNO=error-code*, *P1=file-to-be-operated*, *P2=file-to-be-renamed* (Blank if no information), *ERRINFO=error-information* (Blank if no information)

An attempt to work with the internal file failed.

operation can be one of the following:

OPEN (R) , OPEN (W) , READ, WRITE, DELETE, OLDRENAME, NEWRENAME, RECOVERY

(S)

If a command outputs this message:

Terminates the command.

If a service outputs this message:

Disables the operation and continues subsequent processing.

(O)

If an error occurs in OPEN (R) :

Make sure that read permissions on the file indicated by P1 have been granted.

If an error occurs in OPEN (W) :

Make sure that write permissions on the file indicated by P1 have been granted.

If an error occurs in WRITE, DELETE, or NEWRENAME:

Remove the cause of the error, delete the file indicated by P1, and then re-execute the command.

If an error occurs in OLDRENAME or READ:

Remove the cause of the error, and then re-execute the command.

If an error occurs in RECOVERY:

Remove the cause of the error that needed a recovery action, and also remove the cause of this error and then rename the file indicated by P1 to the name indicated by P2.

Do not execute the command or delete the file indicated by P1 before you rename the file. Doing so deletes all the information about paused tasks already registered.

KAVK43009-W

A communication to the service failed. *SERVICE=daemon*

A pause or resumption notification to the Probe Daemon or IE Probe Daemon failed.

daemon can be either of the following:

PROBE, IEPROBE

(S)

Continues subsequent processing.

(O)

Make sure that the task ID specified in the command is registered with the measurement condition registration file (*esptask.xml*).

If the task ID specified in the command is not found in the measurement condition registration file, no action is required.

If the task ID specifies a scenario other than IE scenarios, check whether the Probe Daemon is running, and if it specifies an IE scenario, check whether the IE Probe Daemon is running.
If the Probe Daemon or IE Probe Daemon is running, execute the `sync` sub-command with the `-v` option specified.
If an error occurs, remove the cause and then re-execute the command.

KAVK43010-E

A communication to the service failed. *OP=operation, ERRNO=error-code, SERVICE=daemon, ERRINFO=error-information* (Blank if no information)

A communication to the service failed.

operation and *daemon* can be either of the following:

- *operation*: SEND or RECV
- *daemon*: PROBE or IEPROBE

(S)

Terminates the command.

(O)

Remove the cause of the error based on the `ERRNO` and `ERRINFO` information, and then re-execute the command.

KAVK43011-E

A communication to the service failed. *OP=operation, ERRNO=error-code, SERVICE=daemon, ERRINFO=error-information* (Blank if no information)

A communication to the service failed.

operation and *daemon* can be either of the following:

- *operation*: CONNECT or CLOSE
- *daemon*: PROBE or IEPROBE

(S)

Terminates the command.

(O)

If `CONNECT` is output:

Make sure that the daemon process indicated by `SERVICE` is running.

If `CLOSE` is output:

No action is required.

KAVK43015-E

An error occurred in Probe/IEProbe daemon. *SERVICE=daemon, ERRINFO=error-information* (Blank if no information)

An error occurred in the Probe Daemon or IE Probe Daemon.

daemon can be either of the following:

PROBE, IEPROBE

(S)

Terminates the command.

(O)

See the integrated trace log to remove the cause of the error, and then re-execute the command.

KAVK43016-E

The internal file is broken. *FILE=file-name*

The internal file is corrupt.

(S)

If a command outputs this message:

Terminates the command.

If a service outputs this message:

Continues subsequent processing assuming that the internal file does not exist.

(O)

Contact the system administrator.

KAVK43017-E

An error occurred in the process for requests to pause or continue monitorings. *ERRNO=error-code*, *ERRINFO=error-information* (Blank if no information)

Requests to pause or resume monitoring can no longer be accepted.

(S)

Cannot accept new requests to pause or resume monitoring, but continues subsequent processing with monitoring paused according to the accepted request.

(O)

Stop the service to remove the cause of the error, and then restart the service.

KAVK43018-I

Status of Probe/IEProbe daemon. *SERVICE=daemon*, *NUMBEROFTASK=number-of-paused-tasks*, *INFO=other-information* (Blank if no information)

This information is sent from the Probe or IE Probe when the command is executed.

daemon can be either of the following:

PROBE, IEPROBE

KAVK43019-W

Specified ID is already registered.

Specified ID is already registered.

(S)

Continues subsequent processing.

(O)

Check whether the specified ID is correct.

If not, specify the correct ID and re-execute the `pause` sub-command.

KAVK43020-W

Specified ID is not registered.

Specified ID is not registered.

(S)

Continues subsequent processing.

(O)

Check whether the specified ID is correct.

If not, specify the correct ID and re-execute the `continue` sub-command.

KAVK43021-E

The number of registered task-IDs reached the maximum number.

The number of registered task-IDs reached the maximum number.

(S)

Terminates the command.

(O)

Unregister some task IDs, and then re-execute the command.

KAVK43023-E

An attempt to open the Probe action condition definition file has failed.

An attempt to access the Probe action condition definition file failed.

(S)

Terminates the command.

(O)

Make sure that the Probe action condition definition file has been stored in the specified folder. Check the access permissions for the Probe action condition definition file.

KAVK43024-E

Information could not be acquired from the Probe action condition definition file.

Information could not be acquired from the Probe action condition definition file.

(S)

Terminates the command.

(O)

Check that the format of the Probe action condition definition file is correct.

KAVK43025-E

The content of a definition in the Probe action condition definition file is invalid. *section:key*

The content of a definition in the Probe action condition definition file is invalid.

(S)

Terminates the command.

(O)

Correct the contents of the Probe action condition definition file, and then retry.

KAVK43026-E

Because a temporary file is left, it cannot start. *info1=action, file1=file-name-1, file2=file-name-2*

The startup process was stopped because the temporary file was found.

(S)

Stops starting the command or daemon.

(O)

If *info1* is set to `DELETE`, delete the file indicated by *file1* and then restart the command or daemon. If *info1* is set to `RENAME`, rename the file indicated by *file1* to the name indicated by *file2* and then restart the command or daemon.

13

Error Handling Procedures

This chapter describes how to handle errors that may occur while you are using Performance Management products. This chapter is concerned primarily with handling errors relating to a PFM - Agent. For details about error handling for the overall Performance Management system, see the chapter that describes troubleshooting in the *JP1/Performance Management User's Guide*.

13.1 Error handling procedures

This section describes the procedures for handling errors that occur while you are using Performance Management products.

Check the event

Check the following:

- Event when the error occurred
- Contents of the message (if a message is displayed)
- Log information, such as the common message log

For details about the messages and how to respond to each message, see [12. Messages](#). For details about the log information that is output by the Performance Management products, see [13.3 Log information to be collected upon troubleshooting](#).

Collect data

Collect data to determine the cause of the error. For details about how to collect the necessary data, see [13.4 Data to be collected when a problem occurs](#) and [13.5 Data collection procedure](#).

Determine the cause

Use the collected data to determine the cause and extent of the error, as well as the range of its consequences.

13.2 Troubleshooting

This section explains how to conduct troubleshooting while you are using Performance Management products. When an error occurs while you are using a Performance Management product, you should first check to see if any of the events described in this section have occurred.

The following table lists the principal types of errors that may occur while you are using a Performance Management product.

Table 13–1: Error types

Classification	Nature of problem	Section
Setting up or starting a service	<ul style="list-style-type: none"> • A Performance Management program service does not start. • It takes a long time for a service to start after startup is requested. • Another program service is started immediately after a Performance Management program service has stopped, but communication is not performed correctly. • The Master Store or Agent Store service stops after display of the message <code>The disk capacity is insufficient</code>. • The Agent Collector service of PFM - Agent does not start. 	See the chapter that explains troubleshooting in the <i>JPI/Performance Management User's Guide</i> .
Executing commands	<ul style="list-style-type: none"> • When the <code>jpctool service list</code> command is executed, the names of services that are not operating are output. • When the <code>jpctool db dump</code> command is executed, data other than the specified Store data is output. 	
Report definitions	<ul style="list-style-type: none"> • Information for some period of time is not displayed in historical reports. 	
Alarm definitions	<ul style="list-style-type: none"> • The program defined for action execution does not function correctly. • Alarm events are not displayed. 	
Collecting and managing performance data	<ul style="list-style-type: none"> • The size of the PFM - Agent's Store database is not reduced even though the data retention period was shortened. • The message <code>Illegal data was detected in the Store database</code> is output to the common message log. 	
Measuring Web transactions	<ul style="list-style-type: none"> • No Web transaction file is found • The user does not have access permissions to the Web transaction file • The Web transaction file contains a format error • The Web transaction file contains a definition error • The transaction specified in the Web transaction file does not exist • The monitored machine is not operating (or communications do not reach it) • The Web service (such as Apache HTTP Server) is not running • The resource specified in the URL does not exist (an HTTP 404 error occurs) • Invalid certificate (self-signed certificate) • A basic authentication error (missing password) occurs • A basic authentication error (incorrect password) occurs • A response determination error occurs • An option specification error occurs during measurement test command execution • A duplicate command execution error occurs during measurement test command execution 	<i>13.2.1</i>

For details about error handling in PFM - Agent for Service Response, see *13.8 Error handling procedure for each problem*.

13.2.1 Measuring Web transactions

This subsection describes how to troubleshoot Web transaction measurement.

The errors described in (13) *An option specification error occurs during measurement test command execution* and (14) *A duplicate command execution error occurs during measurement test command execution* might occur only when a measurement test command is executed. Other errors might occur when a Web transaction is measured or when a measurement test command is executed.

(1) No Web transaction file is found

The following message might be displayed:

```
KAVK08324-E An attempt to open the file has failed. FILE="C:\Program Files\Hitachi\jp1pc\agtv\probe\webtrans\wt3.xml", INFO="no such file"
```

Make sure that a Web transaction file exists in *installation-folder*\agtv\probe\webtrans\. Check the file access permissions.

(2) The user does not have access permissions to the Web transaction file

The following message might be displayed:

```
KAVK08324-E An attempt to open the file has failed. FILE='C:\Program Files\Hitachi\jp1pc\agtv\probe\webtrans\wt3.xml', INFO='Access was denied.'
```

Check the file access permissions.

(3) The Web transaction file contains a format error

(a) The format of the Web transaction file is invalid

The following message might be displayed:

```
KAVK08025-E The format of a definition in the file is invalid. File='C:\Program Files\Hitachi\jp1pc\agtv\probe\webtrans\wt2.xml', INFO='Close tag 'TAITLE' does not match opening tag 'TITLE'. line : 11 char : 44'
```

See the locations of the tags indicated by the message, and correct the format error.

(b) Character encoding declared in the Web transaction file does not match the actually used character encoding

The following message might be displayed:

```
KAVK08025-E The format of a definition in the file is invalid. File='C:\Program Files\Hitachi\jp1pc\agtv\probe\webtrans\wt.xml', INFO=xxxxx#
```

#: Detailed error information is output to xxxxx in a language according to the OS setting.

Make sure that the encoding declaration (`encoding=`) specified in the XML declaration (`<?XML ?>`) in the Web transaction file indicated by `FILE=` is consistent with the character encoding actually used in the file.

If a Web transaction file is created by using the Web Recorder, URLs, titles, and other page information are written in `Shift_JIS`.

Therefore, if any character encoding other than **Shift_JIS** is specified for **Encoding of the Web transaction file** in the Web Recorder Create New Web Transaction window, the specified character encoding might be inconsistent with the one actually used in a file.

In this case, open a Web transaction file by using the Web Recorder. In the Web recorder (main) window, select **Transaction** and then **Save As**. In the Save As window, select **Shift-JIS** in **Encoding of the Web transaction file**, and then save the Web transaction file. After saving the file, perform measurement or execute the command again.

(4) The Web transaction file contains a definition error

The following message might be displayed:

```
KAVK08173-E The content of a definition in the wWeb transaction file is invalid.  
File=wt2.xml, TAG=STEP_ID
```

See the location of the tag indicated by `TAG=`, and correct the definition error.

(5) The transaction specified in the Web transaction file does not exist

The following message might be displayed:

```
KAVK08171-E There is no Web transaction. ID=0, File=wt.xml, Web transaction=wtz
```

Make sure that the Web transaction file indicated by `File=` is correct. Make sure that the specified Web transaction has been defined.

(6) The monitored machine is not operating (or communications do not reach it)

The following message might be displayed:

```
KAVK08340-E Socket API error. SOCKET_ERRNO=10060,OPERATION=select  
KAVK08211-E An attempt to establish a TCP connection for measurement has failed.  
ID=0,Service_type=WEBTRANS
```

`SOCKET_ERRNO=10060` (detailed code `WSAETIMEDOUT` for `Winsock2API`) indicates that there is no correct response from the connection destination during the three-way handshake performed by TCP connection processing. Check the following points:

- Is the connection destination host (Web server or HTTP proxy server) operating?
- Are TCP connections blocked by a firewall or other security measures?
- Is IP routing correct?
- Is the host name or IP address specified in the URL correct?
- When a host name is specified, can the host name be resolved to the correct IP address? (Address resolution results can be verified using the `-v` option.)

(7) The Web service (such as Apache HTTP Server) is not running

The following message might be displayed:

```
KAVK08340-E Socket API error. SOCKET_ERRNO=10061,OPERATION=select
KAVK08211-E An attempt to establish a TCP connection for measurement has failed.
ID=0,Service_type=WEBTRANS
```

SOCKET_ERRNO=10061 (detailed code WSAECONNREFUSED for Winsock2API) indicates that the connection destination host has rejected a connection from a Web server or HTTP proxy server. Check the following points:

- Is the Web server program or HTTP proxy server program running correctly?
- Is the port number specified in the URL correct?

(8) The resource specified in the URL does not exist (an HTTP 404 error occurs)

The following message might be displayed:

```
KAVK08261-E The requested resource was not found.
ID=0,Service_type=WEBTRANS,URL=172.16.233.12/~example/
KAVK08341-E A HTTP response was failed. ID=0,ERRNO=404
```

The Web server detected that the requested resource was not found. Check the following points:

- Does the requested resource exist on the Web server?
- Did any error occur on the Web server?
- Can the Web server return the resource in response to a request message from PFM - Agent for Service Response? (Requests can be verified using the `-v` option.)
- Is the URL correct?

(9) Invalid certificate (self-signed certificate)

The following message might be displayed:

```
KAVK08253-E A self-signed certificate was found in the chain.
ID=0,Service_type=WEBTRANS,URL=172.16.233.12/~example/
```

Check the server certificate on the HTTP server.

(10) A basic authentication error (missing password) occurs

The following message might be displayed:

```
KAVK08174-EA password has not been set up. File=wt.xml, TAG=WEB_AUTH
```

Define a password in the Web transaction file, or register a password with the password utility, and then re-execute the command.

(11) A basic authentication error (incorrect password) occurs

The following message might be displayed:

```
KAVK08257-E An authentication is required. ID=0,Service_type=WEBTRANS,URL=www.xxx.co.jp/~example/basicauth/  
KAVK08341-E A HTTP response was failed. ID=0,ERRNO=401
```

The Web server detected that an authentication error occurred. Check the following points:

- Are the Web authentication user name and Web authentication password correct?
- Are there any problems with Web server logs?

(12) A response determination error occurs

The following message might be displayed:

```
KAVK08310-E It was not consistent to response pattern. ID=0, URL=www.xxx.co.jp/~example/basicauth/
```

Check the HTTP server or the network status.

(13) An option specification error occurs during measurement test command execution

The following message might be displayed:

```
KAVK08332-E The specification of an option is invalid. INFO="-wtfile"
```

Check the format of the option specification, and then re-execute the command.

(14) A duplicate command execution error occurs during measurement test command execution

The following message might be displayed:

```
KAVK42007-E The command is already running.
```

Wait for the preceding command to finish, and then re-execute the command.

13.2.2 Other problems

When other errors occur, you should check the circumstances at the time the error occurred. If a message is output, consider its contents carefully. For details about the log information that is output by Performance Management, see [13.3 Log information to be collected upon troubleshooting](#).

If you cannot resolve an error by taking any of the steps described in the chapter that explains troubleshooting in the *JP1/Performance Management User's Guide* and [13.2.1 Measuring Web transactions](#), or if an error occurs that is not described in these sections, collect all data that would be helpful for investigating the error and contact the system administrator.

For details about the data you should collect and how to collect it, see *13.4 Data to be collected when a problem occurs* and *13.5 Data collection procedure*.

13.3 Log information to be collected upon troubleshooting

When an error occurs in Performance Management, you should check the log information and investigate the problem. The following five types of log information are output during operation of Performance Management:

- System log
- Common message log
- Operation status log
- Trace log
- Integrated trace log

This section describes the five types of log information and the log options that can be set for each type.

13.3.1 Types of log information to be collected upon troubleshooting

(1) System log

The system log contains log information that reports the system status and the errors that have occurred. Performance Management outputs the system log to the event log file.

For details about the output formats, see the chapter that describes log information in the manual *JPI/Performance Management Reference*.

Notes about logical host operation:

In addition to the system log for Performance Management, you need the log information for the cluster software in order to check information such as the control of Performance Management by the cluster software.

(2) Common message log

The common message log contains log information that reports the system status and errors that have occurred. The information output to this log is more detailed than the system log information. For details about the common message log's output destination file name and file size, see [13.3.2 Lists of log files and folders accessed upon troubleshooting](#). For details about the output format, see the chapter that describes log information in the manual *JPI/Performance Management Reference*.

Notes about logical host operation:

When Performance Management is under logical host operation, the common message log is output to the shared disk. Because a log file on the shared disk is inherited together with the system during a failover, messages continue to be recorded in the same log file.

(3) Operation status log

The operation status log is the log information that is output by Web Console. For details about the name and size of the operation status log file, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*. For details about the output format, see the chapter that describes log information in the manual *JPI/Performance Management Reference*.

(4) Trace log

When an error occurs, the trace log contains log information that is needed to investigate the cause of the error, or to determine the processing time required by each process.

The trace log is output to a log file for that particular Performance Management program service.

Notes about logical host operation:

When Performance Management is under logical host operation, the trace log is output to the shared disk. Because a log file on the shared disk is inherited together with the system during a failover, messages continue to be recorded in the same log file.

(5) Integrated trace log

The integrated trace log is a collection of trace information output by each program; it is output to a single file by the Hitachi Network Objectplaza Trace Library (HNTRLib2). PFM - Agent for Service Response uses the Hitachi Network Objectplaza Trace Library (HNTRLib2) to output log files.

Notes about logical host operation:

When Performance Management is under logical host operation, the trace log is output to the shared disk. Because a log file on the shared disk is inherited together with the system during a failover, messages continue to be recorded in the same log file.

13.3.2 Lists of log files and folders accessed upon troubleshooting

This subsection describes the log information that is output from Performance Management. For details about the name and size of the file to which the operation status log information is output, see the chapter that describes troubleshooting in the *JPI/Performance Management User's Guide*.

(1) Common message log

This section describes the common message log, which is one of the types of log information for Performance Management. The table below lists the service or control names and the log file names for the log output source files, as well as the amount of disk space used.

Table 13–2: File names of the common message log

Type of log information	Output source	File name	Disk space used ^{#1} (KB)
Common message log	Performance Management	<i>installation-folder</i> \log\jpclog{01 02} ^{#2}	2,048 (x2)
		<i>installation-folder</i> \log\jpclogw{01 02} ^{#2}	2,048 (x2)
Common message log (for logical host operation)	Performance Management for logical host operation	<i>environment-folder</i> ^{#3} \jplpc\log\jpclog{01 02} ^{#2}	2,048 (x2)
		<i>environment-folder</i> ^{#3} \jplpc\log\jpclogw{01 02} ^{#2}	2,048 (x2)

#1

The value in parentheses is the number of log files that can be created for a single service. For example, 2,048 (x2) indicates that a maximum of two log files, each with a size of 2,048 KB, can be created. In this case, the total available disk space is 4,096 KB.

#2

The value 01 or 02 is appended to the file name of the common message log.

Sequential file method (jpclog):

Log information is first output to the log file whose name ends with 01. When the maximum log file size is reached, the suffix at the end of the log file name is changed from 01 to 02, and a new log file with the 01 suffix is created. Log information is then output to the new 01 log file. If a log file with a name ending in 02 already exists, that log file is overwritten when the 01 suffix is changed to 02. The most recent log information is always output to the log file with the 01 suffix.

Wraparound file method (jpclogw):

Log information is first output to the log file whose name ends with 01. When the maximum log file size is reached, a new log file with the 02 suffix is created. Log information is then output to the new 02 log file. If a log file with a name ending in 02 already exists, all data is deleted from that log file, and then log information is output from the beginning of the file. Thereafter, the log files are used alternately.

For details about how to output log information to log files, see the chapter that describes detection of Performance Management failures in the *JPI/Performance Management User's Guide*.

#3

The environment folder is on the shared disk that was specified when the logical host was created.

(2) Trace log

This subsection describes the trace log, which is one of the types of log information for Performance Management. The table below lists the service names or control names that are the output sources of PFM - Agent trace logs, as well as the names of the storage folders.

Table 13–3: Names of the trace log storage folders

Type of log information	Output source	Folder name
Trace log	Action Handler service	<i>installation-folder</i> \bin\action\log\
	Performance Management command	<i>installation-folder</i> \tools\log\
	Agent Collector service	<i>installation-folder</i> \agtv\agent\log\
	Agent Store service	<i>installation-folder</i> \agtv\store\log\
Trace log (for logical host operation)	Action Handler	<i>environment-folder</i> #\jplpc\bin\action\log\
	Performance Management command	<i>environment-folder</i> #\jplpc\tools\log\
	Agent Collector	<i>environment-folder</i> #\jplpc\agtv\agent\log\
	Agent Store	<i>environment-folder</i> #\jplpc\agtv\store\log\

#

The environment folder is on the shared disk that was specified when the logical host was created.

(3) Integrated trace log

The table below lists the output file name and folder name for the integrated trace log of the Performance Management log information.

Table 13–4: Name of the integrated trace log storage folder

Type of log information	Output source	File name	Disk space used (KB)
Integrated trace log	Probe Daemon	<i>HNTRLib2-installation-folder</i> \spool\hntr2[n#].log	256
	IE Probe Daemon	<i>HNTRLib2-installation-folder</i> \spool\hntr2[n#].log	256

#

n represents a number in the range from 1 to 4.

13.4 Data to be collected when a problem occurs

If the appropriate action described in [13.2 Troubleshooting](#) is not successful in correcting the error, you should collect the necessary data and contact the system administrator to determine the cause of the error. This section describes the data that should be collected in the event of an error.

Performance Management provides commands for collecting the needed data in the batch mode. Use the `jpcras` command to collect PFM - Agent data. The tables in this section indicate the data that can be collected by the `jpcras` command.

Note:

The data collected by the `jpcras` command depends on the options you specify when you execute the command. For details about the command's options and the data that can be collected, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

Notes about logical host operation:

The following notes apply to logical host operation:

- During logical host operation, Performance Management log information is stored on the shared disk. If the shared disk is placed online (Windows), you can also use the `jpcras` command to collect the log information on the shared disk in the batch mode.
- To investigate a problem during a failover, you need information for both before and after the failover. This means that you need information about both the executing system and the standby system.

To investigate Performance Management for logical host operation, information about the cluster software is also necessary. Because Performance Management for logical host operation is started and terminated from the cluster software, the behavior of the cluster software must be compared with the behavior of Performance Management.

13.4.1 In Windows

(1) Log information about the OS

The following table lists the OS-related information that must be collected.

Table 13–5: Log information about the OS

Type of information	Overview	Default file name	Collected by jpcras command?
System log	Windows event log	--	Y
Process information	List of processes	--	Y
System file	hosts file	<i>system-folder</i> \system32\drivers\etc\hosts	Y
	services file	<i>system-folder</i> \system32\drivers\etc\services	Y
OS information	System information	--	Y
	Network status	--	Y
	Host name	--	Y

Type of information	Overview	Default file name	Collected by jpcras command?
Dump information (In Windows Server 2003)	Dr. Watson log file	<ul style="list-style-type: none"> <i>system-drive</i>\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwtsn32.log# <i>system-drive</i>\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dump# 	Y
Dump information	Log file containing error reports and corrective actions	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;"> <i>user-mode-process-dump-output-folder\program-name.process-ID.dmp</i> </div> Example: jpcagtv.exe.2420.dmp	N

Legend:

Y: Can be collected.

N: Cannot be collected.

--: Not applicable.

#

If your setup provides for output of log files to a different folder, make sure that you collect the data from the correct folder.

(2) Information about Performance Management

You should collect information about Performance Management, as listed in the table below. In the case of a network error, you should also collect applicable files from the connection-destination machine.

Table 13–6: Performance Management information

Type of information	Overview	Default file name	Collected by jpcras command?
Common message log	Message log output from Performance Management (sequential file method)	<i>installation-folder</i> \log\jpclog{01 02}#1	Y
	Message log output from Performance Management (wraparound file method)	<i>installation-folder</i> \log\jpclogw{01 02}#1	Y
Configuration information	Each configuration information file	--	Y
	Output results of the jpc tool service list command	--	Y
Version information	Product version	--	Y
	Historical information	--	Y
Database information	Agent Store service	<ul style="list-style-type: none"> For Store 1.0 <i>installation-folder</i>\agtv\store*.DB <i>installation-folder</i>\agtv\store*.IDX For Store 2.0 <i>installation-folder</i>\agtv\store\STPD 	Y

Type of information	Overview	Default file name	Collected by jpcras command?
Database information	Agent Store service	The following files under the <i>installation-folder</i> \agtv\store\STPI folder: *.DB *.IDX	Y
Trace log	Trace information for each Performance Manager	__#2	Y
Install log ^{#3}	Installation message log	The following files under the <i>system-folder</i> \TEMP \HCDINST folder: <ul style="list-style-type: none"> HCDMAIN.LOG and HCDMAINn.LOG^{#4} HCDINST.LOG and HCDINSTn.LOG^{#4} <i>product-model-name</i>.LOG 	N
Information about PFM - Agent for Service Response	Log files for PFM - Agent for Service Response	All files under <i>installation-folder</i> \agtv\probe\log	Y
	Definition files for PFM - Agent for Service Response	All files under <i>installation-folder</i> \agtv\probe\conf	Y
	Measurement condition registration and storage files	All files under <i>installation-folder</i> \agtv\probe\task	Y
	Password files	All files under <i>installation-folder</i> \agtv\probe\passwd	Y
	Report files	All files under <i>installation-folder</i> \agtv\probe\report	Y
	User-defined commands	All files under <i>installation-folder</i> \agtv\probe\user	Y
	Temporary files	All files under <i>installation-folder</i> \agtv\probe\tmp	Y
	Certificate files	All files under <i>installation-folder</i> \agtv\probe\cert	Y
	IE scenario file	All files under <i>installation-folder</i> \agtv\probe\iescena	Y
	Web transaction files	All files under <i>installation-folder</i> \agtv\probe\webtrans	Y
	Registry information	HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\JP1PCAGTV	Y
	Environment variable information	--	Y
	Integrated trace log	--	<i>system-drive</i> \Program Files\hitachi\HNTRLib2\spool\hntr2[n ^{#4}].log

Legend:

Y: Can be collected.

N: Cannot be collected.

--: Not applicable.

#1

For details about how to output log information to the log files, see the chapter that describes detection of Performance Management failures in the *JP1/Performance Management User's Guide*.

#2

For details about the trace log storage folder, see *13.3.2 Lists of log files and folders accessed upon troubleshooting*.

#3

Collect this log information if installation fails.

#4

n represents a number in the range from 1 to 4.

(3) Operation information

You should collect the following information about the operation that was being performed when the error occurred:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, OS version, host name, and PFM - Manager and PFM - Agent configuration)
- Whether or not the problem is replicable
- Performance Management user name used during logon, if the user logged on from PFM - Web Console
- The argument specified for the command if the error occurred during command execution.

(4) Error information on screen displays

You should obtain printouts of the following:

- The active screen when the application error occurred
- The error message dialog box (including the contents of detail information if it is displayed)
- The Command Prompt window, if the error occurred during command execution
- Hard copy of the Command Prompt window or Administrator Console window if a problem occurred during command execution

(5) User mode process dump

If a Performance Management process stops due to an application error, obtain a user dump.

(6) Collecting problem reports

If a Performance Management process stops due to an application error, obtain a problem report.

(7) Other information

You should also collect the following information:

- Contents of **System** and **Application** in the Windows Event Viewer window
- Content of **System Information** under **System Tools** under **Accessories**

13.5 Data collection procedure

This section explains how to collect data in the event of an error.

13.5.1 In Windows

(1) Collecting dump information

To collect dump information in Windows:

1. Open Task Manager.
2. Select the process tab.
3. Right-click the process name for which you want to collect dump information, and then select **Create Dump File**.
Dump files are stored in the following folder:

```
system-drive\Users\user-name\AppData\Local\Temp
```

4. Obtain the dump file from the folder created in step 3.
If you have changed the environment variable settings so that dump files are output to a different folder, obtain the dump file from that folder.

(2) Executing the data collection command

Use the `jpccras` command to collect data needed to determine the cause of an error (note that an OS user with Administrator permissions must execute the procedure described below).

To execute the data collection command:

1. Log on to the host where the service subject to this data collection is installed.
2. At the command prompt, execute the following command to enable the extension function of the command interpreter:

```
cmd /E:ON
```

3. Specify in the `jpccras` command the data to be collected and the storage folder for the data, and then execute the command.

The following `jpccras` command stores all available information in the

```
c:\tmp\jpc\agt folder:  
jpccras c:\tmp\jpc\agt all all
```

When the `jpccras` command is executed, the `jpctool service list -id * -host *` command is executed internally to obtain a list of PFM services and to confirm whether the services are running. Execution of this internal command might take a long time if a firewall exists between the host that executes the command and a host in another Performance Management system or if the system configuration is large. In either case, you can set the `JPC_COLCTRLNOHOST` environment variable to 1 to suppress processing of the `jpctool service list -id * -host *` command to shorten the command execution time.

For details about the `jpcras` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

(3) Executing the data collection command (for logical host operation)

Performance Management information for logical host operation is on the shared disk and must be collected in both the executing system and the standby system.

To collect information needed to investigate the cause of a problem, use the `jpcras` command. This subsection describes how to execute the data collection command. This procedure must be executed by an OS user with Administrator permissions.

To execute the data collection command for logical host operation:

1. Bring the shared disk online.

Information about the logical host is stored on the shared disk. At the executing node, make sure that the shared disk is online, and then collect the information.

2. In both the executing system and the standby system, execute the `jpcras` command, in which the information to be collected and its storage folder are specified.

The following example stores all the information collectible by the `jpcras` command in the `c:\tmp\jpc\agt` folder:

```
jpcras c:\tmp\jpc\agt all all
```

Executing the `jpcras` command without the `lhost` argument specified collects all the Performance Management information on the physical and logical hosts at that node. If there is Performance Management in the logical host environment, the log files on the shared disk are acquired.

If the `jpcras` command is executed at a node where the shared disk is offline, files cannot be acquired from the shared disk, but the command terminates normally without resulting in an error.

Note:

Execute the data collection command at both executing and standby nodes to collect information. To examine an event before and after failover, you need the information for both the executing system and the standby system.

When the `jpcras` command is executed, the `jpctool service list -id * -host *` command is executed internally to obtain a list of PFM services and to confirm whether the services are running. Execution of this internal command might take a long time if a firewall exists between the host that executes the command and a host in another Performance Management system or if the system configuration is large. In either case, you can set the `JPC_COLCTRLNOHOST` environment variable to 1 to suppress processing of the `jpctool service list -id * -host *` command to shorten the command execution time.

For details about the `jpcras` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*.

3. Collect information about the cluster software.

This information is needed to determine whether the problem occurred in the cluster software or in Performance Management. Collect the information that provides control requests, such as start and termination of Performance Management from the cluster software, and the results of the control requests.

Note:

If the user account control functionality (UAC) is enabled in the operating system, the User Account Control dialog box might be displayed during command execution. If it is displayed, click the **Continue** button to continue data collection, or click the **Cancel** button to cancel data collection.

(4) Obtaining the Windows event log

Collect the contents of **System** and **Application** in the Windows Event Viewer window.

(5) Checking information about the operation

You should check and save the following information about the operation that was being performed when the error occurred:

- Details of the operation
- Time the error occurred
- Machine configuration (for example, OS version, host name, and PFM - Manager and PFM - Agent configuration)
- Whether or not the problem is replicable
- Performance Management user name used during logon, if the user logged on from PFM - Web Console
- The argument specified for the command if the error occurred during command execution.

(6) Collecting error information on screen displays

Collect hard copies of the following items:

- Hard copy of the window operation if an application error occurred
- Hard copy of the error message dialog box
If detailed information is available, also copy its content.
- Hard copy of the Command Prompt window or Administrator Console window if a problem occurred during command execution

To obtain a hard copy of the Command Prompt window or Administrator Console window, specify the following in the Command Prompt Properties window:

- **Edit Options** under the **Options** tab
Select **Quick Edit Mode**.
- **Layout** tab
Set **Height** under **Screen Buffer Size** to 500.

(7) Collecting other information

Information to be collected for all operating systems

- Contents of the dialog box displayed by choosing **Accessories**, **System Tools**, and then **System Information**

13.6 Detecting problems within Performance Management

You can use the health check function to detect problems within Performance Management itself. This function monitors the operating status of the monitoring agent and the host on which the monitoring agent is running, and displays the monitoring results in PFM - Web Console as changes in the status of the monitoring agent.

You can also use the PFM service Auto-restart functionality that automatically restarts the PFM service when it abnormally terminates for some reason or restart it on a regular basis.

To use the health check function to monitor the operating status of the monitoring agent or use the PFM service Auto-restart functionality, you need to use the status management function. This function checks the detailed status of the Performance Management service. Therefore, the version of the target monitoring agent must support the status management function and the status management function must be enabled. There are no requirements when you monitor the operating status of the host.

Using JPI/Base, which is an integrated system monitoring and management product, to monitor Performance Management log files can also detect problems within Performance Management itself. This allows the system administrator to quickly detect an error if a problem occurs, determine the cause of the error, and take an appropriate recovery measure.

For details about detecting problems within Performance Management itself, see the chapter explaining error detection in Performance Management in the *JPI/Performance Management User's Guide*.

13.7 Performance Management system error recovery

When an error occurs on a Performance Management server, you need to restore the server to the normal state that was present before the error occurred, based on a backup file.

For details about how to restore a server to its pre-error state, see the chapter explaining troubleshooting in the *JP1/Performance Management User's Guide*.

13.8 Error handling procedure for each problem

This section describes common problems and how to troubleshoot them in PFM - Agent for Service Response. See this section when you investigate the cause of a problem or try to isolate where a problem lies.

This section uses the following icons for records, field values, and log information for identifying error information such as messages.

Integrated Trace Log and **Common Message Log**

For details, see [13.3.1 Types of log information to be collected upon troubleshooting](#) and [13.3.2 Lists of log files and folders accessed upon troubleshooting](#).

Result Code

See *Common fields* in *10. Records*.

PL_IESM Record

Collect Logged Message for IE Scenario (PL_IESM) records to see error messages in them. For details about the records, see [Logged Message for IE Scenario \(PL_IESM\)](#) in *10. Records*.

13.8.1 PFM - Agent for Service Response service cannot be started

The following subsections describe how to handle the problem when the PFM - Agent for Service Response service cannot be started.

(1) Extensible Service Probe service cannot be started or will be inactive when reloaded (in cases other than IE scenarios)

Integrated Trace Log

```
KAVK08137-E A password has not been set up.
```

This problem occurs when the password needed for measurement conditions is not specified as defined in the measurement condition registration file (`esptask.xml`). For details about how to handle this problem, see the description of the message with ID `KAVK08137-E` in [12.4 Messages](#).

Integrated Trace Log

```
KAVK08171-E There is no Web transaction.  
KAVK08172-E The format of a definition in the Web transaction file is  
invalid.
```

This problem is specific to a Web transaction. The Web transaction may not be defined correctly. See the description of the message with each ID in [12.4 Messages](#) to handle the problem indicated by each message.

For the causes other than above, check the contents of the integrated trace log output, and use the ID of the recorded message to see the description in [12.4 Messages](#).

(2) Extensible Service Probe service cannot be started or will be inactive when reloaded (in IE scenarios)

Integrated Trace Log

```
KAVK10002-E jpcviemd has already started.
```

This problem occurs when the IE Probe Daemon service is started as a Windows service after it is started as an application. Start the service in either of the methods. For details about how to start the service, see [5.1.2 \(2\) Starting the IE Probe Daemon service](#).

Integrated Trace Log

```
KAVK10033-E The content of a definition in the measurement condition registration file is invalid. (ID=measurement-condition-ID, TAG=<INTERVAL>)
```

If the value of TAG is <INTERVAL>, the same value may be specified for both the measurement interval (INTERVAL) and timeout period (TIMEOUT) in the measurement condition registration file. Review the values in this file, and then start the PFM - Agent for Service Response service again or reload it.

Integrated Trace Log

```
KAVK10040-E An attempt to open the IE scenario file has failed.
```

This may be due to either of the following reasons:

- The IE scenario file cannot be accessed.
- The specification of the IE scenario file in the measurement condition registration file (`esptask.xml`) is invalid.

For details about how to handle the problem, see the description of the message with ID KAVK10040-E in [12.4 Messages](#).

Common Message Log

```
KAVF16028-E Processing to reload the IE Probe daemon has failed.
```

Although no measurement condition for IE scenarios is defined in the measurement condition registration file (`esptask.xml`), the `ie_service_flag` setting may be set to Y in the Probe action condition definition file (`esp.conf`).

If you want to measure IE scenarios, add at least one measurement condition for an IE scenario in the measurement condition registration file. If you do not measure IE scenarios, set `ie_service_flag` to N. For details about the definitions in the Probe action condition definition file and measurement condition registration file, see [8.2 Probe action condition definition file \(`esp.conf`\)](#) and [8.3 Measurement condition registration file \(`esptask.xml`\)](#).

For the causes other than above, check the contents of the integrated trace log output, and use the ID of the recorded message to see the description in [12.4 Messages](#).

13.8.2 PFM - Agent for Service Response cannot perform measurements

Result Code

You can see measurement results from result codes, which are the common field in the PI record. Any result code value other than 0 (SUCCESS) indicates that the measurement failed, and you can use the value of the code to isolate the cause of the failure.

Also, when the measurement fails, an error message may be written to the integrated trace log or PL_IESM record. So you can check these together with the result code. You can also view the error information by using the measurement test command for Web transactions (`jpcvtest`), as long as you measure Web transactions. For details about the command, see *jpcvtest (executes measurement tests)* in *11. Commands* and *13.2.1 Measuring Web transactions*.

This subsection describes cases where measurements often fail, organized by the value of the result code.

 **Tip**

The description contains the cases that can apply to the situation where scenarios cannot be replayed by the IE Recorder, and is worth reading.

(1) Value of the result code is 1 (NETWORK ERROR) Integrated Trace Log

The measurement failed because of a communication error caused by a failure on the network between a monitored server and a PFM - Agent for Service Response host, on the monitored sever, or on anywhere else. The following table lists possible causes of the error.

Table 13–7: Possible causes when the value of the result code is 1 (NETWORK ERROR)

Cause	What you check	Action
The monitored server or service is not running.	Check whether the monitored server or service is running.	Start the monitored server or service.
The name resolution via DNS failed.	Check whether the name of the monitored host or proxy server host can be resolved (by trying the <code>nslookup</code> command or viewing the <code>hosts</code> file).	Set up your DNS system or the <code>hosts</code> file, so that the name of the monitored host or proxy server host can be resolved.
TCP connection failed.	Check whether the measurement condition registration file (<code>esptask.xml</code>) has the correct values for the following settings: <ul style="list-style-type: none"> • Host name • Port number • Host name of the proxy server 	Correct the setting in the measurement condition registration file (<code>esptask.xml</code>).
	Check whether a firewall located between the monitored server and a PFM - Agent for Service Response host blocks communication.	Configure the firewall to allow communication.
	Check how the monitored server (including relay devices) communicates with the PFM - Agent for Service Response host, in terms of: <ul style="list-style-type: none"> • Whether they can reach each other (through the <code>ping</code> command or other means) • Which path is used for communication (through the <code>tracert</code> command or other means) • Whether the monitored service can be connected (through the <code>telnet</code> command or other means) 	According to the <i>What you check</i> column, check how the monitored server communicates with the PFM - Agent for Service Response host, and address problems, if any.

Cause	What you check	Action
It takes long time to establish the TCP connection, resulting in the failure of the connection.	Check the load on the monitored server (including relay devices) and the PFM - Agent for Service Response host.	Review the operation so that the monitored server (including relay devices) and PFM - Agent for Service Response host are not overloaded.

In most cases, network failure occurs when PFM - Agent for Service Response starts monitoring additional new targets or when a communication path is changed in the monitored environment (for example, when a proxy setting is changed or a load balancer is added). Therefore, Hitachi recommends that you check in advance to ensure that PFM - Agent for Service Response can communicate with monitored servers successfully.

(2) Value of the result code is 2 (TIME OUT) Integrated Trace Log PL_IESM Record

PFM - Agent for Service Response failed to perform a measurement because it could not finish processing within the timeout period defined in the measurement condition registration file (`esptask.xml`).

Table 13–8: Possible causes when the value of the result code is 2 (TIME OUT)

Cause	What you check	Action
The monitored server responded, but the specified timeout period was exceeded.	<ul style="list-style-type: none"> Check the load on the monitored server or network. Check the log for the monitored service (such as the Web server log) to see if communication is normal. Check the timeout period defined in the measurement condition registration file (<code>esptask.xml</code>) to see if the file has a valid value. 	According to the <i>What you check</i> column, check the monitored service and whether communication is normal, and address problems, if any.
Unmeasurable Web pages are monitored (IE scenario).	<ul style="list-style-type: none"> Check whether the software is monitoring Web pages that open dialog boxes which cannot be monitored.^{#1} Check whether the requested Web page does not issue the completion notification and is automatically forwarded to another page through JavaScript.^{#2} 	<p>This problem cannot be avoided in the measurement of IE scenarios, and thus consider measuring such Web pages in Web transactions. For details about whether these can be measured in Web transactions, read the following notes in advance to determine if they apply:</p> <ul style="list-style-type: none"> 5.2.2 (3) Notes about service monitoring Web transaction operating environment and notes of Web Transaction (PI_WT) in 10. Records

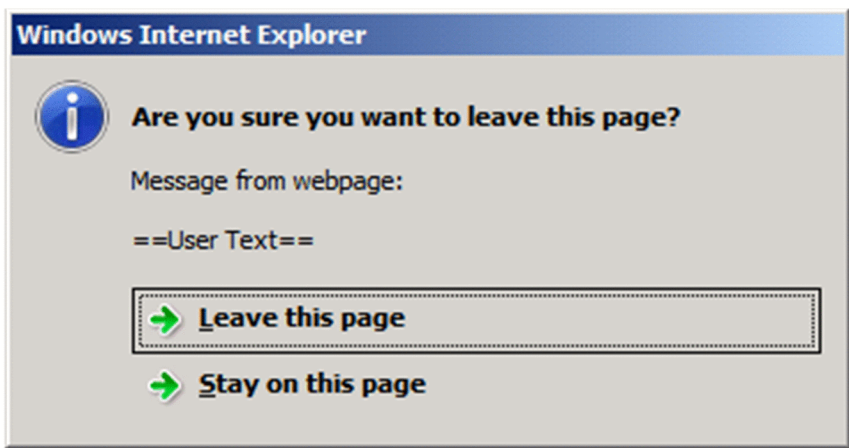
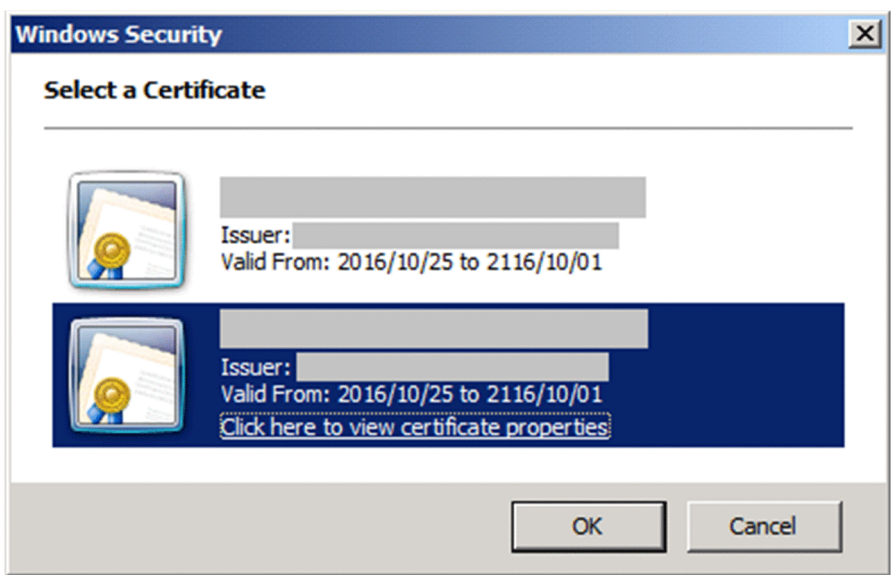
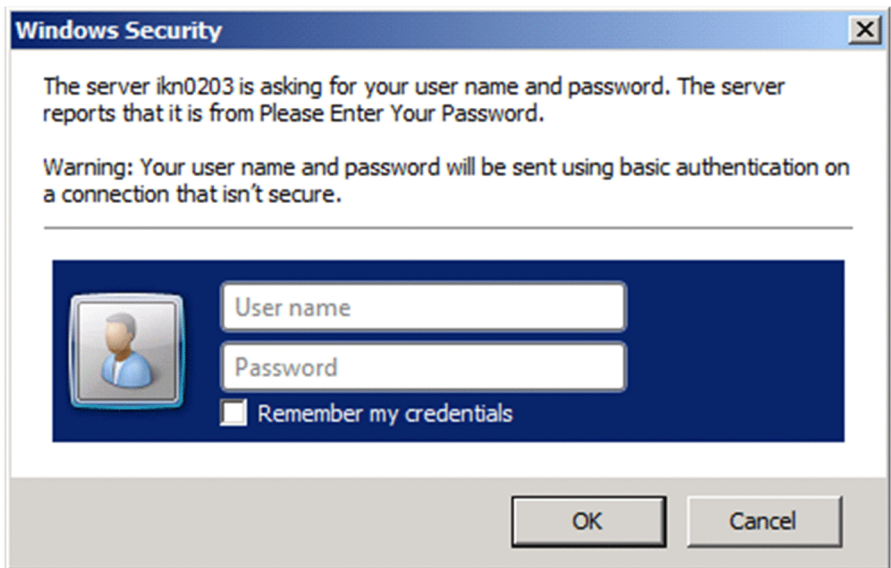
#1

The IE scenario cannot be used to monitor pages from which the following sample dialog boxes (such as a security dialog box) open.

When the IE probe is used for measurement, it cannot control the dialog box and enters the waiting state, resulting in a timeout.

If you try to replay the IE scenario in the IE Recorder, it cannot be replayed because timeout will not occur and the recorder will wait forever for the operation on the dialog box.

Figure 13–1: Dialog boxes that cannot be monitored in IE scenarios



#2

PFM - Agent for Service Response requests a Web page and replays the next operation when it receives a completion notification from the Web server. However, if it does not receive the completion notification for the Web page it

requested, and the page is automatically forwarded to another Web page through JavaScript, it cannot perform the next operation and enters the waiting state.

If the IE probe is used for measurement, a timeout occurs.

If you try to replay an operation in the IE Recorder, it cannot be replayed because timeout will not occur and the recorder will wait forever for the operation on the dialog box.

Note that some Web pages display a waiting window indicating a message such as `Waiting . . .` only when it takes time to show the window. Depending on how long it takes to show the window, the IE Recorder may be able to replay the scenario successfully, but a timeout may occur during a measurement using the IE probe.

This applies to the following sample script:

```
<html>
  <body>
    <form name="form1" action="next.html">
      <script> document.form1.submit(); </script>
    </form>
  </body>
</html>
```

(3) Value of the result code is 3 (SERVICE ERROR) Integrated Trace Log

The measurement failed because the monitored server is working properly, but it did not return the response to the request it received. An example may include the case where requested pages and files cannot be obtained (such as an HTTP 404 error) if the monitoring target is a Web server. The following table lists possible causes of the error.

Table 13–9: Possible causes when the value of the result code is 3 (SERVICE ERROR)

Cause	What you check		Action
Authentication-related information (user name or password) is incorrect.	When an Internet service is monitored: Check whether the user names and passwords for the monitored service and the proxy server specified in the measurement condition registration file (<code>esptask.xml</code>) and by using the password utility (<code>esppasswd</code> command) are correct. When a Web transaction is monitored: <ul style="list-style-type: none"> • Check whether the user names and passwords for Web authentication and the proxy server specified in the Web transaction file and by using the password utility (<code>esppasswd</code> command) are correct. • If more than one step is needed to access the Web server that requires Web authentication, check whether Web authentication is set up for all the steps. 		According to the <i>What you check</i> column, specify the correct user name and password for the monitored service.
The monitored service returns an error response.	Check the log for the monitored service (such as the Web server log) to see what the error is.		According to the <i>What you check</i> column, address the error on the monitored service.
SSL authentication failed in measurements of HTTPS (including Web transactions)	Check whether an SSL/TLS communication error occurs.	Check whether the monitored server supports the encryption algorithm and SSL/TLS communication protocol that are supported by PFM - Agent for Service Response.	<ul style="list-style-type: none"> • Configure the monitored server so that the software can connect to it using the supported encryption algorithm and SSL/TLS communication protocol. • If the monitored server does not

Cause	What you check		Action
SSL authentication failed in measurements of HTTPS (including Web transactions)	Check whether an SSL/TLS communication error occurs.	Check whether the monitored server supports the encryption algorithm and SSL/TLS communication protocol that are supported by PFM - Agent for Service Response.	support TLSv1.1 or TLSv1.2, configure PFM - Agent for Service Response not to use the corresponding protocol. ^{#1} If neither approach works, PFM - Agent for Service Response cannot be used for monitoring.
	Check for certificate errors (those that are checked for both server certificate and client certificate).	Check whether the certificates are stored in <i>installation-folder\agtv\probe\cert</i> .	If not, store them in the folder shown in the left. ^{#2}
		Check whether the certificates are using the hash algorithm supported by PFM - Agent for Service Response.	Use the hash algorithm supported by PFM - Agent for Service Response. ^{#2}
		<ul style="list-style-type: none"> • Check whether a self-signed certificate is being used. • Check whether an invalid certificate is being used, such as an expired one. 	Use the correct certificate. ^{#2}
	Check for certificate errors (those that are checked for the client certificate).	Check whether the Base64-encoded file in X.509 format is stored in <i>installation-folder\agtv\probe\cert</i> .	If not, store the Base64-encoded file in X.509 format.
		Check whether the Base64-encoded file in X.509 format contains the encrypted private key.	If not, store the Base64-encoded file in X.509 format that contains the private key there.
		Check whether the password in the client certificate matches the one specified using the password utility (<i>esppasswd</i> command).	Check the password in the client certificate and use the password utility (<i>esppasswd</i> command) to reset the password.

#1

If the Web server does not support TLSv1.1 or TLSv1.2, PFM - Agent for Service Response tries to continue to communicate with the Web server through a lower-level protocol, but it may not be able to reconnect the Web server through such a protocol. Eventually, an error occurs saying *An SSL handshake has failed*. because the Web server cannot communicate with PFM - Agent for Service Response.

This problem can sometimes be avoided if you set a `disable_ssl_protocol` key value in the [General] section of the Probe action condition definition file (`esp.conf`). For details, see the description of `disable_ssl_protocol` in [Table 8-3 Definition in the General section](#).

#2

When the software is allowed to continue processing even if an error related to the server certificate occurs, the measurement continues if the `<SSL_AUTH_IGNORE>` tag is added to the measurement condition registration file (`esptask.xml`) or Web transaction file. However, the software cannot continue the measurement when an error related to the client certificate occurs.

(4) Value of the result code is 6 (IE SCENARIO REPLAY ERROR)

PL_IESM Record

The measurement failed due to such an error that prevents the replay from continuing in IE scenario monitoring. For details about possible causes, see [5.2.3 Notes on IE scenarios](#) and [5.2.4 Notes on the navigation](#). The following table lists common problems.

Table 13–10: Possible causes when the value of the result code is 6 (IE SCENARIO REPLAY ERROR)

Cause		What you check	Action
A pop-up dialog box that is not recorded in the IE scenario appeared.		If the value of the <code>ie_service_flag</code> is set to <code>Y</code> in the [General] section of the Probe action condition definition file (<code>esp.conf</code>), check whether the account for the measurement used when the IE scenario is recorded in the IE Recorder is specified as the account for the Extensible Service IE Probe service.	Specify the account for the measurement used when the IE scenario is recorded in the IE Recorder as the account for the Extensible Service IE Probe service.
		Check whether all of the following conditions apply: <ul style="list-style-type: none"> • Internet Explorer Enhanced Security Configuration is enabled on the PFM - Agent for Service Response host. • The monitored page uses scripts and ActiveX controls. • Replays are successful in the IE Recorder (but measurements fail in the IE probe). 	See note 34. in 5.2.3 (3) Notes on recording and replaying the IE scenarios .
		Check whether the monitored page shows the security dialog box of Internet Explorer saying Revocation information for the security certificate for this site is not available. Do you want to proceed?	In Internet Explorer, open Internet Options , select the Advanced tab, and clear the Check for server certificate revocation check box.
A pop-up dialog box that is not recorded in the IE scenario appeared.	A script error occurred.	Check whether the monitored page depends on the version of Internet Explorer.	Configure either of the following settings: <ul style="list-style-type: none"> • Specify the version of the browser to connect to the page in the setting options for specifying the browser version (<code>ie_rec_browser_mode</code> and <code>ie_probe_browser_mode</code>). For details about the option, see 8.2 Probe action condition definition file (esp.conf) and 8.8 IE Recorder action condition definition file (jpcvierec.conf). • In Compatibility View Settings of Internet Explorer, add applicable monitored pages to the list of compatibility view pages. (The pages are displayed in compatibility mode.)
		Check whether the zone settings in Internet Explorer disable scripting if the monitored page uses JavaScript.	Add the monitored page to the list of trusted sites.
		Check whether the monitored page contains the cause of the script error.	Review the script so that it will not cause the script error. You may be able to measure the page depending on the settings of Internet Explorer. For details, see notes 4 and 5 in 5.2.3 (3) Notes on recording and replaying the IE scenarios .

Cause	What you check	Action
The target of an operation (such as a tag or button) during recording of the IE scenario was not found.	Check whether the monitored page has been modified since the IE scenario was recorded and the target of the operation has been removed from the page (if it has been removed, the operation when the scenario was recorded cannot be continued, causing the measurement to fail).	Re-create the IE scenario with the monitored page after the modification.
	Check whether a description in <i>5.2.4 (4) How to handle the error There is no tag that will be operated although the Web page does not change</i> applies.	Follow the description in <i>5.2.4 (4) How to handle the error There is no tag that will be operated although the Web page does not change</i> .
Others	Check whether a description in <i>5.2.3 Notes on IE scenarios</i> applies.	Follow the description in <i>5.2.3 Notes on IE scenarios</i> . Depending on the note that applies, the IE scenario may not be available for measurement. In this case, consider using the Web transaction for measurement. Note that you should read the following notes in advance to determine if the Web transaction is available for the measurement: <ul style="list-style-type: none"> • <i>5.2.2 (3) Notes about service monitoring</i> • <i>Web transaction operating environment and notes of Web Transaction (PI_WT) in 10. Records</i>

(5) Value of the result code is 7 (IE SCENARIO NAVIGATE ERROR)

PL_IESM Record

The measurement failed because an error occurred during page transition (navigation) recorded by the IE Recorder when the IE scenario was replayed.

Table 13–11: Possible causes when the value of the result code is 7 (IE SCENARIO NAVIGATE ERROR)

Cause	What you check	Action
The browser function of Windows (.NET Framework) detected an error.	Check the PL_IESM record for the code 0x800C0005.	0x800C0005 (INET_E_RESOURCE_NOT_FOUND) The server or proxy was not found. If you see the code above, the target server may not be able to be reached. Check that the monitored server, proxy server on the communication path, and other devices are up and running.
Others	Check whether any of the descriptions in <i>5.2.4 Notes on the navigation</i> applies.	Follow the description in <i>5.2.4 Notes on the navigation</i> . Depending on the note that applies, the IE scenario may not be available for measurement.

(6) Result code cannot be used to determine the cause (the measurement result itself is not returned)

The following table shows a possible cause of the error if the result code cannot be used to determine it.

Table 13–12: Possible cause when the result code cannot be used to determine the cause

Cause	What you check	Action
The last operation recorded in an IE scenario involves displaying a dialog box (to close its own window, for example).	Check whether the last operation recorded in the IE scenario involves displaying a dialog box (to close its own window, for example).	Add one more operation (such as moving to another page by entering an address) after the last operation in the IE scenario.

13.8.3 Error and normal alarms are raised alternately in PFM - Agent for Service Response measurement

In PFM - Agent for Service Response measurement, if a measurement result contains alternate error alarms and normal alarms, it may be caused by the loss of performance data to be collected.

The loss of performance data may occur if the collection interval for the Agent Collector service of PFM - Agent for Service Response (`Collection Interval` property value) is less than twice the measurement interval specified in the measurement condition registration file (`<INTERVAL>` tag value). For details about the loss of performance data, see Example 2 in [5.2.2 \(2\) Notes about Agent Collector's collection interval settings](#).

To avoid the error caused by the loss of performance data, use the following methods:

- Review the collection interval for the Agent Collector service and the measurement interval in the measurement condition registration file. (Double the collection interval for the Agent Collector service compared to the measurement interval in the measurement condition registration file.)
- Interpolate the lost performance data using the previously collected data.
For details about how to interpolate the lost data, see [3.4.4 Interpolating performance data](#).

Appendixes

A. Estimating System Requirements

Hitachi recommends that you estimate in advance whether the computer to be configured in your PFM - Agent for Service Response system has sufficient processing capacity to run the program.

A.1 Estimating memory requirements

The memory requirements vary depending on the setup conditions and on the conditions under which PFM - Agent for Service Response will be used.

For details about the formula for estimating memory requirements, see the *Release Notes*.

A.2 Estimating disk space requirements

The required disk space varies depending on the number of records used to store performance data.

To estimate the disk space requirements, you need to estimate the disk space requirements of the entire system and the Store database of Store version 1.0 or of Store version 2.0. For details about the formula for estimating these requirements, see the *Release Notes*.

A.3 Disk space requirements for operation in a cluster system

The disk space requirements for cluster use are the same as for non-cluster system operation. For details about the disk space requirements, see the *Release Notes*.

B. List of Identifiers

To operate PFM - Agent for Service Response or to extract performance data from the Store database of PFM - Agent for Service Response, identifiers are required so that the system can identify PFM - Agent for Service Response. The following table shows the identifiers of PFM - Agent for Service Response.

Table B–1: Identifiers of PFM - Agent for Service Response

Use	Name	Identifier	Description
Commands, etc.	Product ID	v	The product ID is part of the service ID. The service ID is required for commands that perform operations, such as checking the system configuration of the Performance Management series and backing up performance data. For details about the service ID, see the naming rule in the <i>JP1/Performance Management Planning and Configuration Guide</i> .
	Service key	agt or SR	This identifier is needed in order to use commands to start and stop PFM - Agent for Service Response. For details about service keys, see the naming rule in the <i>JP1/Performance Management Planning and Configuration Guide</i> .
Help	Help ID	pcav	This is the identifier for PFM - Agent for Service Response help.

C. List of Processes

This appendix lists the processes of PFM - Agent for Service Response.

For details about the processes of PFM - Manager, PFM - Web Console, and PFM - Base, see the Appendixes in the manual *JP1/Performance Management Reference*.

The following table lists the processes of PFM - Agent for Service Response. The value in parentheses following each process name is the number of instances of that process that can run concurrently.

Table C–1: Processes of PFM - Agent for Service Response

Process name (Number of processes)	Function
<code>jpcagtv.exe</code> (1)	Process of the Agent Collector service. One instance of this process is started for each PFM - Agent for Service Response.
<code>jpcsto.exe</code> (1)	Process of the Agent Store service. One instance of this process is started for each PFM - Manager and each PFM - Agent.
<code>jpcvieprobed.exe</code> (5) #1	IE Probe Daemon. Five instances of this process are started for each PFM - Agent for Service Response.
<code>esprobed.exe</code> (1)	Probe Daemon. One instance of this process is started for each PFM - Agent for Service Response.
<code>jpcviemd.exe</code> (1)	Process for controlling a system tray button and the IE Probe Daemon process to start, scheduling IE scenario measurement, and outputting the reports.
<code>espsvc.exe</code> (1)	Probe Daemon service process; performs communication between Probe Daemon and Windows service control manager. One instance of this process is started for each PFM - Agent for Service Response.
<code>jpcviesvc.exe</code> (1)	IE Probe Daemon service process; performs communication between IE Probe Daemon and Windows service control manager. One instance of this process is started for each PFM - Agent for Service Response.
<code>stpqlpr.exe</code> (1) #2	Process for executing a backup or export of the Store database.
<code>espwebrec.exe</code> #3	Web Recorder process.
<code>JpcvIERec.exe</code> (1)	IE Recorder process.
<code>esprobed_tm.exe</code> (1)	Process for executing a Web transaction measurement test. This process is executed by the <code>jpcvtest</code> command.

#1

This is a default value.

#2

This is a child process of the `jpcsto.exe` process.

#3

There is no restriction on the number of processes that can be executed simultaneously.

D. List of Port Numbers

This appendix lists the port numbers used by PFM - Agent for Service Response.

For details about the port numbers for PFM - Manager, PFM - Web Console, and PFM - Base, and the firewall passage directions, see the Appendixes in the manual *JPI/Performance Management Reference*.

You can change a port number to suit your system environment. For details about how to change a port number, see the chapter that describes installation and setup in the *JPI/Performance Management Planning and Configuration Guide*. The TCP/IP protocol is used.

Note:

Performance Management supports static NAT (Basic NAT) that performs one-to-one address conversion.

It does not support dynamic NAT or NAT (IP Masquerade, NAT+) that includes a port conversion function.

D.1 Port numbers of PFM - Agent for Service Response

The following table explains the port numbers used by PFM - Agent for Service Response.

Table D–1: Port numbers used by PFM - Agent for Service Response

Port number	Service name	Parameter	Usage
--	Agent Store service	jp1pcstov	Used to record performance data and acquire historical reports.
--	Agent Collector service	jp1pcagtv	Used to bind alarms and acquire real-time reports.

Legend:

--: When the `jpccconf port define` command is executed, a port number that is not in use is automatically assigned and displayed. If the `jpccconf port define` command is not executed, the system automatically assigns a port number that is not in use each time the service is restarted.

D.2 Firewall passage directions

(1) Setting firewall passage directions

If there is a firewall between PFM - Manager and PFM - Agent for Service Response, you must set fixed port numbers for all services of PFM - Manager and PFM - Agent.

For more details, see the section describing the firewall passage direction in the manual *JPI/Performance Management Reference*.

(2) Setting firewall passage directions (for logical host operation)

If there is a firewall between PFM - Manager and PFM - Agent for Service Response, you must set fixed port numbers for all services of PFM - Manager and PFM - Agent. To enable communications to all services to pass through the firewall, the port numbers that you set must comply with the directions shown in the following table.

Table D–2: Firewall passage directions (between PFM - Manager and PFM - Agent (for logical host operation))

Service name	Parameter	Passage directions
Agent Store service (logical host)	jp1pcstov	Agent (logical host) ← Manager
Agent Collector service (logical host)	jp1pcagtν	Agent (logical host) ← Manager

Legend:

Manager: PFM - Manager host

Agent (logical host): PFM - Agent host

←: Direction in which communication (connection) begins, from the right-hand item to the left-hand item.

When communication (connection) is initiated, the receiving side (the side indicated by the tip of the arrow) uses the port numbers shown in Table D-1 as receiving ports. The connecting side uses the free port numbers assigned by the OS as sending ports. The available range of port numbers depends on the OS.

When a connection is initiated from Manager to Agent as shown above, set the firewall so that the sending ports temporarily used by Manager can pass through to the receiving ports of Agent.

D.3 Notes on measurement in a firewall/NAT environment

If there is a firewall/NAT between PFM - Agent for Service Response host and the target services for measuring, you need to set the communications that can pass through the firewall/NAT for each target service.

The following table lists how to set the communications that can pass through the firewall/NAT for each target service.

Table D–3: How to set the communications that can pass through the firewall/NAT for each target service

Target service for measuring	How to set	Port number
<ul style="list-style-type: none"> • DHCP • DNS • FTP • HTTP • HTTPS • IMAP4 • POP3 • SMTP 	Set the port numbers for the communication protocol that can pass through the firewall/NAT.	--
TCP	Set the port numbers for TCP communication specification (IP address, port number) that can pass through the firewall/NAT.	--
<ul style="list-style-type: none"> • Web transactions • IE scenarios 	Set the port numbers for the target Web pages that can pass through the firewall/NAT.	--
User-defined services	Set the port numbers for the user-defined programs that can pass through the firewall/NAT.	--

Legend:

--: Port numbers vary depending on the target services for measuring.

E. Properties of PFM - Agent for Service Response

This appendix lists the properties of the Agent Store and Agent Collector services of PFM - Agent for Service Response that are displayed in PFM - Web Console.

E.1 Agent Store service properties

The following table lists the properties of the Agent Store service of PFM - Agent for Service Response.

Table E–1: Properties of the Agent Store service of PFM - Agent for Service Response

Folder name	Property name	Description
--	First Registration Date	Displays the first date and time the service was recognized by PFM - Manager.
	Last Registration Date	Displays the most recent date and time the service was recognized by PFM - Manager.
General	--	Stores information such as host names and folders. You cannot change properties stored in this folder.
	Directory	Displays the name of the current folder where the service is running.
	Host Name	Displays the name of the physical host where the service is running.
	Process ID	Displays the service's process ID.
	Physical Address	If the IPv6 communication function is disabled, displays the IP address and port number of the host where the service is running.
	Physical Address(IPv4)	If the IPv6 communication function is enabled, displays the IP address (IPv4) of the host where the service is running.
	Physical Address(IPv6)	If the IPv6 communication function is enabled, displays the IP address (IPv6) of the host where the service is running.
	Port Number	If the IPv6 communication function is enabled, displays the port number of the host where the service is running.
	User Name	Displays the name of the user who executed the service process.
	Time Zone	Displays the time zone in which the service is used.
System	--	Stores information about the operating system where the service is running. You cannot change properties stored in this folder.
	CPU Type	Displays the CPU type.
	Hardware ID	Displays the hardware ID.
	OS Type	Displays the type of operating system.
	OS Name	Displays the name of the operating system.
	OS Version	Displays the version of the operating system.
Network Services	--	Stores information about the Performance Management communication common library. You cannot change properties stored in this folder.
	Build Date	Displays the creation date of the Agent Store service.
	INI File	Displays the name of the directory containing the <code>jpcns.ini</code> file.

Folder name		Property name	Description
Network Services	Service	--	Stores information about the service. You cannot change properties stored in this folder.
		Description	Displays the host name.
		Local Service Name	Displays the service ID.
		Remote Service Name	Displays the service ID of the Master Manager service at the connection-target PFM - Manager host.
		EP Service Name	Displays the service ID of the Correlator service at the connection-target PFM - Manager host.
Retention		--	Specifies the retention period for records when the Store version is 1.0. For details, see the chapter explaining management of operation monitoring data in the <i>JP1/Performance Management User's Guide</i> .
		Product Interval - Minute Drawer	Specifies the retention period for records of the P I record type that are collected each minute. The following periods can be selected: <ul style="list-style-type: none"> • Minute • Hour • Day • 2 Days • 3 Days • 4 Days • 5 Days • 6 Days • Week • Month • Year
		Product Interval - Hour Drawer	Specifies the retention period for records of the P I record type that are collected hourly. The following periods can be selected: <ul style="list-style-type: none"> • Hour • Day • 2 Days • 3 Days • 4 Days • 5 Days • 6 Days • Week • Month • Year
		Product Interval - Day Drawer	Specifies the retention period for records of the P I record type that are collected daily. The following periods can be selected: <ul style="list-style-type: none"> • Day • 2 Days • 3 Days • 4 Days • 5 Days • 6 Days • Week • Month • Year
		Product Interval - Week Drawer	Specifies the retention period for records of the P I record type that are collected weekly. The following periods can be selected:

Folder name		Property name	Description
Retention		Product Interval - Week Drawer	<ul style="list-style-type: none"> • Week • Month • Year
		Product Interval - Month Drawer	Specifies the retention period for records of the PI record type that are collected monthly. The following periods can be selected: <ul style="list-style-type: none"> • Month • Year
		Product Interval - Year Drawer	Specifies the retention period for records of the PI record type that are collected annually. This retention period is fixed to Year .
		Product Detail - <i>record-ID-of-PD-record-type</i>	For a record of the PD record type, specifies the number of records to be saved. You can specify an integer in the range from 0 to 2,147,483,647 (inclusive). <i>Note:</i> An error message is displayed if you specify an out-of-range value or a non-numeric character.
RetentionEx		--	Specifies the retention period for records when the Store version is 2.0. For details, see the chapter explaining management of operation monitoring data in the <i>JP1/Performance Management User's Guide</i> .
RetentionEx	Product Interval - <i>record-ID-of-PI-type-record</i>	--	Specifies the record retention period for PI -type records.
		Period - Minute Drawer (Day)	Specifies the minute-by-minute performance data retention period for each PI -type record ID. An integer in the range from 0 to 366 can be specified for the retention period (number of days).
		Period - Hour Drawer (Day)	Sets the hourly performance data retention period for each PI -type record ID. An integer in the range from 0 to 366 can be specified for the retention period (number of days).
		Period - Day Drawer (Week)	Sets the daily performance data retention period for each PI -type record ID. An integer in the range from 0 to 522 can be specified for the retention period (number of weeks).
		Period - Week Drawer (Week)	Sets the weekly performance data retention period for each PI -type record ID. An integer in the range from 0 to 522 can be specified for the retention period (number of weeks).
		Period - Month Drawer (Month)	Sets the monthly performance data retention period for each PI -type record ID. An integer in the range from 0 to 120 can be specified for the retention period (number of months).
		Period - Year Drawer (Year)	Displays the yearly performance data retention period for each PI -type record ID.
	Product Detail - <i>record-ID-of-PD-type-record</i>	Period (Day)	Sets the performance data retention period for each PD -type record ID. An integer in the range from 0 to 366 can be specified for the retention period (number of days).
Product Log - <i>record-ID-of-PL-type-record</i>	Period (Day)	Specifies the performance data retention period for each PL -type record ID. An integer in the range from 0 to 366 can be specified for the retention period (number of days).	

Folder name	Property name	Description
Disk Usage	--	This folder stores the amounts of disk space used by each database. Displayed disk space usage values are current as of the time of the display. You cannot change the properties stored in this directory.
	Product Interval	Displays the disk space used by records of the <code>PI</code> record type.
	Product Detail	Displays the disk space used by records of the <code>PD</code> record type.
	Product Alarm	Displays the disk space used by records of the <code>PA</code> record type. PFM - Agent for Service Response does not use this property.
	Product Log	Displays the disk space used by records of the <code>PL</code> record type. PFM - Agent for Service Response does not use this property.
	Total Disk Usage	Displays the total amount of disk space used by the entire database.
Configuration	--	Displays the properties of the Agent Store service.
	Store Version	Displays the Store database version. <ul style="list-style-type: none"> • For Store version 1.0: 1.0 • For Store version 2.0: 2.0
Multiple Manager Configuration	Primary Manager	Displays the host name of the manager specified as the primary manager for multiple monitoring. This property cannot be changed.
	Secondary Manager	Displays the host name of the manager specified as the secondary manager for multiple monitoring. This property cannot be changed.

Legend:

--: Not applicable

E.2 Agent Collector service properties

The following table lists the properties of the Agent Collector service of PFM - Agent for Service Response.

Table E-2: Properties of the Agent Collector service of PFM - Agent for Service Response

Folder name	Property name	Description
--	First Registration Date	Displays the first date and time the service was recognized by PFM - Manager.
	Last Registration Date	Displays the most recent date and time the service was recognized by PFM - Manager.
	Data Model Version	Displays the version of the data model.
General	--	Stores information such as host names and folders. You cannot change properties stored in this folder.
	Directory	Displays the name of the current folder where the service is running.
	Host Name	Displays the name of the physical host where the service is running.
	Process ID	Displays the service's process ID.
	Physical Address	If the IPv6 communication function is disabled, displays the IP address and port number of the host where the service is running.

Folder name		Property name	Description
General		Physical Address(IPv4)	If the IPv6 communication function is enabled, displays the IP address (IPv4) of the host where the service is running.
		Physical Address(IPv6)	If the IPv6 communication function is enabled, displays the IP address (IPv6) of the host where the service is running.
		Port Number	If the IPv6 communication function is enabled, displays the port number of the host where the service is running.
		User Name	Displays the name of the user who executed the service process.
		Time Zone	Displays the time zone in which the service is used.
System		--	Stores information about the operating system where the service is running. You cannot change properties stored in this folder.
		CPU Type	Displays the CPU type.
		Hardware ID	Displays the hardware ID.
		OS Type	Displays the type of operating system.
		OS Name	Displays the name of the operating system.
		OS Version	Displays the version of the operating system.
Network Services		--	Stores information about the Performance Management communication common library. You cannot change properties stored in this folder.
		Build Date	Displays the creation date of the Agent Store service.
		INI File	Displays the name of the directory containing the <code>jpcns.ini</code> file.
Network Services	Service	--	Stores information about the service. You cannot change properties stored in this folder.
		Description	Displays additional service information, such as host name and service type.
		Local Service Name	Displays the service ID.
		Remote Service Name	Displays the service ID of the Agent Store service to which the Agent Collector service connects.
		AH Service Name	Displays the service ID of the Action Handler service on the same host.
JP1 Event Configurations		--	Sets the condition for issuing JP1 events.
		<i>service</i>	Yes or No is selected from a list for the Agent Collector service, Agent Store service, Action Handler service, and Status Server service to specify whether to output JP1 system events for each service.
		JP1 Event Send Host	Specifies the name of the event server to which JP1/Base connects. However, only the event server running on the logical host or physical host on the same machine as for the Action Handler service can be specified. From 0 to 255 bytes of alphanumeric characters, periods (.), and hyphens (-) can be specified. If a value outside this range is specified, it is assumed that no value has been specified. If no value is specified, the host on which the Action Handler service is running is used as the host that issues events. If localhost is specified, the physical host is assumed.
		Monitoring Console Host	Specifies the PFM - Web Console host that is to be started by starting the JP1/IM - Manager monitor. From 0 to 255 bytes of alphanumeric characters, periods (.), and hyphens (-). If a value outside this range is

Folder name		Property name	Description
JP1 Event Configurations		Monitoring Console Host	specified, it is assumed that no value has been specified. If no value is specified, the PFM - Manager host to be connected is assumed.
		Monitoring Console Port	Specifies the port number of PFM - Web Console (http request port number) to be started. A value in the range from 1 to 65,535 can be specified. If a value outside this range is specified, it is assumed that no value has been specified. If no value is specified, 20358 is set.
		Monitoring Console Https	Specifies whether to use HTTPS-encrypted communication to access PFM - Web Console when PFM - Web Console is started by JP1/IM - Manager monitor startup. By default, this property is set to No . <ul style="list-style-type: none"> • Yes: Use encrypted communication. • No: Do not use encrypted communication.
JP1 Event Configurations	Alarm	JP1 Event Mode	Specifies which of the following events is to be issued if the alarm status changes. <ul style="list-style-type: none"> • JP1 User Event: A JP1 user event is issued. • JP1 System Event: A JP1 system event is issued.
Detail Records		--	Stores the properties of records of the PD record type. The record IDs of the collected records are displayed in boldface type.
Detail Records	<i>record-ID</i> ^{#1}	--	Stores the properties of a record.
		Description	Displays a description of the record. You cannot change this property.
		Log	Select Yes or No from the list to specify whether or not the record is to be logged into (stored in) the Store database. If this value is set to Yes and Collection Interval is set to a value greater than 0, the record is logged into the database.
		Log(ITSLM)	Displays Yes or No to indicate whether JP1/SLM - Manager logs the record into the Store database of PFM - Agent for Service Response when JP1/SLM - Manager is linked. If JP1/SLM - Manager is not linked, No is always displayed. You cannot change this property.
		Monitoring(ITSLM)	Displays Yes or No for the JP1/SLM - Manager setting to indicate whether the record is to be sent to JP1/SLM - Manager when JP1/SLM - Manager is linked. If JP1/SLM - Manager is not linked, No is always displayed. You cannot change this property.
		Collection Interval	Specifies the data collection interval. You can specify a value in the range from 0 to 2,147,483,647 seconds (inclusive) in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.
		Collection Offset	Specifies the offset value (in seconds) for starting data collection. The specified value must not exceed the value specified for Collection Interval, and must be in the range from 0 to 32,767 seconds (inclusive). The storage time for data collection does not depend on the Collection Offset value, and is the same time as the Collection Interval.
		Over 10 Sec Collection Time	This property is only displayed if collection of historical data takes precedence over the display processing of real-time reports (if the functionality that prioritizes the collection of historical data is enabled). Whether record collection might require 10 seconds or more is indicated by Yes or No . <ul style="list-style-type: none"> • Yes: Might require 10 seconds or more. • No: Does not require 10 seconds. The value of this property cannot be changed.
		Realtime Report Data Collection Mode	This property is only displayed if collection of historical data takes precedence over the display processing of real-time reports (if the

Folder name		Property name	Description
Detail Records	<i>record-ID</i> ^{#1}	Realtime Report Data Collection Mode	<p>functionality that prioritizes the collection of historical data is enabled). Specifies the display mode of the real-time report.</p> <ul style="list-style-type: none"> • Reschedule: Reschedule mode • Temporary Log: Temporary save mode <p>Note that temporary save mode (Temporary Log) must be specified for records whose Over 10 Sec Collection Time value is Yes.</p> <p>Specifies the condition for registering records in the database. Only those records satisfying the condition are registered in the database. Displays the conditional expression (character string) created in the LOGIF Expression Setting window, which is displayed by clicking LOGIF on the bottom frame of the Property window of the service that is displayed under the Services tab in PFM - Web Console.</p>
		LOGIF	<p>Specifies the condition for registering records in the database. Only those records satisfying the condition are registered in the database. Displays the conditional expression (character string) created in the LOGIF Expression Setting window, which is displayed by clicking LOGIF on the bottom frame of the Property window of the service that is displayed under the Services tab in PFM - Web Console.</p>
Interval Records		--	Stores the properties of records of the PI record type. The record IDs of the collected records are displayed in boldface type.
Interval Records	<i>record-ID</i> ^{#1}	--	Stores the properties of a record.
		Description	Displays a description of the record. You cannot change this property.
		Log	Select Yes or No from the list to specify whether or not the record is to be logged into (stored in) the Store database. If this value is set to Yes and Collection Interval is set to a value greater than 0, the record is logged into the database.
		Log(ITSLM)	Displays Yes or No to indicate whether JP1/SLM - Manager logs the record into the Store database of PFM - Agent for Service Response when JP1/SLM - Manager is linked. If JP1/SLM - Manager is not linked, No is always displayed. You cannot change this property.
		Monitoring(ITSLM)	Displays Yes or No for the JP1/SLM - Manager setting to indicate whether the record is to be sent to JP1/SLM - Manager when JP1/SLM - Manager is linked. If JP1/SLM - Manager is not linked, No is always displayed. You cannot change this property.
		Collection Interval	Specifies the data collection interval. You can specify a value in the range from 0 to 2,147,483,647 seconds (inclusive) in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.
		Collection Offset	Specifies the offset value (in seconds) for starting data collection. The specified value must not exceed the value specified for Collection Interval, and must be in the range from 0 to 32,767 seconds (inclusive). The storage time for data collection does not depend on the Collection Offset value, and is the same time as the Collection Interval.
		Over 10 Sec Collection Time	<p>This property is only displayed if collection of historical data takes precedence over the display processing of real-time reports (if the functionality that prioritizes the collection of historical data is enabled).^{#2} Whether record collection might require 10 seconds or more is indicated by Yes or No.</p> <ul style="list-style-type: none"> • Yes: Might require 10 seconds or more. • No: Does not require 10 seconds. <p>The value of this property cannot be changed.</p>

Folder name		Property name	Description		
Interval Records	<i>record-ID</i> ^{#1}	Realtime Report Data Collection Mode	<p>This property is only displayed if collection of historical data takes precedence over the display processing of real-time reports (if the functionality that prioritizes the collection of historical data is enabled).^{#2} Specifies the display mode of the real-time report.</p> <ul style="list-style-type: none"> • Reschedule: Reschedule mode • Temporary Log: Temporary save mode <p>Note that temporary save mode (Temporary Log) must be specified for records whose Over 10 Sec Collection Time value is Yes.</p>		
		LOGIF	<p>Specifies the condition for registering records in the database. Only those records satisfying the condition are registered in the database. Displays the conditional expression (character string) created in the LOGIF Expression Setting window, which is displayed by clicking LOGIF on the bottom frame of the Property window of the service that is displayed under the Services tab in PFM - Web Console.</p>		
Log Records		Description	Displays a description of the record. You cannot change this property.		
		Log	Select Yes or No from the list to specify whether or not the record is to be logged into (stored in) the Store database. If this value is set to Yes and Collection Interval is set to a value greater than 0, the record is logged into the database.		
		Collection Interval	Specifies the data collection interval. You can specify a value in the range from 0 to 2,147,483,647 seconds (inclusive) in increments of 1. If you specify 0 for the property, 0 seconds is assumed, in which case no data is collected.		
		Collection Offset	Specifies the offset value (in seconds) for starting data collection. The specified value must not exceed the value specified for Collection Interval, and must be in the range from 0 to 32,767 seconds (inclusive). The storage time for data collection does not depend on the Collection Offset value, and is the same time as the Collection Interval.		
Agent Configuration		LOGIF	Specifies the condition for registering records in the database. Only those records satisfying the condition are registered in the database. Displays the conditional expression (character string) created in the LOGIF Expression Setting window, which is displayed by clicking LOGIF on the bottom frame of the Property window of the service that is displayed under the Services tab in PFM - Web Console.		
		--	Stores the properties of the records for the settings of the data interpolation and the probe.		
		Agent Configuration	Agent	--	Stores the properties of records for the data interpolation.
		Data Interpolation	Select Yes or No from the list to specify whether or not you use the last stored data to interpolate data when the performance data is not stored. If this value is Yes , the last stored data is interpolated when the performance data is not stored.		
Agent Configuration		Probe	--	Stores the properties of records for setting the probe.	
		Use Probe	<p>Select Yes or No from the list to specify whether or not the Probe Daemon is to start when the Agent Collector service starts. If this value is Yes, the Probe Daemon is to start when the Agent Collector service starts. If this value is No, the Probe Daemon is not to start when the Agent Collector service starts.</p> <p>If this value is set to Yes and the Probe Daemon is stopped, the Probe Daemon is starting. If this value is set to No and the Probe Daemon is started, the Probe Daemon is stopping.</p>		

Folder name		Property name	Description
Agent Configuration	Probe	Reload	Select Yes or No from the list to specify whether or not the measurement condition registration file is to be reloaded. If this value is set to Yes , the measurement condition registration file is reloaded.
		Probe Status	Displays the status of the Probe Daemon, and one of the following values can be displayed: <ul style="list-style-type: none"> • Active The Probe Daemon is started or stopping. • Inactive The Probe Daemon is stopped or starting. • Unknown Failure to collect the Probe Daemon status. • Reloading The Probe Daemon is reloading.
		IE Probe Status	Displays the status of the IE Probe Daemon, and one of the following values can be specified: <ul style="list-style-type: none"> • Active The IE Probe Daemon is started or stopping. • Inactive The IE Probe Daemon is stopped or starting. • Unknown Failure to collect the IE Probe Daemon status. • Reloading The IE Probe Daemon is stopped or starting.
		Initial	Displays the number of the tasks which are added but whose properties are not specified.
		Invalid	Displays the number of the tasks one or more of whose property values are invalid.
		Valid	Displays the number of the tasks one or more of whose properties are updated. To apply the changes, the measurement condition registration file must be reloaded.
		Deleted	Displays the number of the deleted tasks. To apply the changes, the measurement condition registration file must be reloaded.
		Applied	Displays the number of the registered tasks in the measurement condition registration file.
		Probe\Task List ^{#2}	--
	Probe\ADD OR DELETE A TASK ^{#3}	--	Stores the properties of the records for the settings to add or delete the measurement conditions.
		New Task ID	Specifies the measurement condition ID.
		New Task Protocol	Select one of the following protocols from the list to create a new task: <ul style="list-style-type: none"> • HTTP • HTTPS • SMTP • POP3 • IMAP4 • DNS • DHCP • FTP

Folder name		Property name	Description
Agent Configuration	Probe\ADD OR DELETE A TASK#3	New Task Protocol	<ul style="list-style-type: none"> TCP WEBTRANS USERSERV
		Delete A Task	Specifies the task to be deleted; otherwise, specifies None .
		Reserved	Reserved record. Not available for use.
Restart Configurations		--	Sets the condition for automatically restarting the PFM service. The condition can be set when the version of PFM - Manager or PFM - Base is 09-00 or later. For details about the PFM service Auto-restart functionality, see the chapter explaining the Performance Management functions in the <i>JP1/Performance Management Planning and Configuration Guide</i> .
		Restart when Abnormal Status	Specifies whether to automatically restart the service if the Status Server service cannot correctly obtain the statuses of the Action Handler service, Agent Collector service, and Agent Store service.
		Restart when Single Service Running	Specifies whether to automatically restart the service if only the Agent Store service or only the Agent Collector service is running.
Restart Configurations	Action Handler	Auto Restart	Specifies whether to use the Auto-restart functionality for the Action Handler service.
		Auto Restart - Interval (Minute)	Specifies the interval for checking the operating status of the service when Auto-restart is used. You can specify a value in the range from 1 to 1,440 minutes (inclusive) in increments of 1.
		Auto Restart - Repeat Limit	Specifies the number of times a restart is retried in succession when Auto-restart is used. You can specify an integer in the range from 1 to 10.
		Scheduled Restart	Select Yes or No from the list to specify whether to use Scheduled restart for the Action Handler service.
		Scheduled Restart - Interval	Sets the restart interval as an integer in the range from 1 to 1,000 when Scheduled restart is used.
		Scheduled Restart - Interval Unit	Select Hour , Day , Week , or Month from the list as the unit of the restart interval when Scheduled restart is used.
		Scheduled Restart - Origin - Year	The restart year can be specified as an integer in the range from 1971 to 2035.
		Scheduled Restart - Origin - Month	The restart month can be specified as an integer in the range from 1 to 12.
		Scheduled Restart - Origin - Day	The restart day can be specified as an integer in the range from 1 to 31.
		Scheduled Restart - Origin - Hour	The restart time (hour) can be specified as an integer in the range from 0 to 23.
	Scheduled Restart - Origin - Minute	The restart time (minute) can be specified as an integer in the range from 0 to 59.	
	Agent Collector	Auto Restart	Specifies whether to use the Auto-restart functionality for the Agent Collector service.
Auto Restart - Interval (Minute)		Specifies the interval for checking the operating status of the service when Auto-restart is used. You can specify a value in the range from 1 to 1,440 minutes (inclusive) in increments of 1.	

Folder name		Property name	Description
Restart Configurations	Agent Collector	Auto Restart - Repeat Limit	Specifies the number of times a restart is retried in succession when Auto-restart is used. You can specify an integer in the range from 1 to 10.
		Scheduled Restart	Select Yes or No from the list to specify whether to use Scheduled restart for the Agent Collector service.
		Scheduled Restart - Interval	Sets the restart interval as an integer in the range from 1 to 1,000 when Scheduled restart is used.
		Scheduled Restart - Interval Unit	Select Hour , Day , Week , or Month from the list as the unit of the restart interval when Scheduled restart is used.
		Scheduled Restart - Origin - Year	The restart year can be specified as an integer in the range from 1971 to 2035.
		Scheduled Restart - Origin - Month	The restart month can be specified as an integer in the range from 1 to 12.
		Scheduled Restart - Origin - Day	The restart day can be specified as an integer in the range from 1 to 31.
		Scheduled Restart - Origin - Hour	The restart time (hour) can be specified as an integer in the range from 0 to 23.
		Scheduled Restart - Origin - Minute	The restart time (minute) can be specified as an integer in the range from 0 to 59.
	Agent Store	Auto Restart	Specifies whether to use the Auto-restart functionality for the Agent Store service.
		Auto Restart - Interval (Minute)	Specifies the interval for checking the operating status of the service when Auto-restart is used. You can specify a value in the range from 1 to 1,440 minutes (inclusive) in increments of 1.
		Auto Restart - Repeat Limit	Specifies the number of times a restart is retried in succession when Auto-restart is used. You can specify an integer in the range from 1 to 10.
		Scheduled Restart	Select Yes or No from the list to specify whether to use Scheduled restart for the Agent Store service.
		Scheduled Restart - Interval	Sets the restart interval as an integer in the range from 1 to 1,000 when Scheduled restart is used.
		Scheduled Restart - Interval Unit	Select Hour , Day , Week , or Month from the list as the unit of the restart interval when Scheduled restart is used.
		Scheduled Restart - Origin - Year	The restart year can be specified as an integer in the range from 1971 to 2035.
		Scheduled Restart - Origin - Month	The restart month can be specified as an integer in the range from 1 to 12.
		Scheduled Restart - Origin - Day	The restart day can be specified as an integer in the range from 1 to 31.
		Scheduled Restart - Origin - Hour	The restart time (hour) can be specified as an integer in the range from 0 to 23.
Scheduled Restart - Origin - Minute	The restart time (minute) can be specified as an integer in the range from 0 to 59.		
ITSLM Connection Configuration	--	Displays information about the linked JP1/SLM - Manager.	

Folder name		Property name	Description
ITSLM Connection Configuration	ITSLM Connection	--	Displays information about the connection-target JP1/SLM - Manager.
		ITSLM Host	Displays the host name of the connected JP1/SLM - Manager. This property is displayed only when JP1/SLM - Manager is connected.
		ITSLM Port	Displays the port number of the connected JP1/SLM - Manager. This property is displayed only when JP1/SLM - Manager is connected.
	MANAGE ITSLM CONNECTION	--	Specifies whether to disconnect JP1/SLM - Manager.
		DISCONNECT ITSLM CONNECTION	From the list, select the host name of the JP1/SLM - Manager to be disconnected. If (empty string) is selected in the list, the system performs no action. If JP1/SLM - Manager is not connected, the list contains only (empty string) .
Multiple Manager Configuration	Primary Manager	Displays the host name of the manager specified as the primary manager for multiple monitoring. This property cannot be changed.	
	Secondary Manager	Displays the host name of the manager specified as the secondary manager for multiple monitoring. This property cannot be changed.	

Legend:

--: Not applicable

#1

The folder name shows the record ID without the database ID. For details about the record ID of each record, see [10. Records](#).

#2

This Probe\Task List means that the Task List folder is under the Probe folder. For details about the properties stored in this folder, see Table E-3.

#3

This Probe\ADD OR DELETE A TASK means that the ADD OR DELETE A TASK folder is under the Probe folder. For details about the properties stored in this folder, see Table E-3.

The properties of measurement condition for the Agent Collector service of PFM - Agent for Service Response are stored in the \Agent Configuration\Probe\Task List folder.

The following table lists the properties of the measurement condition:

Table E-3: Properties of the measurement condition

Folder name#1	Property name	XML tag#2	Description
<i>service-name</i> _[0-9]+	--	--	<i>service-name</i> displays any one of the following services: HTTP, HTTPS, SMTP, POP3, IMAP4, DNS, DHCP, FTP, TCP, WEBTRANS or USERSERV services. Task ID, Status, Task Label, Interval and Timeout properties are the common properties, regardless of the type of the measurement services.#1
	Task ID	<TASKID>	Displays the measurement condition ID.
	Status	--	As the setting status of the task's status property and the apply status of the Probe Daemon, display the following statuses: <ul style="list-style-type: none"> Applied The status that the settings are applied to the Probe Daemon. Deleted

Folder name#1	Property name	XML tag#2	Description
service-name _[0-9]+	Status	--	<p>The status that the settings are deleted, but are not applied to the Probe Daemon.</p> <ul style="list-style-type: none"> Initial The status between the time a task is newly created and the time you click the OK button for the first time. Invalid The status that the properties with the invalid values exist. The property names with the invalid values are separated by comma (,), surrounded by brackets ([]), and displayed after the "Invalid". Valid The status that all the necessary properties are properly input but the settings are not applied to the Probe Daemon.
	Task Label	<TASKLABEL>	<p>Specifies a label name if you give any label name to the task. Hitachi recommends that the name is unique among the other task labels in the other measurement conditions.</p> <p>The label names are stored in the Measurement Condition Name field in each record. You cannot use the comma (,) and double quotation mark (") to specify the label names. PFM - Web Console 08-50 or later supports Japanese (multibyte character sets) in a Japanese environment or Chinese (multibyte character sets, except for 4-byte characters) in a Chinese environment.</p> <p>If no value is specified, the value specified in the measurement condition label definition file is assumed to be the task label. In this case, the task label cannot be checked as the properties.</p>
	Interval	<INTERVAL>	<p>Specifies the interval time in seconds when measuring repeatedly. None is set by default. Specifies the value that is greater than the value of the Timeout property (timeout value).</p>
	Timeout	<TIMEOUT>	<p>Specifies the maximum amount of time in seconds within which a single measurement must be completed.</p> <p>Specifies the value that is smaller than the value of the Interval property.</p>
HTTP_[0-9]+	--	--	Stores the properties for measuring the HTTP service.
	URL#3	<URL>	<p>Specifies the URL of the measuring target Web page up to 255-byte characters. None is set by default.</p> <p>The protocol identifier (http://) is not included. The port number can be omitted. If the port number is omitted, the port number 80 is used.</p>
	Method	<POST>#4	<p>Displays the request method. The default value is GET. You cannot use PFM - Web Console to change this value. As a result, if you use the POST method, edit the measurement condition registration file directly or define the measurement condition as a Web transaction.</p> <p>PFM - Web Console cannot display a character string to be sent as the message body (specified as the value of the <MESSAGE_BODY> tag in the measurement condition registration file) using the POST method. If the <MESSAGE_BODY> tag is specified in the measurement condition registration file, the specified value is not checked.</p>
	Depth	<DEPTH>	<p>Specifies the depth of embedded resources and frames to be acquired within the range from 1 to 100 bytes. This is the depth of the resources and frames in the Web page that are to be downloaded. The following shows examples:</p> <p>DEPTH=1 is specified: Only the Web page is downloaded.</p> <p>DEPTH=2 is specified: The Web page and the resources and frames embedded in the page are downloaded.</p>

Folder name#1	Property name	XML tag#2	Description
HTTP_[0-9]+	Depth	<DEPTH>	3 or a greater value is specified in DEPTH: The Web page, the resources and frames embedded in the page, and the information embedded in the acquired frames (such as the resources and frames embedded in the downloaded frames) are downloaded up to the specified depth. If nothing is embedded in an acquired frame, no more acquisition is performed. For details about embedded resources and frames, see <i>HTTP</i> in <i>10. Records</i> .
	Web Auth	<WEB_AUTH>	Select Yes or No from the list to specify whether or not Web authentication is to be performed.
	Web Username	<WEB_USERNAME>	Specifies the user name to be used for Web authentication by character string up to 64 bytes. None is set by default. If the value of the Web Auth property is Yes , this value must be specified. If the value of the Web Auth property is No , this value is not applicable.
	Proxy	<PROXY>	Select Yes or No from the list to specify whether or not a proxy is to be used.
	Proxy Hostname#5	<PROXY_HOSTNAME>	Specifies the proxy server's host name or IP address by character string up to 255 bytes. None is set by default. If the value of the Proxy property is Yes , this value must be specified. If the value of the Proxy property is No , this value is not applicable.
	Proxy Port	<PROXY_PORT>	Specifies the proxy server's port number in the range from 1 to 65,535. None is set by default. If the value of the Proxy property is Yes , this value must be specified. If the value of the Proxy property is No , this value is not applicable.
	Proxy Auth	--	Select Yes or No from the list to specify whether or not proxy authentication is to be used. If the value of the Proxy property is No , this value is not applicable.
	Proxy Username	<PROXY_USERNAME>	Specifies the user name to be used for proxy authentication by character string up to 64 bytes. None is set by default. If the value of the Proxy Auth property is Yes , this value must be specified. If the value of the Proxy Auth property is No , this value is not applicable.
HTTPS_[0-9]+#6	--	--	Stores the properties for measuring HTTPS service.
	URL	<URL>	Specifies the URL of the measuring target Web page by using a character string of 255 or fewer bytes. None is set by default. The protocol identifier (<code>https://</code>) is not included. The port number can be omitted. If the port number is omitted, port 80 is used.
	Method	<POST>#4	Displays the request method. The default value is GET. You cannot use PFM - Web Console to change this value. As a result, if you use the POST method, edit the measurement condition registration file directly or define the measurement condition as a Web transaction. PFM - Web Console cannot display a character string to be sent as the message body using the POST method.
	Depth	<DEPTH>	Specifies the depth of embedded resources and frames to be acquired by using a number in the range from 1 to 100. This is the depth of the resources and frames in the Web page that are to be downloaded. The following shows examples. DEPTH=1 is specified: Only the Web page is downloaded.

Folder name# ¹	Property name	XML tag# ²	Description
HTTPS_[0-9]+# ⁶	Depth	<DEPTH>	<p>DEPTH=2 is specified: The Web page and the resources and frames embedded in the page are downloaded.</p> <p>3 or a greater value is specified in DEPTH: The Web page, the resources and frames embedded in the page, and the information embedded in the acquired frames (such as the resources and frames embedded in the downloaded frames) are downloaded up to the specified depth. If nothing is embedded in an acquired frame, no more acquisition is performed.</p> <p>For details about embedded resources and frames, see HTTPS in <i>10. Records</i>.</p>
	Web Auth	<WEB_AUTH>	Select Yes or No from the list to specify whether or not Web authentication is to be performed.
	Web Username	<WEB_USERNAME>	<p>Specifies the user name to be used for Web authentication by using a character string of 64 or fewer bytes. None is set by default.</p> <p>This property must be specified if the value of the Web Auth property is Yes. This property is not applicable if the value of the Web Auth property is No.</p>
	Proxy	<PROXY>	Select Yes or No from the list to specify whether or not a proxy is to be used.
	Proxy Hostname	<PROXY_HOSTNAME>	<p>Specifies the proxy server's host name or IP address by using a character string of 255 or fewer bytes. None is set by default.</p> <p>This property must be specified if the value of the Proxy property is Yes. This property is not applicable if the value of the Proxy property is No.</p>
	Proxy Port	<PROXY_PORT>	<p>Specifies the proxy server's port number in the range from 1 to 65,535. None is set by default.</p> <p>This property must be specified if the value of the Proxy property is Yes. This property is not applicable if the value of the Proxy property is No.</p>
	Proxy Auth	--	<p>Select Yes or No from the list to specify whether or not proxy authentication is to be used.</p> <p>This property is not applicable if the value of the Proxy property is No.</p>
	Proxy Username	<PROXY_USERNAME>	<p>Specifies the user name to be used for proxy authentication by using a character string of 64 or fewer bytes. None is set by default.</p> <p>This property must be specified if the value of the Proxy Auth property is Yes. This property is not applicable if the value of the Proxy Auth property is No.</p>
	SSL Auth Ignore	<SSL_AUTH_IGNORE>	<p>Select Yes or No from the list to specify whether or not measurement is to continue when SSL server authentication fails.</p> <p>Select Yes to continue measurement when SSL server authentication fails.</p>
	Client Auth	<CLIENT_AUTH>	Select Yes or No from the list to specify whether or not client authentication is to be performed.
	Client Certification File	<CLIENT_CERT_FILE>	<p>Specifies the file in which the client certificate and private key are stored, by using a character string of 255 or fewer bytes. None is specified by default.</p> <p>Specify the name of a file that is stored in <i>installation-folder\agt\probe\cert</i>. Do not include the path. The file must be converted to Base64-encoded X.509 format. PFM - Web Console 08-50 or later supports Japanese (multibyte character sets) in a Japanese environment</p>

Folder name# ¹	Property name	XML tag# ²	Description
HTTPS_[0-9]+# ⁶	Client Certification File	<CLIENT_CERT_FILE>	or Chinese (multibyte character sets, except for 4-byte characters) in a Chinese environment.
SMTP_[0-9]+	--	--	Stores the properties for measuring the SMTP service.
	Hostname	<HOSTNAME>	Specifies the SMTP server's host name or IP address by character string up to 255 bytes. None is set by default.
	Port	<PORT>	Specifies the SMTP server's port number in the range from 1 to 65,535.
	Message Size	<MSG_SIZE>	Specifies the size of the text for a measurement email by character string up to 10,000 bytes. None is set by default.
	Destination Mail Address	<DST_MAIL_ADDRESS>	Specifies exactly one email address to which a measurement email is to be sent by character string up to 256 bytes. None is set by default.
	Source Mail Address	<SRC_MAIL_ADDRESS>	Specifies the email address from which a measurement email is to be sent by character string up to 256 bytes. None is set by default.
	POP3 Auth	<POP3_AUTH>	Select Yes or No from the list to specify whether or not POP3 (POP before SMTP) authentication is to be performed.
	POP3 Hostname	<POP3_HOSTNAME>	Specifies the POP3 server's host name or IP address by character string up to 255 bytes. None is set by default. If the value of the POP3 Auth property is Yes , this value must be specified. If the value of the POP3 Auth property is No , this value is not applicable.
	POP3 Port	<POP3_PORT>	Specifies the POP3 server's port number in the range from 1 to 65,535. If the value of the POP3 Auth property is Yes , this value must be specified. If the value of the POP3 Auth property is No , this value is not applicable.
POP3 Username	<POP3_USERNAME>	Specifies the user name to be used for POP3 authentication by character string up to 40 bytes. None is set by default. If the value of the POP3 Auth property is Yes , this value must be specified. If the value of the POP3 Auth property is No , this value is not applicable.	
POP3_[0-9]+	--	--	Stores the properties for measuring the POP3 service.
	Hostname	<HOSTNAME>	Specifies the POP3 server's host name or IP address by character string up to 255 bytes. None is set by default.
	Port	<PORT>	Specifies the POP3 server's port number in the range from 1 to 65,535.
	Username	<USERNAME>	Specifies the user name to be used in the POP3 service by character string up to 40 bytes. None is set by default.
	Delete Mail	<NON_DELETE_MAIL>	Select Yes or No from the list to specify whether or not read emails are to be deleted.
IMAP4_[0-9]+	--	--	Stores the properties for measuring the IMAP4 service.
	Hostname	<HOSTNAME>	Specifies the IMAP4 server's host name or IP address by character string up to 255 bytes. None is set by default.
	Port	<PORT>	Specifies the IMAP4 server's port number in the range from 1 to 65,535.
	Username	<USERNAME>	Specifies the user name to be used in the IMAP4 service by character string up to 64 bytes. None is set by default.
	Delete Mail	<DELETE_MAIL>	Select Yes or No from the list to specify whether or not read emails are to be deleted.
DNS_[0-9]+	--	--	Stores the properties for measuring the DNS service.

Folder name# ¹	Property name	XML tag# ²	Description
DNS_[0-9]+	IP Address	<IPADDRESS>	Specifies the DNS server's IP address by character string up to 15 bytes. Only the IP address is accepted; the DNS name is not accepted. None is set by default.
	Port	<PORT>	Specifies the DNS server's port number in the range from 1 to 65,535.
	Query	<QUERY>	Specifies the name of the host to be searched by character string up to 255 bytes. None is set by default.
	Retry	<RETRY>	Specifies the number of retries in the range from 1 to 5. From this value and the timeout value specified in the <TIME_OUT> tag contained in the <GEN_PARAM> tag, the retry timeout value is determined and set automatically. The formula is as follows: Retry timeout value = timeout value/(number of retries + 1)
DHCP_[0-9]+	--	--	Stores the properties for measuring the DHCP service.
	Hostname	<HOSTNAME>	Specifies the DHCP server's host name or IP address by character string up to 255 bytes. None is set by default.
	Port	<PORT>	Specifies the DHCP server's port number in the range from 1 to 65,535.
	Probe Port	<PROBE_PORT>	Specifies the port number of the probe in the range from 1 to 65,535 that is used as the DHCP client in measuring the measurement condition.
	Accept Offer	<NON_ACCEPT_OFFER> ^{#7}	Select Yes or No from the list to specify whether or not IP address assigned from the DNS server is to be accepted.
FTP_[0-9]+	--	--	Stores the properties for measuring the FTP service.
	Hostname ^{#5}	<HOSTNAME>	Specifies the FTP server's host name or IP address by character string up to 255 bytes. None is set by default.
	Port	<PORT>	Specifies the FTP server's port number in the range from 1 to 65,535.
	Username	<USERNAME>	Specifies the user name to be used in the FTP service by character string up to 64 bytes. None is set by default.
	Direction	<TRANS_DIRECTION>	Specifies the file transfer method. To transfer a file to the server, specify UPLOAD ; to transfer a file from the server, specify DOWNLOAD . A transfer file for measurement must already be stored in the following folder: For UPLOAD : <i>installation-folder\agtv\probe\probedata\ftp</i> For DOWNLOAD : Specified account's home directory
	File	<FILE_NAME>	Specifies the name of the file to be transferred by character string up to 32 bytes. PFM - Web Console 08-50 or later supports Japanese (multibyte character sets) in a Japanese environment or Chinese (multibyte character sets, except for 4-byte characters) in a Chinese environment. None is set by default.
Connection Mode	<PASSIVE> ^{#8}	Select ACTIVE or PASSIVE from the list to specify the connection mode. The connection establishment method depends on the connection mode, as described below: In the ACTIVE mode: The connection request for file transfer is issued from the FTP server. In the PASSIVE mode: The connection request for file transfer is issued from the FTP probe.	
TCP_[0-9]+	--	--	Stores the properties for measuring the TCP service.

Folder name#1	Property name	XML tag#2	Description
TCP_[0-9]+	Hostname#5	<HOSTNAME>	Specifies the TCP server's host name or IP address by character string up to 255 bytes. None is set by default.
	Port	<PORT>	Specifies the TCP server's port number in the range from 1 to 65,535. None is set by default.
WEBTRANS_[0-9]+	--	--	Stores the properties for measuring the Web transaction.
	Filename	<TRANSACTION_FILE>	Specifies the name of the Web transaction file. None is set by default. Specify a file with the extension .xml that is stored in <i>installation-folder\agtv\probe\webtrans</i> . <ul style="list-style-type: none"> Do not include the path. The specified name is not case sensitive. PFM - Web Console 08-50 or later supports Japanese (multibyte character sets) in a Japanese environment or Chinese (multibyte character sets, except for 4-byte characters) in a Chinese environment.
	Transaction	<TRANSACTION_NAME>	Specifies the name of the Web transaction by character string up to 255 bytes. None is set by default. The vertical bar character () cannot be used. PFM - Web Console 08-50 or later supports Japanese (multibyte character sets) in a Japanese environment or Chinese (multibyte character sets, except for 4-byte characters) in a Chinese environment.
USERSERV_[0-9] +	--	--	Stores the properties for measuring the user-defined service.
	User Service ID	<USER_SERVICE_ID>	Specifies a user-defined service ID in the range from 1 to 100 that has been registered in the command registration file. None is set by default.
IESCENA_[0-9] +	--	--	Stores the properties for measuring the IE scenario.
	Filename	<IESCENA_FILE>	Specifies the name of the IE scenario file. Specify a file with the extension .xml that is stored in <i>installation-folder\agtv\probe\iescena</i> . <ul style="list-style-type: none"> Do not include the path. The specified name is not case sensitive. PFM - Web Console 08-50 or later supports Japanese (multibyte character sets) in a Japanese environment or Chinese (multibyte character sets, except for 4-byte characters) in a Chinese environment.

Legend:

--: Not applicable

#1

The listed folders are the folders under the \Agent Configuration\Probe\Task List folder.

The string after the folder name, "[0-9] +", means a numeric character occurring one or more times. This number is the same as the one you specified as a task ID when creating a task.

The following is an example of the properties for Web transaction measurement when its Task ID is 100:

Name	Value	Description
Task ID	100	ID of this task is displayed.
Status	Applied	Status of this task is displayed.
Task Label		Specifies user friendly name for this task. Must be shorter than 64 bytes width. (optional item)
Interval	80	Specifies the measurement interval. Values from 60 to 86400 can be specified.
Timeout	30	Specifies the maximum amount of time within which a single measurement must be completed by second. Values from 1 to 3600 can be specified.
Filename	sample01.xml	Specifies the name of Web transaction file.
Transaction	sample01	Specifies the name of Web transaction.

#2 The listed tags are used to define the properties in the measurement condition registration file.

#3 To use an IP address to specify a host name, use an IPv4 dotted-decimal address (for example: `http://172.16.233.12/example.html`) or an IPv6 hexadecimal address enclosed in square brackets, using colons as separators (for example: `http://[ACE6:45:75:91::1]/example.html`).

#4 If the `POST` method is used, the setting is defined in the `<POST>` tag. If the `GET` method is used, the tags are omitted.

#5 To specify an IPv4 address for the host name, use dotted-decimal format (for example: `172.16.233.12`). To specify an IPv6 address, use hexadecimal format, using colons as separators (for example: `ACE6:45:75:91::1`).

#6 For the `URL` and `Proxy Hostname` properties of the `HTTPS_[0-9]+` folder, you cannot specify an IPv6 address for the host name.

#7 If `No` is specified, the setting is defined in the `<NON_ACCEPT_OFFER>` tag. If `Yes` is specified, the tags are omitted.

#8 If the `Passive` method is used, the setting is defined in the `<PASSIVE>` tag. If the `Active` method is used, the tags are omitted.

F. List of Files and Folders

This appendix lists the files and folders of PFM - Agent for Service Response.

You may specify any folder as the installation folder of Performance Management. The following is the default installation folder:

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

The following table lists the files and folders for PFM - Agent for Service Response.

Table F–1: Files and folders for PFM - Agent for Service Response

Folder name	File name	Description
<i>installation-folder</i> \agtv\	--	Base folder of PFM - Agent for Service Response
	Readme_ja.txt	README file (Japanese)
	Readme_en.txt	README file (English)
	VERSION.TXT	Version information
	.	Various files of PFM - Agent for Service Response
<i>installation-folder</i> \agtv\agent\	--	Base folder of the Agent Collector service
	COSLMMI.DB	Data file for the JP1/SLM linkage setting
	COSLMMI.IDX	Index file for the data file for the JP1/SLM linkage setting
	COSLMMI.LCK	Lock file for the data file for the JP1/SLM linkage setting
	jpcagt.ini	Agent Collector service settings file
	jpcagt.ini.model	Model file for the Agent Collector service settings file
	jpcagtv.exe	Executable program of the Agent Collector service
<i>installation-folder</i> \agtv\agent\log\	--	Storage folder for internal log files of the Agent Collector service
<i>installation-folder</i> \agtv\lib\	--	Storage folder for message catalogs
	jpcagtvmsg.dll	Message catalog file for PFM - Agent for Service Response
<i>installation-folder</i> \agtv\probe\	--	Base folder of the Probe Daemon and the IE Probe Daemon services
<i>installation-folder</i> \agtv\probe\bin\	--	Binary command storage folder for Probe Daemon
	esplastresult.exe	Display program of the measurement result
	esprobed.exe	Executable program of the Probe Daemon service
	esprobed_tm.exe	Executable program of the Probe Daemon service (jpcvtest command)
	espasswd.exe	Password registration, change, and deletion commands
	espstatus.exe	Display program of the status of the Probe Daemon
	espsvc.exe	Executable program of the Probe Daemon service

Folder name	File name	Description
<i>installation-folder</i> \agtv\probe\bin\	espwebrec.exe	Web Recorder
	jpcviemd.exe	IE Probe master daemon
	jpcvieprobed.exe	Executable program of the IE Probe Daemon
	jpcvierec.exe	IE Recorder
	jpcviesvc.exe	Executable program of the IE Probe Daemon service
	jpcviebrwsctrl.dll	IE common browser control library
	jpcviectrl.dll	IE common user control library
	jpcvieopctrl.dll	IE common operation data control library
	jpcvieparts.dll	IE common management parts library
	jpcviexml.dll	IE common XML processing parts library
	jpcvtaskctl.exe	Command to pause or resume monitored tasks
	jpcvumcommon.dll	IE common log control library
	jpcvumiecom.dll	IE common COM processing library
	jpcvumiehook.dll	IE common dialog control library
	jpcvumiemsg.dll	IE common unmanagement parts library
	jpcvumprbpipe.dll	Common control pipes of Collector and IE probes library
	libtaskctl.dll	Monitored task control library
<i>installation-folder</i> \agtv\probe\cert\	--	Storage folder for certificates
<i>installation-folder</i> \agtv\probe\conf\	--	Storage folder for definition files
	esp.conf	Probe action condition definition file
	espras.conf	Maintenance information condition definition file
	esptasklabel.conf	Measurement condition label definition file
	jpcvierec.conf	IE Recorder action condition definition file
	wr.conf	Web Recorder action condition definition file
<i>installation-folder</i> \agtv\probe\log\	--	Storage folder for log files
<i>installation-folder</i> \agtv\probe\passwd\	--	Storage folder for password files
<i>installation-folder</i> \agtv\probe\probedata\	--	Work folder for Probe Daemon
<i>installation-folder</i> \agtv\probe\probedata\ftp\	--	Temporary file storage folder for FTP measurement
<i>installation-folder</i> \agtv\probe\probedata\http\	--	Temporary file storage folder for HTTP(S) measurement
<i>installation-folder</i> \agtv\probe\probedata\webtrans\	--	HTML file output folder during Web transaction measurement
<i>installation-folder</i> \agtv\probe\probedata\webtrans_cmd\	--	HTML file output folder during jpcvtest command execution

Folder name	File name	Description
<i>installation-folder</i> \agtv\probe\probedata\iescena\	--	HTML file output folder while measuring IE scenarios
<i>installation-folder</i> \agtv\probe\probedata\iescena\ieprobed_ <i>measurement-condition-ID</i> \	--	HTML file output folders for each measurement condition ID while measuring IE scenario
<i>installation-folder</i> \agtv\probe\report\	--	Storage folder for Probe Daemon's reports
<i>installation-folder</i> \agtv\probe\task\	--	Storage folder for Probe Daemon's measurement condition registration files
<i>installation-folder</i> \agtv\probe\task\esp\	--	Storage folder for Probe Daemon's measurement conditions
<i>installation-folder</i> \agtv\probe\tmp\	--	Temporary file storage folder for Probe Daemon
<i>installation-folder</i> \agtv\probe\user\	--	Storage folder for Probe Daemon's user-defined commands
<i>installation-folder</i> \agtv\probe\usertools\	--	Storage folder for Probe Daemon's sample files
<i>installation-folder</i> \agtv\probe\webtrans\	--	Storage folder for Probe Daemon's Web transaction files
<i>installation-folder</i> \agtv\probe\iescena\	--	Storage folder for IE scenario files of IE Probe Daemon
<i>installation-folder</i> \agtv\store\	--	Base folder of the Agent Store service
	*.DB	Performance data files
	*.IDX	Index files for performance data files
	*.LCK	Lock files for performance data files
	jpcsto.ini	Agent Store service settings file
	jpcsto.ini.model	Model file for the Agent Store service settings file
	*.DAT	Definition file for the data model
<i>installation-folder</i> \agtv\store\backup\	--	Default database backup folder
<i>installation-folder</i> \agtv\store\dump\	--	Default database export folder
<i>installation-folder</i> \agtv\store\import\	--	Default database import destination folder
<i>installation-folder</i> \agtv\store\log\	--	Storage folder for internal log files of the Agent Store service
<i>installation-folder</i> \agtv\store\STPD\	--	PD database specific folder
<i>installation-folder</i> \agtv\store\STPI\	--	PI database specific folder
<i>installation-folder</i> \agtv\store\STPL\	--	PL database specific folder
<i>installation-folder</i> \auditlog\	--	Default output folder for action log files
	jpcauditn.log#	Action log file
<i>installation-folder</i> \setup\	--	Storage folder for setup files
	jpcagtvu.Z	Archive file for PFM - Agent setup (UNIX)
	jpcagtvw.EXE	Archive file for PFM - Agent setup (Windows)
<i>installation-folder</i> \setup\alarm	--	Storage folder for alarm table recovery

Folder name	File name	Description
<i>installation-folder</i> \setup\extract	--	Setup file extraction folder
<i>system-drive</i> \Program Files\Hitachi\	--	HNTRLib2 public DLL folder
	.	HNTRLib2 public DLL
<i>system-drive</i> \Program Files\Hitachi\HNTRLib2\	--	Storage folder for HNTRLib2 executable files and include files
	.	HNTRLib executable files and include files
<i>system-drive</i> \Program Files\Hitachi\HNTRLib2\spool	--	Integrated trace log directory

Legend:

--: Not applicable

#

n is a numeric value. The number of log files can be changed in the `jpccomm.ini` file.

G. Migration Procedure and Notes on Migration

To upgrade PFM - Agent for Service Response to a newer version, install the newer version by overwriting the older version. For details about installation operations, see [3. Installation and Setup](#).

For details about notes on upgrading the versions of Performance Management programs, see the section describing the notes on version upgrading in the chapter and appendix that explain installation and setup in the *JPI/Performance Management Planning and Configuration Guide*.

Observe the following precautions when upgrading the version of PFM - Agent for Service Response:

- When upgrading the PFM - Agent for Service Response version, do not uninstall the older version. If you uninstall it, performance data and other data created with the older version are also deleted, and as a result, the newer version will not work.
- When a newer version of PFM - Agent for Service Response is installed by overwriting an older version, the following items are automatically updated:
 - Store database file of the Agent Store service
 - `ini` file
- When upgrading PFM - Agent for Service Response that is running in a cluster system, you must copy the measurement condition registration file to the shared disk. For details, see [6.3.4 Setup](#).

H. Version Compatibility

In PFM - Agent, there are product versions as well as data model versions.

Because data models maintain upward compatibility, report definitions and alarm definitions created in the older version can also be used in the newer version of the data model.

The table below shows version compatibility of PFM - Agent for Service Response.

Table H–1: PFM - Agent for Service Response version compatibility

PFM - Agent for Service Response version	Data model version	Alarm table version of the monitoring template
08-00	4.0	8.00
09-00	5.0	09.00
10-00	5.0	09.00
10-50	5.0	09.00
11-00	5.0	09.00
11-10	5.0	09.00

In PFM - Agent for Service Response, an alarm table of a version that is not available in the Performance Management system being used may sometimes be displayed under **Alarms** in the PFM - Web Console window. Therefore, check the alarm table version being used by the Performance Management system and its compatibility before using an alarm table.

For details about version compatibility, see the version compatibility description in the appendix to the *JPI/Performance Management Planning and Configuration Guide*.

I. Outputting Action Log Data

Action log data of Performance Management is history information that is output in cooperation with the alarm function related to exceeded thresholds, such as for a system load.

For example, when a PFM service starts or stops or when the state of connection with PFM - Manager changes, log data is output to the action log.

Action log data can be output when the version of PFM - Manager or PFM - Base is 08-11 or later.

An action log is a CSV text file. By saving action logs periodically and converting them with spreadsheet software, you can use the action logs as analysis data.

Output of action log data is specified in the `jpccomm.ini` file. This appendix describes the contents of the action log data output by PFM - Agent and PFM - Base, and how to specify the setting for outputting the action log data.

I.1 Types of events output to the action log

The following table describes the types of events output to the action log and the times at which PFM - Agent and PFM - Base output data to the action log. The event types are the identifiers used within the action log to classify the events output to the action log.

Table I-1: Types of events output to the action log

Event type	Explanation	PFM - Agent and PFM - Base output the action log when:
StartStop	Events indicating that software is started or terminated.	<ul style="list-style-type: none">• A PFM service is started or stopped.• Stand-alone mode is started or terminated.
ExternalService	Events indicating the result of communication between a JP1 product and an external service. This event type also indicates that an abnormal communication has occurred.	The status of a connection with PFM - Manager has changed.
ManagementAction	Events indicating that an important action of the program has been executed. This event type also indicates that the action was executed in response to another audit category.	An automated action is executed.

I.2 Format for saving the action log files

This section explains the format for saving the action log files.

Action log data is output to a specified file (the current output file). When the current output file becomes full, the action log data in that file is saved to another file (the shift file). The procedure for switching the file for storing action log data is as follows:

1. Action log data is output sequentially to the current output file `jpcaudit.log`.
2. When the current output file becomes full, the action log data is saved in a shift file.

The name of a shift file is the current output file name suffixed with a number. Each time the current output file becomes full, each shift file is renamed by incrementing the suffix by 1. Therefore, the file whose name has the largest number is the oldest log file.

Example:

When the current output file `jpcaudit.log` becomes full, the contents of the file are saved to the shift file `jpcaudit1.log`.

When the current output file becomes full again, the information is moved to `jpcaudit1.log`, and the existing shift file `jpcaudit1.log` is renamed to `jpcaudit2.log`.

Note that when the number of log files exceeds the number of saved log files (specified in the `jpccomm.ini` file), the oldest log file is deleted.

3. The current output file is initialized, and new action log data is written.

Whether action log data is to be output, the output destination, and the number of output files are specified in the `jpccomm.ini` file. For details about how to specify the `jpccomm.ini` file, see [I.4 Settings for outputting action log data](#).

I.3 Format of output action log data

Data related to audit events is output to the Performance Management action log. Action log data is output to one file for one host. The action log data is output to a file on either of the following hosts:

- When a service is executed: The data is output to the file on the host on which the service runs.
- When a command is executed: The data is output to the file on the host on which the command was executed.

The following describes the format of the action log, the output destination, and the items that are output.

(1) Output format

```
CALFHM x.x, output-item-1=value-1, output-item-2=value-2, ..., output-item-n=value-n
```

(2) Output destination

```
installation-folder\auditlog\
```

The output destination for action log data can be changed in the `jpccomm.ini` file. For details about how to specify the `jpccomm.ini` file, see [I.4 Settings for outputting action log data](#).

(3) Output items

There are two types of output items:

- Common output items
Items that are always output by all JP1 products that output action log data
- Fixed output items
Items that are optionally output by a JP1 product that outputs action log data

(a) Common output items

The following table lists and describes the common output items and their values. This table also includes the items and information output by PFM - Manager.

Table I–2: Common output items in action logs

No.	Output item		Value	Explanation
	Item name	Output attribute name		
1	Common specification identifier	--	CALFHM	Indicates the action log format
2	Common specification revision number	--	x.x	Revision number for managing action logs
3	Serial number	seqnum	<i>serial-number</i>	Serial number of the action log record
4	Message ID	msgid	KAVExxxx-x	Message ID of the product
5	Date and time	date	YYYY-MM-DDThh:mm:ss.sssTZD#	Date, time, and time zone indication identifying when the action log was output
6	Program name	progid	JP1PFM	Name of the program for which the event occurred
7	Component name	compid	<i>service-ID</i>	Name of the component for which the event occurred
8	Process ID	pid	<i>process-ID</i>	Process ID of the process for which the event occurred
9	Location	ocp:host	<ul style="list-style-type: none"> <i>host-name</i> <i>IP-address</i> 	Location where the event occurred
10	Event type	ctgry	<ul style="list-style-type: none"> StartStop Authentication ConfigurationAccess ExternalService AnomalyEvent ManagementAction 	Category name used to classify the event output to the action log
11	Event result	result	<ul style="list-style-type: none"> Success Failure Occurrence 	Result of the event
12	Subject identification information	subj:pid	<i>process-ID</i>	One of the following: <ul style="list-style-type: none"> Process ID of a process running as a user operation Process ID of the process that caused the event
		subj:uid	<i>account-identifier</i> (PFM user/JP1 user)	
		subj:euid	<i>effective-user-ID</i> (OS user)	

No.	Output item		Value	Explanation
	Item name	Output attribute name		
12	Subject identification information	subj:euid	<i>effective-user-ID</i> (OS user)	<ul style="list-style-type: none"> Name of the user who caused the event Identification information in a one-to-one correspondence with the user

Legend:

--: None

#

T is a separator between the date and the time.

TZD is the time zone specify. One of the following values is output.

+hh:mm: The time zone is hh:mm ahead of UTC.

-hh:mm: The time zone is hh:mm behind UTC.

Z: The time zone is the same as UTC.

(b) Fixed output items

The following table lists and describes the fixed output items and their values. This table also includes the items and information output by PFM - Manager.

Table I-3: Fixed output items in action logs

No.	Output item		Value	Explanation
	Item name	Output attribute name		
1	Object information	obj	<ul style="list-style-type: none"> <i>PFM - Agent-service-ID</i> <i>added-deleted-or-updated-user-name</i> (PFM user) 	Intended object for the operation
		obj:table	<i>alarm-table-name</i>	
		obj:alarm	<i>alarm-name</i>	
2	Action information	op	<ul style="list-style-type: none"> Start Stop Add Update Delete Change Password Activate Inactivate Bind Unbind 	Information about the action that caused the event
3	Permissions information	auth	<ul style="list-style-type: none"> Administrator Management General user Ordinary Windows 	Permissions information of the user who executed the command or service

No.	Output item		Value	Explanation
	Item name	Output attribute name		
3	Permissions information	auth	Administrator • UNIX SuperUser	Permissions information of the user who executed the command or service
		auth:mode	• PFM authentication mode pfm • JP1 authentication mode jpl • OS user os	Authentication mode of the user who executed the command or service
4	Output source	outp:host	<i>PFM - Manager-host-name</i>	Host that output the action log
5	Instruction source	subjp:host	• <i>login-host-name</i> • <i>execution-host-name</i> (only when the <code>jpctool alarm</code> command is executed)	Host that issued the instruction for the operation
6	Descriptive text	msg	<i>message</i>	Message that is output when an alarm occurs or when an automated action is executed

Whether the fixed output items are output and what they contain differ depending on when the action log data is output. The following describes the message ID and output data for each case.

■ A PFM service starts or stops (StartStop)

- Output host: The host on which the service is running
- Output component: The service that started or stopped

Item name	Attribute name	Value
Message ID	msgid	Started: KAVE03000-I Stopped: KAVE03001-I
Action information	op	Started: Start Stopped: Stop

■ Stand-alone mode starts or stops (StartStop)

- Output host: PFM - Agent host
- Output component: Agent Collector service and Agent Store service

Item name	Attribute name	Value
Message ID	msgid	Stand-alone mode has started: KAVE03002-I Stand-alone mode has terminated: KAVE03003-I

Notes:

1. No fixed output items are output.

2. When PFM - Agent is started, PFM - Agent services connect to the PFM - Manager host, register node information, and obtain the latest alarm definition information. If a connection with the PFM - Manager host cannot be established, PFM - Agent starts in stand-alone mode, in which only part of its functionality, such as collection of operating information, is enabled. In addition, KAVE03002-I is output to indicate that PFM - Agent has started in stand-alone mode. From this point, the PFM - Agent services periodically attempt to connect to PFM - Manager. When the services are able to successfully register node information or obtain definition information, PFM - Agent leaves stand-alone mode and KAVE03003-I is output. In this way, the action log enables you to understand that PFM - Agent was running in an imperfect condition for the period from the output of KAVE03002-I to the output of KAVE03003-I.

■ The status of the connection with PFM - Manager changes (ExternalService)

- Output host: PFM - Agent host
- Output component: Agent Collector service and Agent Store service

Item name	Attribute name	Value
Message ID	msgid	Sending of an event to PFM - Manager failed (queuing was started): KAVE03300-I. An event was resent to PFM - Manager: KAVE03301-I.

Notes:

1. No fixed output items are output.
2. If the Agent Store service is unable to send an event to PFM - Manager, the Agent Store service starts queuing events, up to a maximum of three. When queuing is started after a failure to send an event, KAVE03300-I is output. When the connection with PFM - Manager is restored and all queued events have been sent, KAVE03301-I is output. In this way, the action log enables you to understand that real-time sending of events to PFM - Manager was disabled for the period from the output of KAVE03000-I to the output of KAVE03001-I.
3. The Agent Collector service usually sends events to PFM - Manager via the Agent Store service. It directly sends events to PFM - Manager only when the Agent Store service has stopped for some reason. If sending of events fails, KAVE03300-I is output, but KAVE03301-I is not output, since no events are queued. In this way, the action log enables you to understand that some events have not been sent to PFM - Manager.

■ An automated action is executed (ManagementAction)

- Output host: The host on which the action was executed
- Output component: Action Handler service

Item name	Attribute name	Value
Message ID	msgid	The command execution process was created successfully: KAVE03500-I. An attempt to create a command execution process failed: KAVE03501-W. Email was send successfully: KAVE03502-I. Sending of email failed: KAVE03503-W
Free description	msg	Command execution: cmd= <i>executed-command-line</i> . Email sending: mailto= <i>destination-email-address</i> .

Notes:

KAVE03500-I is output when the command execution process is created successfully. Thereafter, log data about whether the command was executed and about the execution results is not output to the action log.

(4) Output example

The following is an example of output action log data.

```
CALFHM 1.0, seqnum=1, msgid=KAVE03000-I, date=2007-01-18T22:46:49.682+09:00,  
progid=JP1PFM, compid=TA1host01, pid=2076,  
ocp:host=host01, ctgry=StartStop, result=Occurrence,  
subj:pid=2076,op=Start
```

I.4 Settings for outputting action log data

The settings for outputting action log data are defined in the `jpccomm.ini` file. If no settings are specified, no action log data is output. The following describes the settings required to output action log data, and how to specify the settings.

(1) Setting procedure

To specify the settings for outputting action log data:

1. Stop all PFM services on the host.
2. Using a text editor, edit the `jpccomm.ini` file.
3. Save and close the `jpccomm.ini` file.

(2) Details about the `jpccomm.ini` file

The following describes the `jpccomm.ini` file in detail.

(a) Storage folder

installation-folder

(b) Format

In the `jpccomm.ini` file, define the following information:

- Whether to output action log data
- Output destination of the action log
- Number of action logs that can be saved
- File size of the action log

The specification format is as follows:

"item-name"=value

The following table describes the items that you can specify.

Table I-4: Items specified in the `jpccomm.ini` file and their initial values

No.	Item	Explanation
1	[Action Log Section]	The section name, which cannot be changed.

No.	Item	Explanation
2	Action Log Mode	<p>Specify whether to output action log data. You must specify this item.</p> <ul style="list-style-type: none"> Initial value: 0 (Data not output) Specifiable value: 0 (Data not output) or 1 (Data output) <p>If any other value is specified, an error message is output and action log data will not be output.</p>
3	Action Log Dir	<p>Specify the action log output destination.</p> <p>If a path longer than the limit is specified or if access to the directory fails, an error message is output to the command log and action log data will not be output.</p> <ul style="list-style-type: none"> Initial value: None set Default value used when no specification is made <i>installation-folder\auditlog\</i> Specifiable value: A character string from 1 to 185 bytes
4	Action Log Num	<p>Specify the upper limit on the total number of log files (number of saved files). Specify the sum of the number of current output files and shift files.</p> <ul style="list-style-type: none"> Initial value: None set Default value used when no specification is made 5 Specifiable value: An integer in the range from 2 to 10 <p>If a character string containing a non-numeric value is specified, an error message is output and the default value 5 is set.</p> <p>If a numeric value outside the valid range is specified, an error message is output and the integer nearest the specified value in the range from 2 to 10 is set.</p>
5	Action Log Size	<p>Specify the log file size in kilobytes.</p> <ul style="list-style-type: none"> Initial value: None set Default value used when no specification is made 2048 Specifiable value: An integer in the range from 512 to 2096128 <p>If a character string containing a non-numeric value is specified, an error message is output and the default value 2048 is set.</p> <p>If a numeric value outside the valid range is specified, an error message is output and the integer nearest the specified value in the range from 512 to 2096128 is set.</p>

J. Linkage with JP1/SLM

By linking with JP1/SLM, PFM - Agent for Service Response can improve monitoring.

PFM - Agent for Service Response supplies the default monitoring items for JP1/SLM to PFM - Manager to enable monitoring with JP1/SLM.

For multi-instance records, records that match the value specified by keys are collected. For details about the keys to be collected, check the results of collection of records.

Table J–1: Default monitoring items supplied to PFM - Manager from PFM - Agent for Service Response

No.	Display name in JP1/SLM	Description	Record	Key (PFM - Manager name)	Field name
1	Total response time (HTTP)	Total response time (seconds)	<i>HTTP (PI_HTTP)</i>	MeasurementCondition ID (MSR_COND_ID)	Total Response Time (TOTAL_RESP_TIME)
2	Total response time (HTTPS)	Total response time (seconds)	<i>HTTPS (PI_HTTPS)</i>	MeasurementCondition ID (MSR_COND_ID)	Total Response Time (TOTAL_RESP_TIME)
3	Total replay time (entire IE scenario)	Total replay time (entire IE scenario) (seconds)	<i>IE Scenario Overview (PI_IESO)</i>	MeasurementCondition ID (MSR_COND_ID)	Total Replay Time (TOTAL_RPLY_TIME)
4	Total response time (TCP)	Total response time (seconds)	<i>TCP (PI_TCP)</i>	MeasurementCondition ID (MSR_COND_ID)	Total Response Time (TOTAL_RESP_TIME)
5	Total response time (entire transaction)	Total response time (seconds)	<i>Web Transaction Overview (PI_WTO)</i>	MeasurementCondition ID (MSR_COND_ID)	Total Response Time (TOTAL_RESP_TIME)

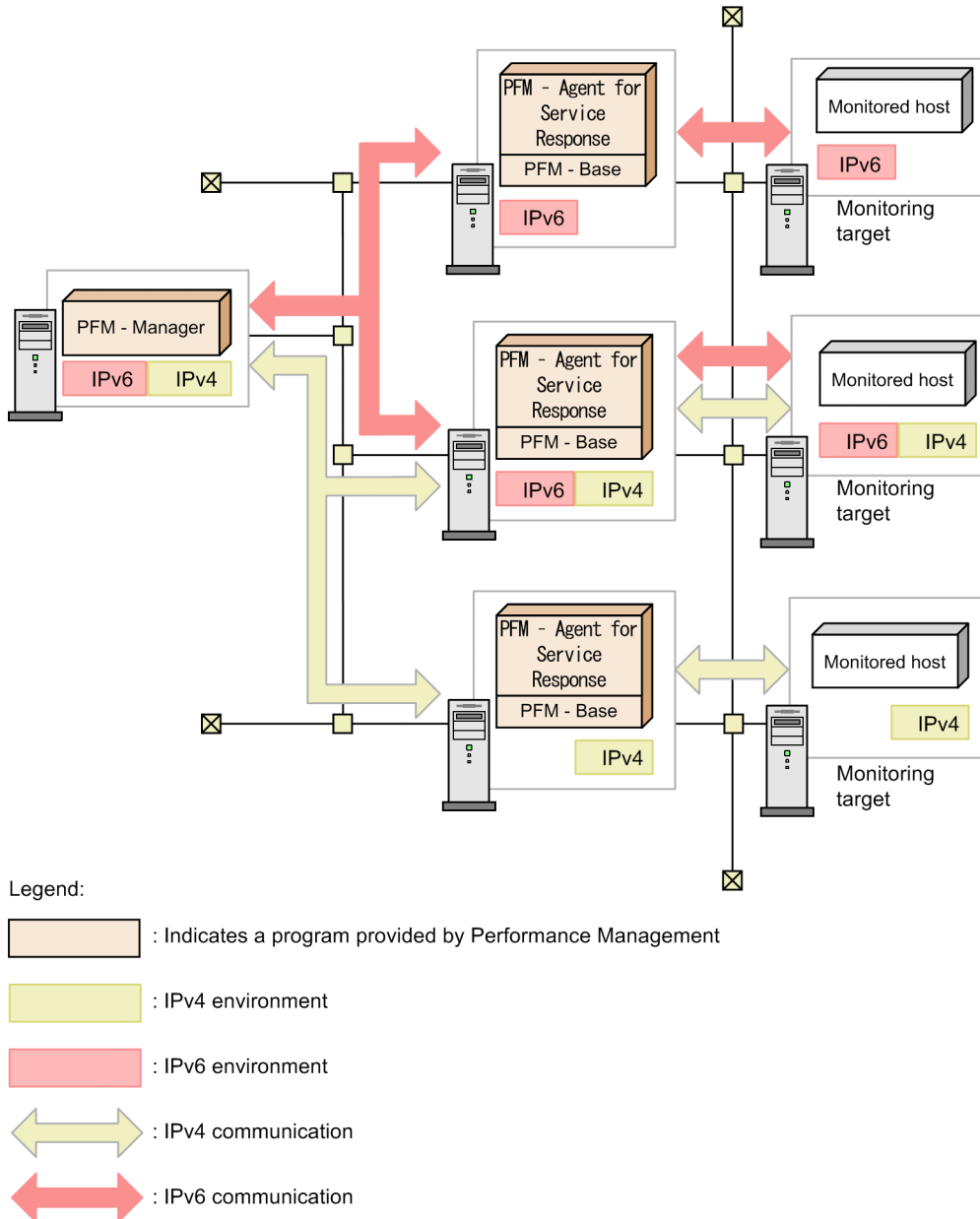
To make the default monitoring items available for PFM - Manager, you need to copy the setup files and execute the setup command. For details, see [3.1.4\(2\) Registering PFM - Agent for Service Response](#).

K. About Communication in IPv4 Environments and IPv6 Environments

Because Performance Management supports network configurations for IPv4 environments and IPv6 environments, you can use Performance Management in a network configuration that contains both IPv4 and IPv6 environments.

Note, however, that this applies only when Windows or Linux runs on a host with PFM - Manager installed.

Figure K–1: Scope of communication when an IPv4 environment and an IPv6 environment are used



To enable communication in an IPv6 environment, you must execute the `jpcconf ipv6 enable` command. For details about the `jpcconf ipv6 enable` command, see the chapter that describes commands in the manual *JPI/Performance Management Reference*. For the conditions and timing for executing the `jpcconf ipv6 enable` command, see the chapter that describes network configuring examples in an IPv6 environment in the *JPI/Performance Management Planning and Configuration Guide*.

L. Version Changes

This appendix shows the changes that have been made to each version of the manual.

L.1 Changes in 11-10

- The subsection that provides an overview of pausing or resuming a measurement was added.
- Windows Server 2016 is now supported as an OS for PFM - Agent Option for Service Response.
- The `jpcvtaskctl` command was added.
- The following messages have been added:
KAVK08026-W, KAVK43000-E, KAVK43001-E, KAVK43002-E, KAVK43003-E, KAVK43004-I, KAVK43005-E, KAVK43006-E, KAVK43007-E, KAVK43008-E, KAVK43009-W, KAVK43010-E, KAVK43011-E, KAVK43015-E, KAVK43016-E, KAVK43017-E, KAVK43018-I, KAVK43019-W, KAVK43020-W, KAVK43021-E, KAVK43023-E, KAVK43024-E, KAVK43025-E, KAVK43026-E
- The explanation of the following message was changed:
KAVK08171-E
- The actions the operator should take for the following messages were changed:
KAVK08172-E, KAVK08302-E, KAVK10040-E
- The section that describes how to troubleshoot some problems was added.

L.2 Changes in 11-00

- Internet Explorer 7 is no longer included in the prerequisite programs.
- TLSv1.2 has been supported as SSL protocols.
- The encryption types that are supported by the HTTPS probe have been changed.
- Hash algorithms that can be used for certificates have been changed.
- The following OSs are no longer included in the applicable OSs:
 - Windows Server 2003
 - Windows Server 2003 R2
 - Windows Server 2008
- The following messages have been added:
KAVK08205-I, KAVK08345-E, KAVK08346-E
- The option to disable protocols for TLSv1.2 and later versions is now supported.
- The following languages can now be used with Performance Management:
 - Korean
 - Spanish
 - German
 - French
 - Russian

- Monitoring Console `Https` is now included as one of the Agent Collector service properties.
- The product name was changed from PFM - Agent for OpenTP1 to PFM - Agent for Transaction System.
- The product name was changed from JP1/ITSLM to JP1/SLM.

L.3 Changes in 10-50

- `Over 10 Sec Collection Time` was added as a property related to the conditions for collecting performance data for each record.
- Descriptions such as usage were added because the `jpcvtest` command can now be used for Web transaction measurement tests.
- The following messages have been added:
KAVK08332-E to KAVK08341-E, KAVK08344-E, KAVK42000-E, KAVK42002-E to KAVK42007-E
- "Realtime Report Data Collection Mode" is added as a property to give priority to the indication of real-time reports over the collection of historical data.

L.4 Changes in 10-00

- Windows Server 2012 is now supported as an OS for PFM - Agent Option for Service Response.
- IPv6 is now supported.
- Windows Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11 are now supported.
- `ie_probe_browser_mode` was added to the definition in the IE Probe section of the Probe action condition definition file.
- `ie_rec_browser_mode` was added to the definition in the IE Recorder section of the IE Recorder action condition definition file.
- Linkage with JP1/ITSLM is now supported.
- The following reports have been added:
 - HTTPS Rate
 - HTTPS Response Time Status
 - HTTPS Response Time Status (real-time report)
 - HTTPS Response Time Summary
 - HTTPS Response Time Trend
 - HTTPS Top 10
- The following records have been added:
 - HTTPS (`PI_HTTPS`)
- GB18030 is added as character set for the Web transaction measurement.
- The following messages have been added:
KAVF16034-W, KAVF16035-W, KAVK08023-E, KAVK08025-E, KAVK08245-E, KAVK08322-E, KAVK08324-E, KAVK10107-E, KAVK37876-E, KAVK37877-E, KAVK38817-E, KAVK41000-E to KAVK41008-I
- The following messages have been deleted:

L.5 Changes in 09-00

- The name *solution set* has changed to *monitoring template*.
- The alarm table version for the monitoring template has been added.
- The version compatibility of data model has been added.
- With the addition of new-format commands compatible with 08-11 or earlier commands, the commands for 09-00 or later is now indicated as follows:
command-for-09-00-or-later (command-for-08-11-or-earlier)
- The following OS have been added as the OSs on which PFM - Agent for Service Response operates and as OSs for programs that can be monitored:
 - Windows Server 2003 (x64)
 - Windows Server 2008
 - Windows Server 2008 (x64)
- A function to measure IE scenarios by the IE Probe Daemon has been added.
- A function to start the IE Probe Daemon service using the Windows services has been added.
- A function to collect records of the PL record type has been added.
- A function to measure the IE scenario in a cluster system has been added.
- The notes about the measurement condition registration file when upgrading PFM - Agent for Service Response in a cluster system have been added.
- A function to collect the information of all logical hosts by executing the `jpcras` command without specifying the logical hosts (using `lhost` option) has been added.
- The following alarms have been added:
 - IES Failure
 - IES Replay Time
- The following reports have been added:
 - FTP Rate
 - FTP Top 10
 - HTTP Rate
 - HTTP Top 10
 - IE Scenario Detail
 - IE Scenario Logged Message
 - IE Scenario Replay Time Status
 - IE Scenario Replay Time Status(real-time report)
 - IE Scenario Replay Time Summary
 - IE Scenario Replay Time Trend
 - IE Scenario Scope Detail
 - IE Scenario Scope Rate

- IE Scenario Top 10
- IMAP4 Rate
- IMAP4 Top 10
- POP3 Rate
- POP3 Top 10
- SMTP Rate
- SMTP Top 10
- The following records have been added:
 - IE Scenario (PI_IIES)
 - IE Scenario Overview (PI_IIESO)
 - Logged Message for IE Scenario (PL_IIESM)
- The measurement condition can be registered in PFM - Web Console window.
- Sites with the dynamic session management can be measured by measuring Web transactions.
- The character set can be set when measuring Web transactions.
- If the characters used as delimiters of URLs are included in the substitution string, these characters can be encoded.
- An example of using PFM - Agent for Service Response to monitor performance has been added.
- The notes about the status management facility have been added.
- The notes about upgrading an older version to a newer version have been added.
- A function that outputs action logs has been added.
- PFM - Agent for Service Response can be registered automatically in PFM - Manager and PFM - Web Console, when it is setting up.
- The store version has changed from 1.0 to 2.0.
- The performance data, when it is not stored, can be interpolated.
- The *measurement-condition-label* can be specified in the measurement condition registration file (`esptask.xml`).
- An explanation of NETWORK_ERROR result code of the common fields has been added.
- HTTP service version using the following records has been added:
 - HTTP (PI_HTP)
 - Web Transaction (PI_WT)
- The following messages have been added:

KAVF16020-W to KAVF16033-W, KAVK08317-W to KAVK08320-E, KAVK08500-E to KAVK08514-E, KAVK10000-I to KAVK11042-E, KAVF16029-I to KAVF16033-W, KAVK37242-E to KAVK37244-E, KAVK37850-E to KAVK37875-E, and KAVK38001-E to KAVK38816-E
- The following messages have been deleted:

KAVF16019-E, KAVF09000-I to KAVF09017-E, KAVK11000-I, KAVK11002-I, and KAVK38600-E
- The following messages have been changed:

KAVK08176-E
- A function that automatically restarts the PFM service when it has stopped abnormally during operation has been added to PFM - Manager. Accordingly, the following folder has been added to the list of properties for the Agent Collector service:

Restart Configurations

- The notes about migrating from an older version of Performance Management to a newer version have been added.
- An explanation about the version compatibility has been added.
- Support of Windows Internet Explorer 8 has been added.
- Extensible Service IE Probe has been added to the list of services.
- The following three items have been added to the definition in the `General` section of the Probe action condition definition file:
 - `ie_service_flag`
 - `disable_ssl_protocol`
 - `html_script_skip_flag`
- IE Probe Daemon has been added in the description of the integrated trace log.

M. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

M.1 Related publications

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

Manuals associated with JP1/Performance Management:

- *JP1 Version 11 Performance Management: Getting Started (Operation and Performance Management)* (3021-3-A36(E))
- *JP1 Version 11 JP1/Performance Management Planning and Configuration Guide* (3021-3-A37(E))
- *JP1 Version 11 JP1/Performance Management User's Guide* (3021-3-A38(E))
- *JP1 Version 11 JP1/Performance Management Reference* (3021-3-A39(E))

Manuals associated with JP1:

- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems

M.2 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
AIX		AIX V6.1
		AIX V7.1
		AIX V7.2
JP1/IM	JP1/IM - Manager	JP1/Integrated Management - Manager
	JP1/IM - View	JP1/Integrated Management - View
JP1/ITSLM (10-50 or earlier)	JP1/ITSLM - Manager	Job Management Partner 1/IT Service Level Management - Manager
	JP1/ITSLM - UR	Job Management Partner 1/IT Service Level Management - User Response
JP1/SLM	JP1/SLM - Manager	JP1/Service Level Management - Manager
	JP1/SLM - UR	JP1/Service Level Management - User Response
JP1/SD	JP1/Software Distribution	Job Management Partner 1/Software Distribution Client
		Job Management Partner 1/Software Distribution Manager

Abbreviation		Full name or meaning	
JP1/SD	JP1/Software Distribution	Job Management Partner 1/Software Distribution SubManager	
Linux	CentOS	CentOS 6 (x64)	CentOS 6.1 (x64) or later
		CentOS 7	CentOS 7.1 or later
	Linux 6 (x64)		Red Hat Enterprise Linux(R) Server 6.1 (64-bit x86_64) or later
	Linux 7		Red Hat Enterprise Linux(R) Server 7.1 or later
	Oracle Linux	Oracle Linux 6 (x64)	Oracle Linux(R) Operating System 6.1 (x64) or later
		Oracle Linux 7	Oracle Linux(R) Operating System 7.1 or later
	SUSE Linux	SUSE Linux 12	SUSE Linux(R) Enterprise Server 12
Performance Management		JP1/Performance Management	
PFM - Agent	PFM - Agent for JP1/AJS [#]		JP1/Performance Management - Agent Option for JP1/AJS3
	PFM - Agent for Cosminexus [#]		JP1/Performance Management - Agent Option for uCosminexus Application Server
	PFM - Agent for DB2		JP1/Performance Management - Agent Option for IBM DB2
	PFM - Agent for Domino		JP1/Performance Management - Agent Option for IBM Lotus Domino
	PFM - Agent for Enterprise Applications		JP1/Performance Management - Agent Option for Enterprise Applications
	PFM - Agent for Exchange Server [#]		JP1/Performance Management - Agent Option for Microsoft(R) Exchange Server
	PFM - Agent for HiRDB [#]		JP1/Performance Management - Agent Option for HiRDB
	PFM - Agent for WebSphere MQ [#]		JP1/Performance Management - Agent Option for IBM WebSphere MQ
	PFM - Agent for IIS [#]		JP1/Performance Management - Agent Option for Microsoft(R) Internet Information Server
	PFM - Agent for Microsoft SQL Server		JP1/Performance Management - Agent Option for Microsoft(R) SQL Server
	PFM - Agent for Oracle		JP1/Performance Management - Agent Option for Oracle
	PFM - Agent for Platform	PFM - Agent for Platform (UNIX)	JP1/Performance Management - Agent Option for Platform (UNIX)
		PFM - Agent for Platform (Windows)	JP1/Performance Management - Agent Option for Platform (Windows)
	PFM - Agent for Transaction System [#]		JP1/Performance Management - Agent Option for Transaction System

Abbreviation		Full name or meaning	
PFM - Agent	PFM - Agent for Service Response	JP1/Performance Management - Agent Option for Service Response	
	PFM - Agent for WebLogic Server [#]	JP1/Performance Management - Agent Option for Oracle(R) WebLogic Server	
	PFM - Agent for WebSphere Application Server [#]	JP1/Performance Management - Agent Option for IBM WebSphere Application Server	
PFM - Base		JP1/Performance Management - Base	
PFM - Manager		JP1/Performance Management - Manager	
PFM - RM	PFM - RM for Microsoft SQL Server	JP1/Performance Management - Remote Monitor for Microsoft(R) SQL Server	
	PFM - RM for Oracle	JP1/Performance Management - Remote Monitor for Oracle	
	PFM - RM for Platform	PFM - RM for Platform (UNIX)	JP1/Performance Management - Remote Monitor for Platform (UNIX)
		PFM - RM for Platform (Windows)	JP1/Performance Management - Remote Monitor for Platform (Windows)
	PFM - RM for Virtual Machine	JP1/Performance Management - Remote Monitor for Virtual Machine	
PFM - Web Console		JP1/Performance Management - Web Console	

PFM - Manager, PFM - Agent, PFM - Base, PFM - Web Console, and PFM - RM may be referred to collectively as *Performance Management*.

#

This product only runs in a Japanese environment.

M.3 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
BOM	Byte Order Mark
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
XML	Extensible Markup Language
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
HTML	Hyper Text Markup Language

Acronym	Full name or meaning
HTTP [#]	Hypertext Transfer Protocol
HTTPS [#]	Hypertext Transfer Protocol Security
IMAP4	Internet Message Access Protocol Version 4
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
NAPT	Network Address Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
ODBC	Open Database Connectivity
OS	Operating System
PDF	Portable Document Format
POP3	Post Office Protocol Version 3
PEM	Privacy Enhanced Mail
RFC	Request for Comments
SSL	Secure Socket Layer
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SCSI	Small Computer System Interface
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Access Control
URL	Uniform Resource Locator

#

HTTP and HTTPS might be referred to as *HTTP(S)*.

M.4 Conventions: Product names, service IDs, and service keys

Performance Management version 09-00 or later can display the product name as the service ID and service key by enabling the product name display functionality.

Identifiers	Product name display functionality	
	Disabled	Enabled
Service ID	<i>VS1hostname</i>	<i>hostname< Service Response >(Store)</i>
	<i>VA1hostname</i>	<i>hostname< Service Response ></i>
Service Key	agtv	SR

Hereafter in this manual, service IDs and service keys are shown in the format when the product name display functionality is enabled.

Note that you can enable the product name display functionality only when you satisfy the two conditions listed below:

- The version number of the prerequisite programs (PFM - Manager or PFM - Base) is 09-00 or later.
- The version number of PFM - Web Console and connection-target PFM - Manager is 09-00 or later.

M.5 Conventions: Installation folder

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

Installation-folder for PFM - Base:

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

This manual uses the term *installation folder* for the PFM - Base installation folder.

Installation-folder for PFM - Management:

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

Installation-folder for PFM - Web Console:

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

M.6 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.
- 1 TB (terabyte) is 1,024⁴ bytes.

N. Glossary

action

The operation that is automatically executed by Performance Management when the monitored data reaches the threshold. The following types of actions are available:

- E-mail transmission
- Command execution
- SNMP trap issuance
- JP1 event issuance

Action Handler

One of the PFM - Manager or PFM - Base services. It is a service for executing an action.

administration tool

Various types of commands and GUI functions that are used for checking service statuses and manipulating performance data. The following operations can be performed:

- Displaying service configuration and status
- Saving and restoring performance data
- Exporting of performance data to a text file
- Erasing of performance data

agent

The PFM - Agent service that collects performance data.

Agent Collector

One of the PFM - Agent services. It is a service for collecting performance data and evaluating performance data based on a threshold value that is set in an alarm.

Agent Store

One of the PFM - Agent services. It is a service for storing performance data. The Agent Store service uses a database for recording performance data. Each PFM - Agent has its own Agent Store service.

alarm

Information that defines the action to be taken or the event message to be issued when the monitored data reaches the threshold.

alarm table

A table into which one or more alarms are collected and which defines the following types of information:

- Objects to be monitored (Process, TCP, WebService, or the like)
- Information to be monitored (CPU usage, number of bytes received per second, or the like)
- Monitoring condition (threshold)

binding

The operation of associating an alarm with an agent. Once binding occurs, when the performance data collected by the agent reaches the threshold defined in the alarm, the user can be notified.

command registration file (espcommand.xml)

A file used to register created user-defined commands. This file is read when the Probe Daemon starts. Service-specific conditions for measuring a user-defined service are registered as command arguments in the command registration file.

Correlator

One of the PFM - Manager services. It is a service for controlling event delivery among services. When the alarm status being monitored by this service exceeds the threshold, this service sends an alarm event and an agent event to the Trap Generator service and PFM - Web Console.

database ID

An ID that is assigned to each record in PFM - Agent that indicates the database for storing records. A database ID indicates the type of records to be stored in the database. The following database IDs are used:

- **PI**: Indicates a database for records of the **PI** record type
- **PD**: Indicates a database for records of the **PD** record type
- **PL**: Indicates a database for records of the **PL** record type

data model

A general term for records and fields that each PFM - Agent has. Data models are managed according to version.

drilldown report

A report that is associated with a report or report field. You use a drilldown report to display the detailed information or related information of a report.

field

Individual operation information entries in a record. Each field serves as a monitoring item for Performance Management.

historical report

A report indicating the status of the monitoring target from the past to the present.

IE probe

A function for measurement (for measuring response performance of operations in Internet Explorer).

IE Probe Daemon

A service for measuring responses performance of operations in Internet Explorer.

IE probe management service

A service for managing the IE Probe Daemon.

IE Recorder

A GUI application used for defining IE scenario information and measurement conditions.

IE Recorder action condition definition file

A file defining IE Recorder's action condition settings. It is loaded when IE Recorder starts.

IE scenario

An operation or operations in the Internet Explorer defined as the measuring target of the response performance. You can define not only an operation but also multiple operations in the Internet Explorer as an IE scenario.

IE scenario file

A file used to define operation information in the Internet Explorer as an IE scenario when you measure IE scenarios. It is loaded when the IE Probe Daemon starts.

IE scenario measurement

You can measure the elapsed time between the time you perform operations in the Internet Explorer and the time these operations are completed as the response performance. You can monitor the approximate response performance to the ones users feel when operating in the Internet Explorer.

To measure an IE scenario, you create an IE scenario, define IE scenario information, and measure the response time of the Internet Explorer according to the IE scenario. Since not only an operation but also multiple operations in the Internet Explorer defined in the IE scenario are simulated to perform, you can measure the response performance of multiple operations as well as an operation in the Internet Explorer. You can measure the response performance of the any page transition as well as the response performance of the entire IE scenario. You can also detect problems of the measurement targets by checking the responses while measuring IE scenarios.

instance

In this manual, the term *instance* is used in the following ways:

- To indicate a recording format for records
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*; and each line inside a record is called an *instance*.
- To indicate a PFM - Agent startup method
When a single agent monitors the monitoring targets on the same host, it is called a *single-instance agent*. In contrast, when the monitoring targets support multiple instances, each agent can monitor each monitoring target instance. This is called a *multi-instance agent*. Each agent of a multi-instance agent is called an *instance*.

JP1/SLM

A product that performs monitoring from the viewpoint of performance as experienced by the service users of a business system, and that supports service-level maintenance. Linkage with JP1/SLM can enhance monitoring of the operating status.

lifetime

The duration in which the integrity of the performance data collected into each record can be guaranteed.

Master Manager

One of the PFM - Manager services. It is the main service of PFM - Manager.

Master Store

One of the PFM - Manager services. It is a service for managing the alarm events issued by each PFM - Agent. The Master Store service uses a database for holding event data.

measurement condition ID

A unique number assigned to a measurement condition for management purposes. A measurement condition ID cannot be duplicated because it becomes the identifier for each measurement condition. The same measurement condition can be registered more than once as separate measurement conditions, by assigning different measurement condition IDs.

measurement condition label definition file (esptasklabel.conf)

A file used to define a desired label name for the measurement conditions for each Internet service.

measurement condition registration file (esptask.xml)

A file used to register measurement conditions, such as the service type of the measurement target, the host name, and the measurement interval. This file is read when the Probe Daemon starts.

monitoring template

Predefined alarms and reports provided in PFM - Agent. The monitoring template enables you to easily prepare for monitoring the operating status of PFM - Agent without writing any complicated definitions.

multi-instance record

A record that is recorded in multiple lines. Such records have a specific ODBC key field.

See *Instance*.

Name Server

One of the PFM - Manager services. It is a service for managing the service configuration information inside a system.

ODBC key field

These fields display the primary keys that are necessary to use the data retrieved from records stored in the Store database on either PFM - Manager or PFM - Base. Some ODBC key fields are common to all records, while others are unique to some records.

password file

A file used to manage the passwords that are needed to log into Internet services. The password utility is used to register passwords into the password file. The registered passwords are converted to character strings.

password utility

The `esppasswd` command, which is used to register, change, and delete passwords.

PD record type

See *Product Detail record type*.

performance data

Resource usage data collected from a monitoring target system.

Performance Management

A general term for a group of software programs necessary for monitoring and analyzing issues related to system performance. Performance Management consists of the following five program products:

- PFM - Manager
- PFM - Web Console
- PFM - Base
- PFM - Agent
- PFM - RM

PFM - Agent

One of the program products comprising Performance Management. PFM - Agent that is equivalent to a system-monitoring facility. Various types of PFM - Agent are available according to the applications, databases, and OSs to be monitored. PFM - Agent has the following functions:

- Monitoring of the performance of the monitoring target
- Collection and recording of data from the monitoring target

PFM - Base

One of the program products comprising Performance Management. PFM - Base provides the basic functions for Performance Management to monitor operations. It is a prerequisite program product for PFM - Agent. PFM - Base provides the following functionality:

- Management tools such as various types of commands
- Common functions needed for linking Performance Management to other systems

PFM - Manager

One of the program products comprising Performance Management. PFM - Manager is equivalent to a manager facility and has the following functions:

- Management of Performance Management program products
- Management of events

PFM - Manager name

A name that identifies the field stored in the Store database. This name is used for specifying a field in a command.

PFM - View name

The alias of a PFM - Manager name. The PFM - View name is more intuitive than the PFM - Manager name. For example, the PFM - View name of the PFM - Manager name `INPUT_RECORD_TYPE` is `Record Type`. The PFM - View names are useful when specifying fields on the GUI of PFM - Web Console.

PFM - Web Console

One of the program products comprising Performance Management. PFM - Web Console provides the web application server functions necessary for centrally monitoring the Performance Management system from a web browser. PFM - Web Console has the following functions:

- GUI display

- Integrated monitoring and management functions
- Report and alarm definition

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*.

PL record type

See *Product Log record type*.

probe

A function for executing measurement (for measuring an Internet service's response performance).

Probe action condition definition file (esp.conf)

A file containing the Probe Daemon's start option settings. This file is read when the Probe Daemon starts. The Probe action condition definition file contains start option settings, such as the maximum number of measurement conditions for a probe and the maximum size of a report file.

Probe Daemon

A service for measuring service responsiveness.

Product Detail record type

The record type that stores the performance data that indicates the system status at a given point in time, such as detailed information on the processes that are currently active. Use the PD record type when you want to determine the system statuses at a given point in time, such as those listed below:

- System's operating status
- Capacity of the file system currently being used

product ID

The 1-byte identifier that indicates the Performance Management program to which the service belongs. It is part of a service ID.

Product Interval record type

The record type that stores the performance data for a specific duration (interval), such as the number of active processes during every minute. Use the PI record type when you want to analyze the changes and trends in the system status over time, such as those listed below:

- Trend in the number of system calls that occurred within a specific time span
- Trend in the capacity of the file system being used

Product Log record type

The record type that stores the log information on applications that are being executed or databases being used on UNIX.

real-time report

A report indicating the current status of the monitoring target.

record

A group of operation information entries categorized by their purpose. A monitoring agent collects operation information from each record. The types of records that can be collected vary depending on the agent program.

report

A report defines the information to be used when graphically displaying the performance data collected by PFM - Agent. A report mainly defines the following types of information:

- Records to be displayed in a report
- Performance data display items
- Performance data display format (table, graph, or the like)

report file

A file used to store measurement results temporarily. The output format is CSV, with each row containing a single measurement result. If measurements extend over a specific period of time, results are output to this file for as many measurements as are executed. In the report file, the most recent value is collected by Agent Collector and managed in record format.

service ID

A unique ID assigned to the service of a Performance Management program. For example, to use a command to check the system configuration of Performance Management or to back up the performance data of individual agents, you specify the service ID of the Performance Management program and execute the command. The format of the service ID differs depending on whether the product name display functionality is enabled. For details about the service ID format, see the chapter explaining the Performance Management functions in the *JP1/Performance Management Planning and Configuration Guide*.

service type

A number indicating the type of an Internet service or user-defined service supported by PFM - Agent for Service Response.

single-instance record

A record that is recorded in a single line. Such records do not have a specific ODBC key field.

See *Instance*.

stand-alone mode

The mode in which PFM - Agent is running alone. Even when the Master Manager service and Name Server service of PFM - Manager cannot be started because of an error, you can start PFM - Agent alone and collect performance data.

status management function

A function for managing the statuses of all services that run on PFM - Manager and PFM - Agent. The status management function enables the system administrator to correctly determine the service startup and stop statuses at each host, making it possible to take the appropriate error recovery measures.

Store database

The database that stores the performance data collected by the Agent Collector service.

Trap Generator

One of the PFM - Manager services. It is a service that issues SNMP traps.

user-defined command

A program created to measure a service other than the standard Internet services supported by PFM - Agent for Service Response. One user-defined command can measure a single measurement item.

user-defined service

A service other than the standard Internet services supported by PFM - Agent for Service Response. The user can measure a user-defined service by creating a user-defined command, and then registering it into PFM - Agent for Service Response.

user-defined service ID

A unique number assigned to a measurement condition for a user-defined service, for management purposes. Each user-defined service ID must be unique, because it is used as the identifier of the measurement condition.

Web Recorder

A GUI used for defining Web transaction information and measurement conditions.

Web Recorder action condition definition file

A file containing Web Recorder's operating condition settings. It is read when Web Recorder starts.

Web transaction file

A file used to define information needed for Web transaction measurement, such as the following: the URL to be accessed by a target Web transaction, Web authentication, and a proxy. This file is read when the Probe Daemon starts.

Web transaction measurement

For measurement of an HTTP(S) service, a single set of a request and a response can be managed, as can a transaction consisting of multiple HTTP(S) requests and responses. To measure a Web transaction, a Web transaction file is created to define information about the Web transaction. Then HTTP(S) requests are issued according to that definition to measure response performance, such as the response time. Playback and measurement of a transaction are achieved by simulating a series of operations using a browser software (such as Internet Explorer). Web transaction measurement supports measurement of an entire Web transaction, measurement of response performance in any given page transition, and error detection in the measurement target by checking the response during transaction measurement processing.

Non-interactive (command)

Command execution method in which operator input required for command execution are provided by values in option specifications or in definition files.

Executing a command non-interactively saves work when configuring an operation monitoring system and can reduce user workload.

Index

A

abbreviations for products 722
acronyms 724
action 24, 727
Action Handler 727
action log
 settings 80
 setting up 197
actual host name 70
administration tool 727
agent 727
Agent Collector 727
 collection interval setting 144
Agent Collector service property 685
Agent Store 727
Agent Store service property 682
alarm 24, 727
 format of explanations 318
 FTP Failure 320
 FTP Response time 321
 IES Failure 322
 IES Replay Time 323
 IMAP4 Failure 324
 IMAP4 Response time 325
 list of 319
 POP3 Failure 326
 POP3 Response time 327
 SMTP Failure 328
 SMTP Response time 329
 TCP Failure 330
 TCP Response time 331
 WT Failure 332
 WT Response Time 333
alarm table 24, 727
alias name 70
applying definition information 102, 112, 124, 127

B

backup 92
binding 24, 728
browsing manuals in web browser 94

C

canceling

 connection-target PFM - Manager 83, 205
Change Password window 257
checking IE scenario 122
cluster software
 registering into 199
 releasing registration from 205
cluster system
 Installing up 73
 operation in 184
 overview of 185
 setting up 73
 setting up environment in 201
command
 list of 470
 storage directory 471
command registration file 308, 728
 definition 308
 example 309
 format 308
common field 424
common message log 79, 197, 653, 654
Conditions of Substitute String window 238
Conditions of Variable String window 234
 Substitute String page 235
 Variable String page 234
connection-target PFM - Manager
 canceling 83, 205
 setup of 194
conventions
 abbreviations for products 722
 acronyms 724
 fonts and symbols 10
 installation folder 726
 KB, MB, GB and TB 726
 product names, service ids, and service keys 725
 version numbers 11
Correlator 728
Create New Web Transaction window 214
creating IE scenario files 116

D

database ID 728
data collection procedure 661
data model 23, 414, 728

- data to be collected when problem occurs 657
- data type
 - list of 420
- defining IE scenarios 116
- defining measurement conditions 50, 99, 111, 123, 126
- definition examples 45, 62
- definition files 262
 - list of 263
 - used for environment setup 263
- definition procedure 97
- definitions for measuring IE scenarios 116
- detecting problem 664
- determining baselines 45
- DHCP (measurement condition) 282
- DHCP (PI_DHCP) record 428
- DHCP Response Time Status (real-time report) 343
- DHCP Response Time Status report 342
- DHCP Response Time Summary report 344
- DHCP Response Time Trend report 345
- direct entry mode 103
- disk space requirement
 - estimating 677
 - for operation in cluster system 677
- DNS (measurement condition) 282
- DNS (PI_DNS) record 430
- DNS Response Time Status (real-time report) 347
- DNS Response Time Status report 346
- DNS Response Time Summary report 348
- DNS Response Time Trend report 349
- drilldown report 728
 - field level 334
 - report level 334

E

- embedded resource
 - acquisition of 31
 - acquisition target of 31
- End Scope Settings window 259
- environment definition file
 - exporting logical host 207
 - importing logical host 207
- Error and normal alarms are raised alternately in PFM - Agent for Service Response measurement 675
- Error handling procedure for each problem 666
- error handling procedures 645
- esp.conf 266
- espcommand.xml 308

- esppasswd command 472
- esptask.xml 272
- esptasklabel.conf 310
- example
 - of performance monitoring operation 45
- Example of scope definitions 38

F

- failover
 - processing at 186
 - when error occurs 186
- field 23, 334, 728
 - added only when data is recorded in Store database 423
 - list of ODBC key fields 417
 - value 421
- files and folders, list of 701, 705–707, 717
- Filtering Conditions window 241
- firewall, passage direction 680
- font conventions 10
- FTP (measurement condition) 283
- FTP (PI_FTP) record 432
- FTP Failure alarm 320
- FTP Rate report 350
- FTP Response time alarm 321
- FTP Response Time Status (real-time report) 352
- FTP Response Time Status report 351
- FTP Response Time Summary report 353
- FTP Response Time Trend report 354
- FTP Top 10 report 355

G

- GB meaning 726

H

- HA cluster system 185
- historical report 23, 728
- hntr2util command 475
- HNTRLib2 90
- HTTP (measurement condition) 275
- HTTP (PI_HTP) record 435
- HTTP Rate report 356
- HTTP Response Time Status (real-time report) 358
- HTTP Response Time Status report 357
- HTTP Response Time Summary report 359
- HTTP Response Time Trend report 360

- HTTPS (measurement condition) 277
- HTTPS(PI_HTTPS) record 439
- HTTPS Rate report 362
- HTTPS Response Time Status (real-time report) 364
- HTTPS Response Time Status report 363
- HTTPS Response Time Summary report 365
- HTTPS Response Time Trend report 366
- HTTPS Top 10 report 367
- HTTP Top 10 report 361

I

- identification of tags 39
- identifier, list of 678
- Identifying Tags 119
- IE mode 103
- IE probe 728
- IE Probe Daemon 728
- IE probe management service 728
- IE probe service using Windows services
 - starting and stopping 137
- IE Recorder 728
 - setting action condition 81
 - windows 242
- IE Recorder (main) window 242
- IE Recorder action condition definition file 312, 729
 - definition 312
 - example 313
 - format 312
- IE Recorder Settings window 257
- IESCENA 286
- IE scenario 729
- IE scenario, measuring
 - overview of 37
- IE Scenario (PI_IES) record 445
- IE Scenario Detail report 368
- IE scenario file 729
- IE scenario files 315
- IE Scenario Logged Message report 369
- IE scenario measurement 729
- IE scenario operation check 67
- IE Scenario Overview (PI_IESO) record 446
- IE Scenario Replay Time Status (real-time report) 371
- IE Scenario Replay Time Status report 370
- IE Scenario Replay Time Summary report 372
- IE Scenario Replay Time Trend report 373
- IE Scenario Scope Detail report 374
- IE Scenario Scope Rate report 376

- IE Scenario Top 10 report 377
- IES Failure alarm 322
- IES Replay Time alarm 323
- IMAP4 449
 - measurement condition 281
- IMAP4 Failure alarm 324
- IMAP4 Rate report 378
- IMAP4 Response time alarm 325
- IMAP4 Response Time Status (real-time report) 380
- IMAP4 Response Time Status report 379
- IMAP4 Response Time Summary report 381
- IMAP4 Response Time Trend report 382
- IMAP4 Top 10 report 383
- installation
 - OS user permission necessary 72
- installation and setup procedures 69
- installation folder conventions 726
- instance 729
- integrated trace log 654, 656
- integrated trace log function settings, changing 90
- integrated trace log settings
 - changing 475
- Internet service, measuring
 - definition for 99
 - overview of 28
- Interpolating performance data 90
- IP addresses, setting 70
- IPv4 and IPv6 environments, communication in 716

J

- JP1/SLM 729
 - linkage with JP1/SLM 715
- jpccconf db define command 85
- jpchosts file 197
- jpccras command 661
- jpcsto.ini
 - setting items 86
- jpcsto.ini file to change settings 86
- jpccvierec.conf 312
- jpccvtaskctl command 476
- jpccvtest command 482

K

- KB meaning 726

L

- lifetime [729](#)
- list, process [679](#)
- lists of log files and folders accessed upon troubleshooting [654](#)
- log file [654](#)
 - changing size [79](#)
- log files and folders
 - common message log [654](#)
 - integrated trace log [656](#)
 - trace log [655](#)
- log file size
 - changing [197](#)
- Logged Message for IE Scenario (PL_IESM) record [452](#)
- logical host environment
 - canceling setup at executing node [203](#)
 - canceling setup at standby node [205](#)
 - canceling setup for other Performance Management programs [204](#)
 - setting up at executing node [194](#)
 - setting up for other Performance Management programs [197](#)
 - setting up for PFM - Agent for Service Response [194](#)
 - setting up for standby system [198](#)
- logical host environment definition
 - exporting [197, 204](#)
 - importing [198](#)
- logical host environment definition file to standby node, copying [198, 204](#)
- log information to be collected upon troubleshooting [653](#)
- log-on account
 - setting service [196](#)
- log types
 - common message log [653](#)
 - integrated trace log [654](#)
 - operation status log [653](#)
 - system log [653](#)
 - trace log [654](#)

M

- Master Manager [729](#)
- Master Store [730](#)
- MB meaning [726](#)
- measurement
 - of IE scenarios [36](#)

- of Internet services [27](#)
- of performance response for operations in Internet Explorer [37](#)
- of performance response for page transitions [30](#)
- of user-defined services [40](#)
- of Web transactions [28, 45](#)
- measurement condition ID [730](#)
- measurement condition label definition file [310, 730](#)
 - definition [310](#)
 - example [311](#)
 - format [310](#)
- measurement condition registration file [272, 730](#)
 - definition [273](#)
 - example [287](#)
 - format [273](#)
 - measurement condition (common section), format and definition of [274](#)
 - measurement condition (service-specific section), format and definition of [275](#)
- Measurement items [123](#)
- measurement of a task
 - pausing [476](#)
- Measurement of IE scenarios [62](#)
- measurement tests
 - executing [482](#)
- measuring Web transactions, definition for [103](#)
- memory requirement, estimating [677](#)
- messages [491, 513](#)
 - explanation format [493](#)
 - format [492](#)
 - format of output [492](#)
 - notes for system administrator [493](#)
 - output destination [494](#)
 - outputting to Windows event log [511](#)
- monitoring template [25, 317, 730](#)
 - overview of [317](#)
- multi-instance record [730](#)

N

- Name Server [730](#)
- network
 - environment setup [70](#)
 - setting up [197](#)
 - specifying settings [79](#)
- network environment setup [70](#)
- non-interactive (command) [734](#)
- note

- on operation 140
- on system operation 140
- notes on IE scenarios 149
- notes on measurement
 - firewall/NAT environment 681
- notes on navigation 166

O

- ODBC key field 730
- operation method, changing 85
- Operation Settings window 250
 - Operation Target page 252
 - Response Determination page 255
 - Wait Time page 250
- operation status log 653
- OS, requisite 70

P

- passage direction, firewall 680
- password
 - changing 472
 - deleting 472
 - registering 472
- password file 730
- password utility 99, 472, 730
- Pausing and resuming a measurement 41
- performance data 730
 - changing storage destination 85
 - changing storage location 79
 - collection procedure 44
 - management procedure 44
 - overview of collecting 44
 - overview of managing 44
- performance data storage destination
 - changing 197
- Performance Management 731
 - checking startup 201
 - checking stop 201
 - setup required to operate 193
- performance management system error recovery 665
- Performing pre-measurement check on target Web pages 116
- PFM - Agent 731
- PFM - Agent for Service Response
 - before installation 70, 190
 - before setup 70

- canceling setup 82, 202, 203
- canceling setup in logical host environment 203
- changing definition files 207
- changing operation method 207
- constructing environment for 188
- copying definition files for 199
- features of 22
- flow from installation to starting operation 188
- flow of canceling setup 202
- flow of uninstallation 202
- function of 27
- installation procedure 75
- installing 68, 193
- properties of 682
- registering 77, 193
- registering into cluster software 199
- setting start option for 80, 195
- setting up 68
- setting up environment for 188
- setup procedure 76
- starting 134
- stopping 134
- uninstalling 82, 83, 202, 206
- unsetup procedures 83
- PFM - Agent for Service Response cannot perform measurements 667
- PFM - Agent for Service Response service cannot be started 666
- PFM - Base 731
 - installing 193
 - uninstalling 206
- PFM - Manager 731
 - effects of failure 186
- PFM - Manager for connection target
 - setting 80
- PFM - Manager name 731
- PFM - View name 731
- PFM - Web Console 731
 - defining measurement conditions 128
- physical host 732
- PI_DHCP 428
- PI_DNS 430
- PI_FTP 432
- PI_HTP 435
- PI_HTTPS 439
- PI_IES 445
- PI_IESO 446

- PI_IMP4 449
- PI_PI 457
- PI_POP3 454
- PI_SMTP 458
- PI_TCP 461
- PI_UDEF 463
- PI_WT 464
- PI_WTO 467
- PI record type 732
- PL_IESM 452
- PL record type 732
- POP3 (measurement condition) 280
- POP3 (PI_POP3) record 454
- POP3 Failure alarm 326
- POP3 Rate report 384
- POP3 Response time alarm 327
- POP3 Response Time Status (real-time report) 386
- POP3 Response Time Status report 385
- POP3 Response Time Summary report 387
- POP3 Response Time Trend report 388
- POP3 Top 10 report 389
- port number
 - deleting settings 203
 - list of 680
 - setting 71
- probe 732
 - maximum number of measurement conditions 141
- Probe action condition definition file 266, 732
 - definition 267
 - example 270
 - format 266
- Probe Daemon 732
- problem
 - detecting 664
- process, list of 679
- Product Detail record type 23, 24, 732
- Product Interval record type 23, 732
- Product Log record type 732
- product names conventions 725
- Properties window 223
 - Page Info page 223
 - Proxy page 229
 - Request Info page 225
 - Response Determination page 230
 - Variable String page 232
 - Web Authentication page 227
- purpose

- of performance monitoring 45

R

- real-time report 23, 733
- record 23, 334, 413, 733
 - explanation format 415
 - list of 427
- recording IE scenario 118
- recording IE scenarios 63
- recording Web transactions 46
- record type
 - PD record type 23, 24, 730
 - PI record type 23
- registration measurement conditions 66
- related publications 722
- replaying by step IE scenarios 122
- replaying IE scenarios 122
- Replay Report window 260
- report 23, 733
 - DHCP DHCP Response Time Status (real-time report) 343
 - DHCP Response Time Status 342
 - DHCP Response Time Summary 344
 - DHCP Response Time Trend 345
 - DNS Response Time Status 346
 - DNS Response Time Status (real-time report) 347
 - DNS Response Time Summary 348
 - DNS Response Time Trend 349
 - folder organization 335
 - format of explanations 334
 - FTP Rate 350
 - FTP Response Time Status 351
 - FTP Response Time Status (real-time report) 352
 - FTP Response Time Summary 353
 - FTP Response Time Trend 354
 - FTP Top 10 355
 - HTTP Rate 356
 - HTTP Response Time Status 357
 - HTTP Response Time Status (real-time report) 358
 - HTTP Response Time Summary 359
 - HTTP Response Time Trend 360
 - HTTPS Rate 362
 - HTTPS Response Time Status 363
 - HTTPS Response Time Status (real-time report) 364
 - HTTPS Response Time Summary 365
 - HTTPS Response Time Trend 366
 - HTTPS Top 10 367

- HTTP Top 10 [361](#)
- IE Scenario Detail [368](#)
- IE Scenario Logged Message [369](#)
- IE Scenario Replay Time Status [370](#)
- IE Scenario Replay Time Status (real-time report) [371](#)
- IE Scenario Replay Time Summary [372](#)
- IE Scenario Replay Time Trend [373](#)
- IE Scenario Scope Detail [374](#)
- IE Scenario Scope Rate [376](#)
- IE Scenario Top 10 [377](#)
- IMAP4 Rate [378](#)
- IMAP4 Response Time Status [379](#)
- IMAP4 Response Time Status (real-time report) [380](#)
- IMAP4 Response Time Summary [381](#)
- IMAP4 Response Time Trend [382](#)
- IMAP4 Top 10 [383](#)
- list of [338](#)
- POP3 Rate [384](#)
- POP3 Response Time Status [385](#)
- POP3 Response Time Status (real-time report) [386](#)
- POP3 Response Time Summary [387](#)
- POP3 Response Time Trend [388](#)
- POP3 Top 10 [389](#)
- Scope Detail [390](#)
- SMTP Rate [391](#)
- SMTP Response Time Status [392](#)
- SMTP Response Time Status (real-time report) [393](#)
- SMTP Response Time Summary [394](#)
- SMTP Response Time Trend [395](#)
- SMTP Top 10 [396](#)
- TCP Response Time Status [397](#)
- TCP Response Time Status (real-time report) [398](#)
- TCP Response Time Summary [399](#)
- TCP Response Time Trend [400](#)
- Transaction Detail [401](#)
- User Defined Service Response Time Status [402](#)
- User Defined Service Response Time Status (real-time report) [403](#)
- User Defined Service Response Time Summary [404](#)
- User Defined Service Response Time Trend [405](#)
- Web Transaction Response Time Status [406](#)
- Web Transaction Response Time Status (real-time report) [407](#)
- Web Transaction Response Time Summary [408](#)
- Web Transaction Response Time Trend [409](#)
- Web Transaction Scope Detail [410](#)

- Web Transaction Scope Rate [411](#)
- Web Transaction Top 10 [412](#)
- report file [733](#)
- required program [72](#)
- requirement
 - disk space, estimating [677](#)
 - memory, estimating [677](#)
 - system, estimating [677](#)
- requisite OS [70](#)
- response determination [30, 38, 121](#)
- response performance information [22](#)
- restoration [93](#)
- resumes the measurement of a task
 - resuming [476](#)

S

- Save As window [216](#)
- saving IE scenario [123](#)
- scope
 - deleting [109](#)
 - example of definition [30](#)
 - setting [109](#)
 - setting end of [109](#)
 - setting start of [109](#)
- Scope Detail report [390](#)
- Scope List window [259](#)
- Selecting the type of measurement for Web server monitoring [43](#)
- Select Scope window [218](#)
- Select Source of Substitute String Settings window [240](#)
- Select Source of Variable String Settings window [237](#)
- Select Web Transaction window [217](#)
- service
 - list of [135](#)
 - setting to start automatically [136](#)
 - starting [136](#)
 - stopping [136](#)
 - using command to start and stop [137](#)
- service ID [733](#)
- service ids conventions [725](#)
- service keys conventions [725](#)
- service measurement definition
 - notes on [98](#)
- Service Summary Interval (PI_PI) record [457](#)
- service type [733](#)
- setting breakpoints [122](#)
- setting conditions for dynamic session management [55](#)

- setting IE scenario options 119
- setting Internet Options 117
- setting of Character set 32
- setting required to view manuals 94
- setting scopes 118
 - deleting 119
 - end 119
 - start 118
- Setting substitute strings 113
- setting language environment 77, 193
- setting up IP addresses 70
- setting up port numbers 71
- Setting variable strings 113
- setup command, executing 78, 79
- setup file, copying 78
- Set Web Transaction Conditions window 218
 - Default Proxy page 220
 - Request Info page 220
 - SSL Authentication page 222
 - Web Transaction Info page 218
- shared disk
 - placing offline 198
 - placing online 194
- single-instance record 733
- SMTP (measurement condition) 279
- SMTP (PI_SMTP) record 458
- SMTP Failure alarm 328
- SMTP Rate report 391
- SMTP Response time alarm 329
- SMTP Response Time Status (real-time report) 393
- SMTP Response Time Status report 392
- SMTP Response Time Summary report 394
- SMTP Response Time Trend report 395
- SMTP Top 10 report 396
- stand-alone mode 733
- starting automatically
 - IE probe 140
- starting IE Recorder 117
- Start Scope Settings window 258
- status management function 664, 733
- step
 - adding 108
 - deleting 109
 - inserting 108
- step information
 - changing 108
 - customizing 108

- defining 104
- defining (direct entry mode) 107
- list of items 105
- recording (IE mode) 106
- required items 105
- Store database 24, 734
- summary rule 418
- support for dynamic session management 32
- symbol conventions 10
- system configuration, changing 84
- system log 653
- system requirement, estimating 677

T

- task information
 - applying 131
 - distributing 133
 - setting 130
- tasks
 - adding 129
 - deleting 130
- TB meaning 726
- TCP (measurement condition) 284
- TCP (PI_TCP) record 461
- TCP Failure alarm 330
- TCP Response time alarm 331
- TCP Response Time Status (real-time report) 398
- TCP Response Time Status report 397
- TCP Response Time Summary report 399
- TCP Response Time Trend report 400
- testing IE scenarios 65
- testing measurement conditions 53
- testing measurements 123
- time, changing 140
- timeout value 142
- trace log 654, 655
- transaction, setting 110
- Transaction Detail 401
- Trap Generator 734
- troubleshooting 647
- types of log information to be collected upon troubleshooting 653

U

- updating Store version to 2.0 88
- url encoded 33

- url encoding process 33
- user-defined command 40, 734
- user-defined service 40, 734
 - definition for measuring 125
 - overview of measurement 40
- User Defined Service (PI_UDEF) record 463
- user-defined service ID 734
- User Defined Service Response Time Status (real-time report) 403
- User Defined Service Response Time Status report 402
- User Defined Service Response Time Summary report 404
- User Defined Service Response Time Trend report 405
- USERSERV (measurement condition) 286

V

- version number conventions 11
- version upgrade, notes on 74
- viewing manuals 95

W

- Web Recorder 734
 - basic window operation 210
 - setting action condition 81
 - window 209, 212
 - window transition 210
- Web Recorder (main) window 212
 - menu items in 213, 247
- Web Recorder action condition definition file 289, 734
 - definition 289
 - example 290
 - format 289
- WEBTRANS (measurement condition) 285
- Web Transaction (PI_WT) record 464
- Web transaction definition, displaying and editing existing 110
- Web transaction file 291, 734
 - definition of measurement condition 292
 - definition of overall 291
 - example 306
 - format of measurement condition 292
 - format of overall 291
- Web transaction measurement 734
 - overview of 29
- Web transaction measurement test 34
- web transaction operation check 62
- Web Transaction Overview (PI_WTO) record 467

- Web Transaction Response Time Status (real-time report) 407
- Web Transaction Response Time Status report 406
- Web Transaction Response Time Summary report 408
- Web Transaction Response Time Trend report 409
- Web Transaction Scope Detail report 410
- Web Transaction Scope Rate report 411
- Web Transaction Top 10 report 412
- wr.conf 289
- WT Failure alarm 332
- WT Response Time alarm 333

X

- XML format, specification 264
 - case 264
 - character requiring replacement 264
 - comment, specifying 264
 - end tag 264
 - linefeed character, deletion of 264
 - linefeed code 264
 - space, deletion of 264
 - start tag 264
 - tab, deletion of 264

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
