HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/IT Service Level Management Description, User's Guide, Reference and Operator's Guide

3021-3-311-20(E)

Notices

■ Relevant program products

Job Management Partner 1/IT Service Level Management - Manager (for Windows)

P-292C-FAAL Job Management Partner 1/IT Service Level Management - Manager version 10-50 (for Windows Server 2008 R2,Windows Server 2012)

Job Management Partner 1/IT Service Level Management - User Response (for Windows)

P-292C-FBAL Job Management Partner 1/IT Service Level Management - User Response version 10-50 (for Windows Server 2008 R2,Windows Server 2012)

■ 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

Adobe and Flash Player are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

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

IBM, DB2 are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

IBM is a trademark 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.

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

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

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

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

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

Microsoft is either a registered trademark or a trademark 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.

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

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.

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.

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

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

This product includes software developed by Andy Clark.

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

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

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

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

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

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

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

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

Job Management Partner 1/IT Service Level Management - Manager and Job Management Partner 1/IT Service Level Management - User Response includes RSA$^{(R)}$ BSAFE^{TM} Cryptographic software of EMC Corporation.

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

■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Windows	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	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
		Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard
Internet Explorer		Microsoft(R) Internet Explorer(R)
		Windows(R) Internet Explorer(R)

■ 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

Dec. 2014: 3021-3-311-20(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-311-10(E)) and product changes related to this manual.

Changes	Location
The following changes were made to support the system monitoring configuration: • The system configuration description was changed. • The procedures for registering monitored services and setting up monitoring items were changed. • A description about the `-m` argument was added to the explanation of the `jslmmgrimport` command. • Changes were made to the following windows and descriptions: Add template window Add/Delete monitor area Monitor settings area	*1.3*, *3.2*, *3.2.1*, *3.2.2*, *3.2.8*, *3.3.3*, *jslmmgrimport* in *Chapter 9*, *10.5.4*, *10.6.4*, *10.6.19*
A description of detection methods was added because the `serviceBaselineExclusion` and `systemBaselineExclusion` properties were added.	*3.1.2*
Because the node status display switch function was added, the following window was changed: • **Performance chart** tab in the Troubleshoot window	*3.1.2*, *3.1.3*, *3.1.4*, *4.4.1*, *4.4.2*, *4.6.1*, *4.6.2*, *4.6.3*, *10.4.4*, *10.4.5*, *10.4.6*
A description was added stating that a node state can be selected to check the timing of an event that caused an error or warning.	*4.4.1*
The procedure for releasing the linkage between ITSLM and Performance Management was changed.	*5.4.3*
The following JP1 events were added: • `0x00006893` • `0x00006894` • `0x00006895` The description stating that JP1 events related to an overage of a threshold are not issued in system performance was changed to state that JP1 events are issued in accordance with property settings.	*5.5.1*, *5.5.2*
The following properties were added as definitions that can be edited by ITSLM: • `dashboardChartPlotInterval` • `dashboardPrioritizeSystem` • `dashboardPropagateSystemStatus` • `JP1EventForSystem` • `serviceBaselineExclusion` • `systemBaselineExclusion`	*5.6.2*
A description was added stating that `service` cannot be specified for the `-t` option when a service in a system monitoring configuration is specified for the `-s` option.	*jslmreport* in *Chapter 9*
The description of a window was changed because the system performance monitoring status is propagated to the service status.	*10.4.4*
A description was added explaining how a performance chart is displayed for a range containing no performance data.	*10.4.4*

Changes	Location
A description was added stating that a performance chart might not be displayed correctly if data for a version earlier than 10-10 is stored in the database and **Monitor item state** is selected in **Node state display**.	*10.4.4*
The descriptions of the following messages were changed: `KNAS15503-E`, `KNAS15721-E`, `KNAS15817-E`, `KNAS15913-E`, `KNAS17603-E`, `KNAS17802-E`	*11.3*
A description of the port numbers used in ITSLM communication and the direction of communication through the firewall were added.	*Appendix B*

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

Preface

This manual describes the functions and operation of *Job Management Partner 1/IT Service Level Management - Manager* and *Job Management Partner 1/IT Service Level Management - User Response*.

Job Management Partner 1/IT Service Level Management - Manager and Job Management Partner 1/IT Service Level Management - User Response are used to monitor the status of services in order to maintain a desired level of service.

In this manual, the combination of Job Management Partner 1/IT Service Level Management - Manager and Job Management Partner 1/IT Service Level Management - User Response is abbreviated as *ITSLM*.

In other Job Management Partner 1 product names, *Job Management Partner 1* is abbreviated as *JP1*.

■ Intended readers

This manual is intended for members of a monitoring staff who use ITSLM to monitor the status of service levels, as well as for system operators (system administrators) who deploy and troubleshoot ITSLM.

Readers of this manual must have:

Monitoring staff:
    A basic knowledge of the operating system

System operators (system administrators):
    A basic knowledge of the applicable operating system
    A basic knowledge of networking
    A basic knowledge of JP1/Base

■ Conventions: Fonts and symbols

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

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`.

Text formatting	Convention
`Monospace`	• Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
|	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means `A`, or `B`, or `C`.
{ }	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of `A`, or `B`, or `C`.
[ ]	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
...	In coding, an ellipsis (`...`) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify `B` as many times as necessary.
< >	Angle brackets indicate items that might be displayed more than once. For example: *monitoring-item-name*< Δ *monitoring-item-name* `...`> This means that following *monitoring-item-name*, a single-byte space (Δ) and *monitoring-item-name* might be displayed repeatedly.

■ Conventions: ITSLM installation folder

This manual uses the following conventions to indicate the ITSLM product installation folder:

Product name	Convention used to indicate the installation folder	Default installation folder#
IT Service Level Management - Manager	*ITSLM-Manager-installation-folder*	*system-drive*`:\Program Files\HITACHI\JP1ITSLM`
IT Service Level Management - User Response	*ITSLM-UR-installation-folder*	

#

The default installation folder is the folder into which the ITSLM products are installed when no other folder is specified. Note also that the *system-drive*`:\Program Files` portion is determined by a value set in an OS environment variable at the time of installation, so it might be different in your environment.

■ 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

1 About ITSLM

ITSLM is a product that provides support for maintaining service levels to certain standards.

This chapter provides an overview of ITSLM and explains the system configuration, the flow of monitoring jobs, and the tasks that can be achieved by using ITSLM. It also explains that when ITSLM is linked with Performance Management, it can also be used for monitoring the status of hosts and middleware. The chapter also discusses the relationship between the organization of this manual and the expected tasks.

1.1 Support for maintaining service levels

In recent years, many business systems have been created to provide services to users.

For example, suppose that a company outsources a business system to a data center so that users can access the business system while it is running on the data center's servers. In such a case, the business system can be regarded as a service being provided to a customer.

If a company runs and manages an in-house business system and the users of the business system are the company's own employees, the business system provided from the servers can still be regarded as a service for users (who, in this case, are employees).

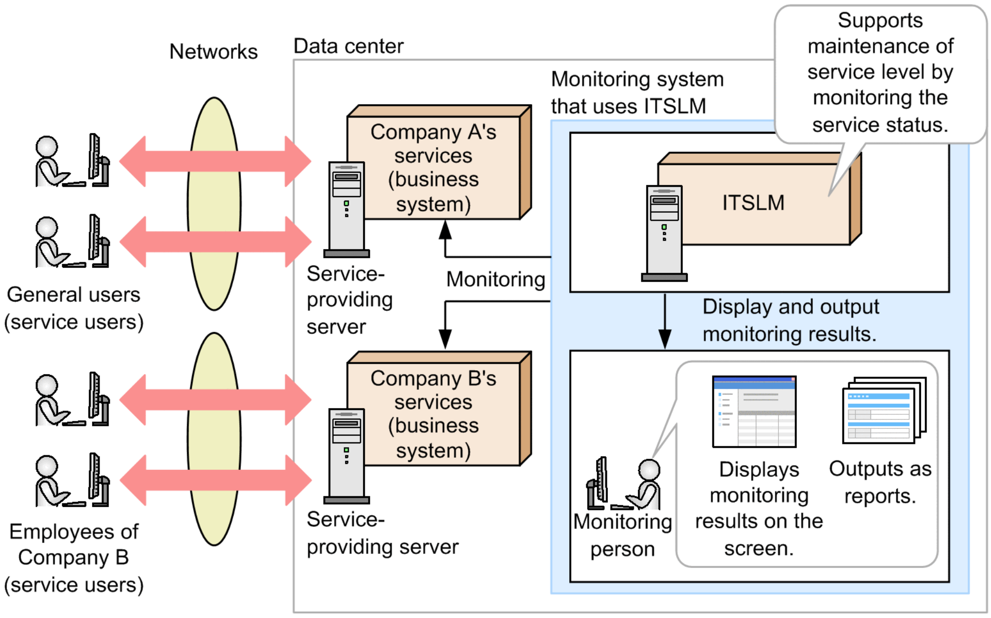
In both cases, the business system (the service) is running normally from the perspective of the service's users. A service provider must maintain the quality (*service level*) of the service it provides, and it must be able to provide the users with hassle-free service. To maintain the expected service level, the status of how the service is being provided must be monitored.

In a business context, there might be a contract between a service's outsourcing company and an outsourced contractor to maintain a certain service level. In such a case, it is crucial that the service status be monitored and the service level be maintained as stipulated in the contract.

ITSLM meets these demands by providing the capability to monitor service status and maintain a required service level.

The following figure provides an example of ITSLM deployed at a data center to monitor the service status and maintain the service level.

Figure 1–1: Example of ITSLM deployed at a data center to monitor the service status


Networks
Data center
Monitoring system that uses ITSLM
Supports maintenance of service level by monitoring the service status.
Company A's services (business system)
ITSLM
General users (service users)
Service-providing server
Monitoring
Display and output monitoring results.
Company B's services (business system)
Displays monitoring results on the screen.
Outputs as reports.
Employees of Company B (service users)
Service-providing server
Monitoring person

In this example, Companies A and B (service providers) outsource their business systems to a data center. Company A provides its service to general users (customers), while Company B provides its service to its own employees. The general users who use Company A's service and the employees of Company B are both service users.

By using ITSLM, you can monitor the statuses of the services of Companies A and B from their users' perspective. The monitoring results can be displayed on a monitoring person's computer, or output as reports. Use these monitoring results to maintain the level of service provided by Company A to the general users and the level of service Company B provides to its employees.

1.1.1 Support for providing stable service

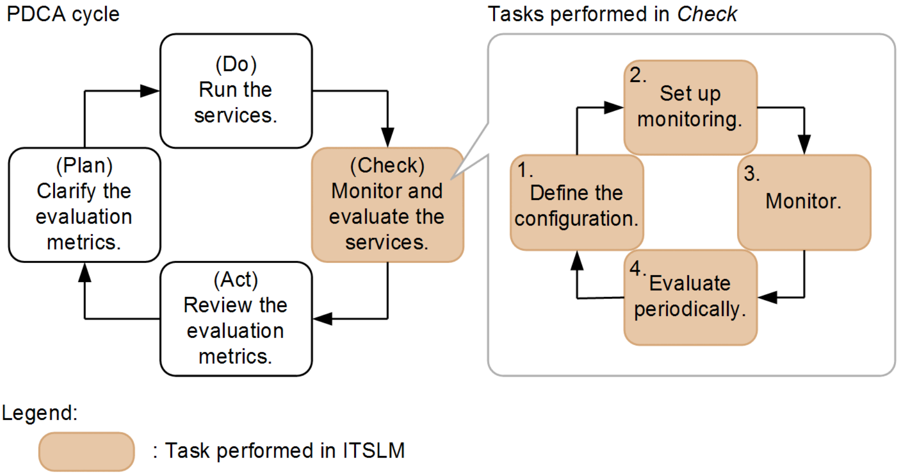
A service provider must be able to maintain the quality of the service and provide stable services to its users.

In other words, a service provider must set evaluation metrics (the *service level objectives* (SLOs)) to maintain the service level, and it must manage and run the service systematically.

To manage and run services systematically, it is helpful to apply a PDCA cycle. *PDCA* stands for *Plan-Do-Check-Act*, and ITSLM supports the tasks that correspond to *C* (*Check*) in the PDCA cycle.

The following figure shows the management and operation of services in a PDCA cycle when ITSLM is used.

Figure 1–2: Management and operation of services in a PDCA cycle using ITSLM


PDCA cycle
(Do) Run the services.
(Plan) Clarify the evaluation metrics.
(Check) Monitor and evaluate the services.
(Act) Review the evaluation metrics.
Tasks performed in *Check*
2. Set up monitoring.
1. Define the configuration.
3. Monitor.
4. Evaluate periodically.
Legend:
: Task performed in ITSLM

Of the *Check* tasks, ITSLM supports *service monitoring and evaluation*. Service monitoring and evaluation by ITSLM involves performing the following tasks cyclically:

1. Define the configuration.

   Define the services to be monitored.

   ITSLM achieves the independence of each customer's business systems by using *service groups* to group monitored services by customer (such as a company) and setting access permissions required for monitoring each group. Therefore, before monitoring can be started, individual services must be registered into ITSLM and then their service groups must be defined.

   ITSLM can help you register services by automatically detecting the URIs of the Web pages of the monitored services.

2. Set up monitoring.

   Configure how to monitor the monitored services.

   ITSLM specifies threshold values that will be used as evaluation metrics (SLOs) for maintaining the service level for each monitored service. Threshold values are provided for three items that are monitored: average response time, throughput, and error rate. Based on the specified threshold values, ITSLM can monitor for over-threshold values as well as possible future over-threshold values. The data obtained as a result of monitoring average response time, throughput, and error rate is referred to as the *service performance*. In addition to threshold values, you can also configure ITSLM to predict abnormalities in service performance stemming from unusual service statuses.

3. Monitor.

   Monitor actual accesses to the services according to the monitoring settings.

   ITSLM totals and analyzes actual accesses from service users and monitors for over-threshold values and possible future over-threshold values specified during monitoring setup, as well as for unusual service statuses (warning signs that might lead to abnormalities in service performance).

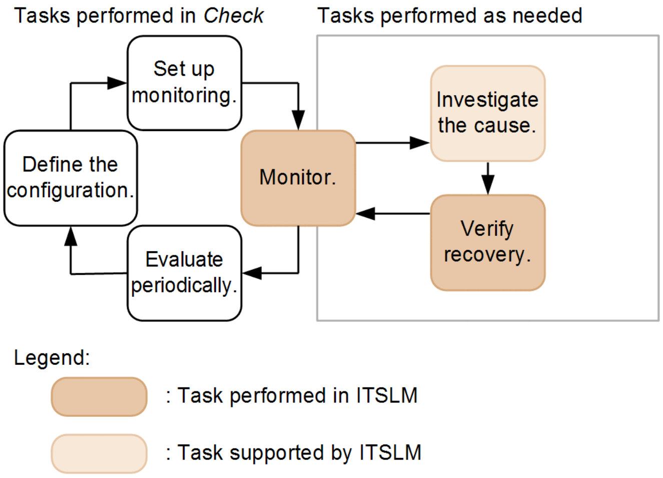
4. Evaluate periodically.

   Output reports of accumulated daily service statuses as monitoring results.

   Such reporting assists you in periodic evaluations to determine whether the evaluation metrics (SLOs) for maintaining the service level are being satisfied.

The monitoring task in 3 above requires some tasks that depend on the monitoring results. The following figure shows the tasks that must be performed depending on the monitoring task.

Figure 1–3: Tasks that must be performed depending on the monitoring task


Tasks performed in *Check*
Tasks performed as needed
Set up monitoring.
Define the configuration.
Monitor.
Evaluate periodically.
Investigate the cause.
Verify recovery.
Legend:
: Task performed in ITSLM
: Task supported by ITSLM

Monitoring, investigating the cause, and verifying recovery are performed in the cycle. Of the tasks that are performed as needed, ITSLM can support investigating the cause and verifying recovery.

Investigating the cause

If an abnormality or a warning sign that might lead to an abnormality is detected in the performance of a monitored service, its cause must be investigated promptly.

Because ITSLM can display ongoing service statuses (monitoring results) as graphs on the screen, the timing of an event that is the cause of a problem, or that might lead to a problem, can be identified more easily.

Verifying recovery

Because ITSLM monitors service statues, you can take an appropriate corrective action in response to a problem or a warning sign of an abnormality and then immediately check the current service status. This enables you to promptly determine whether services can be provided normally.

Thus, ITSLM plays an important role in the management and operation of services in the PDCA cycle and supports stable service operations.

1.1.2 Monitoring service status

If a service that has many users or that is critical to some users' business is interrupted, those users are greatly affected. ITSLM can achieve monitoring based on threshold values that are used as evaluation metrics (SLOs). ITSLM can also predict an abnormality in service performance by monitoring for unusual service status.

- Monitoring based on threshold values

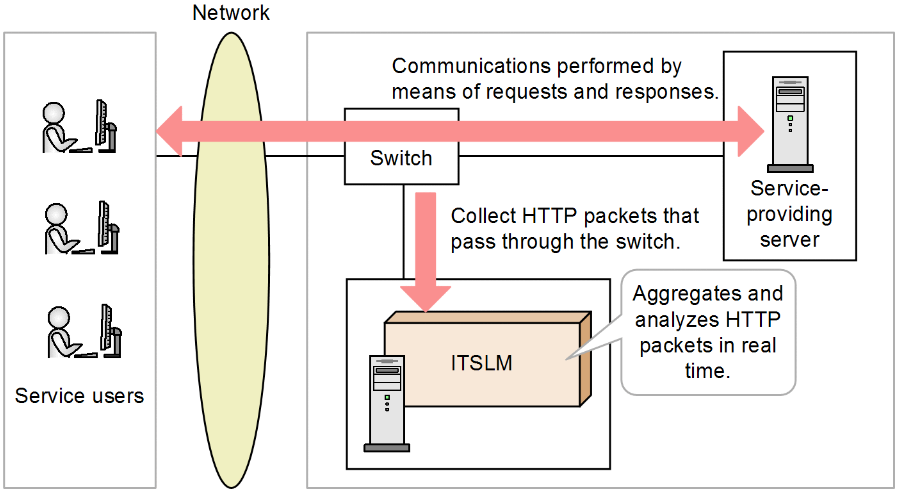
  You can evaluate service status based on specific metrics of the SLOs. You can also detect a service that might exceed an SLO in the future by analyzing trends in the service's status in real time.

- Monitoring for an unusual service status

You can detect at an early stage a warning sign of a possible abnormality that feels unusual to service users, before it develops into a real service performance error. By handling an abnormality at the stage of the early warning sign, you can provide stable services and increase service users' sense of satisfaction.

The following figure shows how ITSLM performs monitoring.

Figure 1–4: Mechanism of monitoring by ITSLM


Network
Communications performed by means of requests and responses.
Switch
Service-providing server
Collect HTTP packets that pass through the switch.
Aggregates and analyzes HTTP packets in real time.
ITSLM
Service users

ITSLM collects, aggregates, and analyzes in real time the HTTP packets that constitute the requests and responses sent between the service users and the service providing server. ITSLM monitors the current service status in this manner.

In services provided by business systems, a single process consists of one or more sets of requests and responses. For example, in a mail service, each process, such as a login process or display of a list of emails, consists of multiple requests and responses. To monitor the status of each service process, ITSLM identifies the requests and responses that make up the process to be monitored among all requests and responses of the monitored service and monitors those requests and responses as a set.

When each service process is monitored, a set of requests and responses is identified based on the queries and cookie information contained in the URIs of the requests and responses.

Whether to monitor services by process is evaluated when the following types of processes occur:

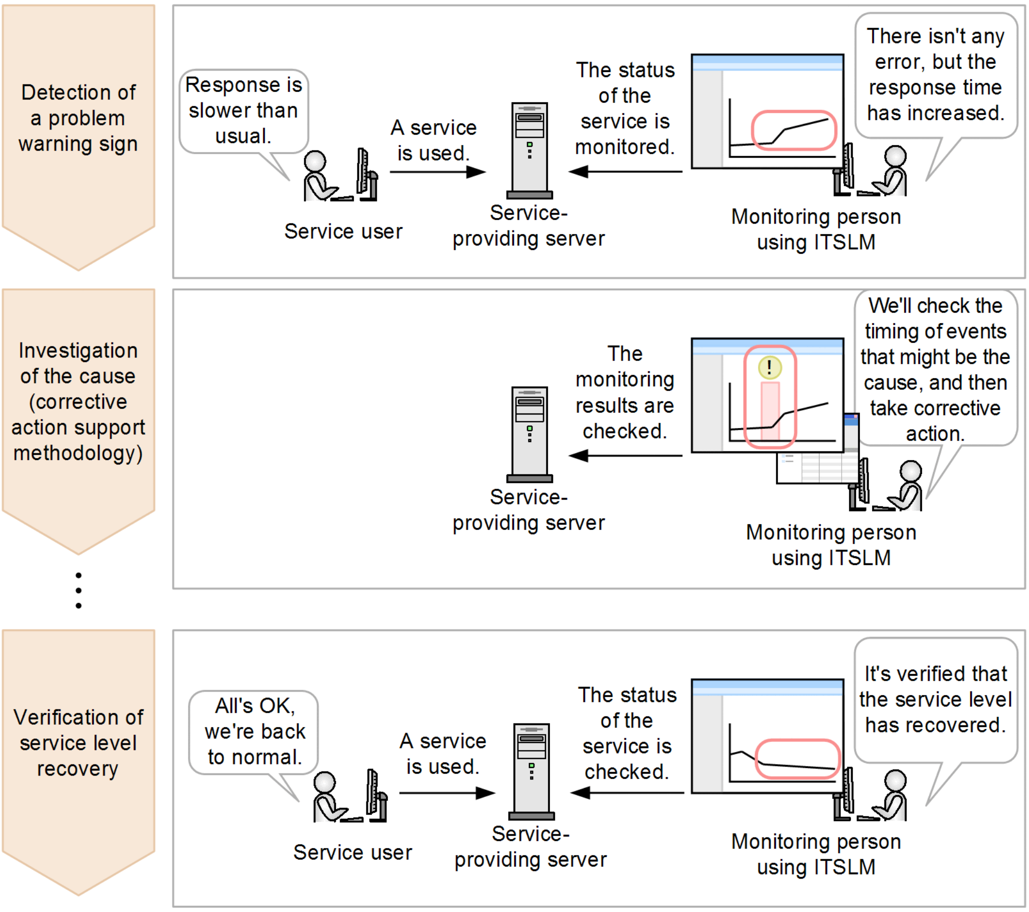
- Newly added processes
- Important processes in terms of system requirements
- Processes that are expected to generate a high workload
- Other processes that require special attention

Example of predictive error detection in the performance of a monitored service and the corrective action support methodology

This example detects an unusual service status that is a warning sign of an abnormality in the performance of a monitored service and takes an appropriate corrective action before an error materializes.

The following figure shows the general procedure for detecting a warning sign of an abnormality in the performance of a monitored service and taking corrective action.

Figure 1–5: General procedure for detecting a warning sign of an abnormality in the performance of a monitored service and taking corrective action


Detection of a problem warning sign
Response is slower than usual.
Service user
A service is used.
Service-providing server
The status of the service is monitored.
There isn't any error, but the response time has increased.
Monitoring person using ITSLM
Investigation of the cause (corrective action support methodology)
The monitoring results are checked.
Service-providing server
We'll check the timing of events that might be the cause, and then take corrective action.
Monitoring person using ITSLM
Verification of service level recovery
All's OK, we're back to normal.
Service user
A service is used.
Service-providing server
The status of the service is checked.
It's verified that the service level has recovered.
Monitoring person using ITSLM

First, use of ITSLM to monitor a service's status detects an increase in response time, which is a warning sign of an abnormality in service performance. Next, from ITSLM's past monitoring records, the timing of an event that might be the cause of the warning sign of an abnormality in service performance is checked. You can use the results of this check to respond to (handle) the detected event.

When ITSLM verifies that the service level has recovered after the cause was identified and you took corrective action, your handling of the abnormality in service performance at the stage of the early warning sign is complete.

ITSLM performs predictive error detection in the performance of a monitored service. It can also help you take corrective action. Because ITSLM enables you to take corrective action before a problem actually occurs in the service, you can improve the service users' sense of satisfaction.

For this example, an example of setting up the monitored items is explained in *3.3.1 Example of setup for predictive error detection in the performance of monitored services and the corrective action support methodology*, and an example of execution of monitoring is explained in *4.6.1 Example of execution for predictive error detection in the performance of monitored services and the corrective action support methodology*.

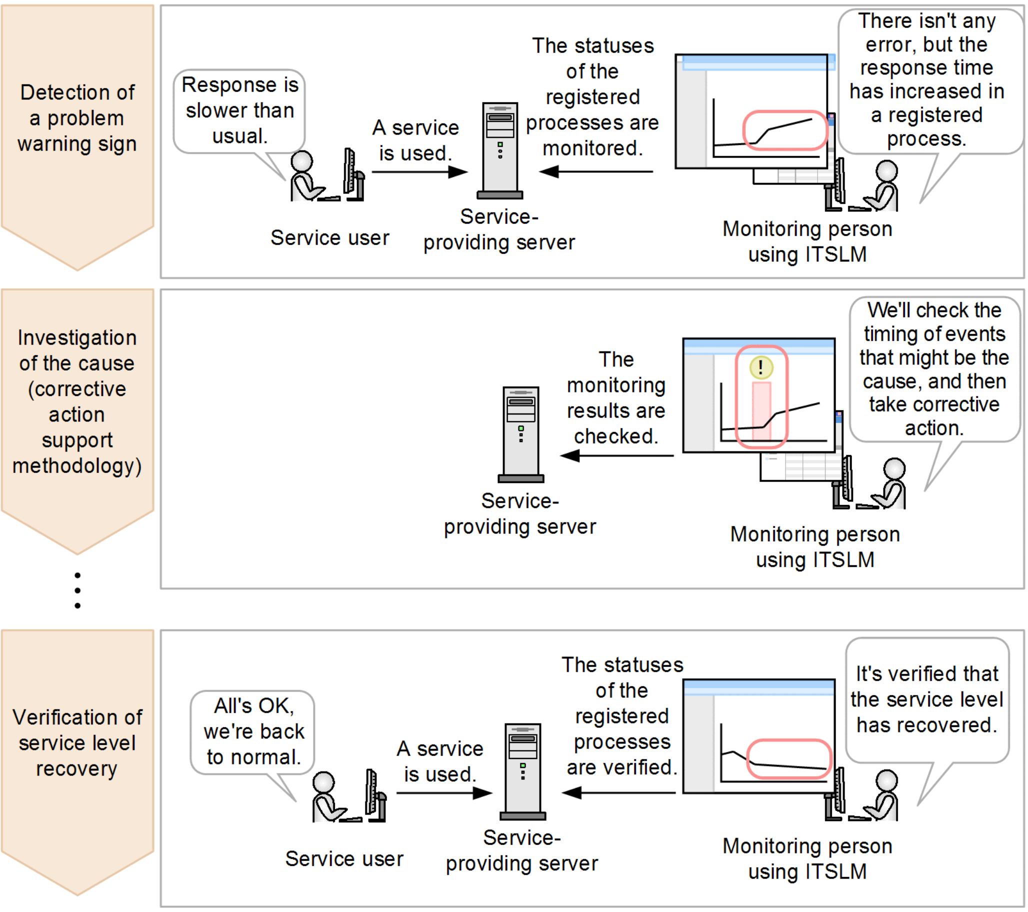
Example of predictive error detection in the performance of processes in a monitored service and the corrective action support methodology

This subsection explains an example of monitoring a new process added to a monitored service.

New functions have been added to a monitored service after upgrading. Because newly added processes are prone to errors, this example registers the new process into ITSLM and monitors it individually in addition to monitoring the entire service.

The following figure shows the general procedure for detecting a warning sign of an abnormality in the performance of a registered process of a monitored service and taking corrective action.

Figure 1–6: General procedure for detecting a warning sign of an abnormality in the performance of a process in a monitored service registered into ITSLM and taking corrective action


Detection of a problem warning sign
Response is slower than usual.
A service is used.
The statuses of the registered processes are monitored.
There isn't any error, but the response time has increased in a registered process.
Service user
Service-providing server
Monitoring person using ITSLM
Investigation of the cause (corrective action support methodology)
The monitoring results are checked.
We'll check the timing of events that might be the cause, and then take corrective action.
Service-providing server
Monitoring person using ITSLM
Verification of service level recovery
All's OK, we're back to normal.
A service is used.
The statuses of the registered processes are verified.
It's verified that the service level has recovered.
Service user
Service-providing server
Monitoring person using ITSLM

This example monitors the status of newly registered processes. First, ITSLM detects an increase in response time in a registered process, a warning sign of an abnormality in service performance for the process. Next, from ITSLM's past monitoring records, the timing of an event that might be the cause of the warning sign of an abnormality in service performance for the process is checked. You can use the results of this check to respond to (handle) the detected event.

When ITSLM verifies that the service level has recovered after the process resulting in the warning sign of the abnormality and the timing of the event were identified and you took an appropriate corrective action, your handling of the abnormality in service performance of the process at the stage of the early warning sign is complete.

ITSLM performs predictive error detection in the performance of each process of a monitored service. It can also assist you in taking an appropriate corrective action.

For this example, an example of setting up the monitored items is explained in *3.3.2 Example of setup for predictive error detection in the performance of processes in monitored services and the corrective action support methodology*, and an example of execution of monitoring is explained in *4.6.2 Example of execution for predictive error detection in the performance of processes in monitored services and the corrective action support methodology*.

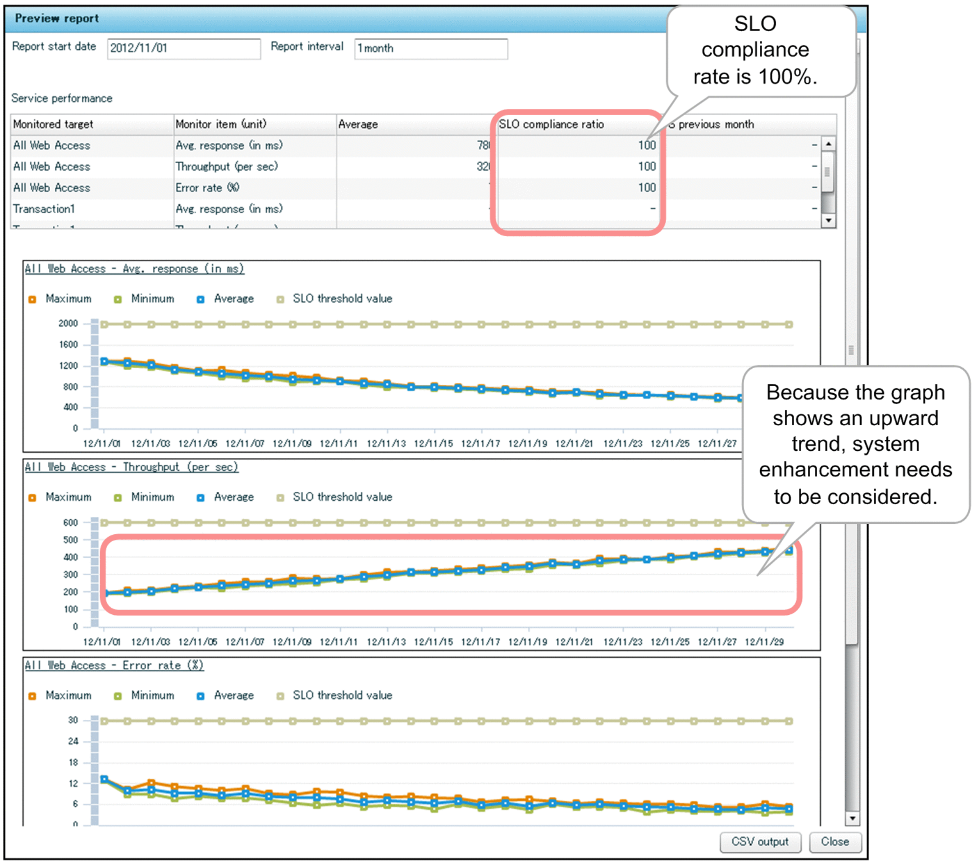
1.1.3 Supporting creation of reports required for periodic reporting

A service provider must check the quality of its services periodically, even if there are no abnormalities in service status. Especially when a service provider outsources the management and operation of its business systems to a data center and provides its services from the data center to its service users, the data center must be requested to report the service status periodically to the service provider in some form, such as reports.

If you use ITSLM, you can display service monitoring results for any specified period. You can select the items to be displayed as appropriate to the circumstances and you can save selected information as templates. You can also output monitoring results as CSV files. All this reduces the time required for performing periodic checking and creating reports, thereby achieving efficient service management and operation.

The following figure shows an example of a report displayed by ITSLM.

Figure 1–7: Example of a report displayed by ITSLM



Preview report

Report start date 2012/11/01 Report interval 1month

Service performance

Monitored target	Monitor item (unit)	Average	SLO compliance ratio	s previous month
All Web Access	Avg. response (in ms)	78	100	-
All Web Access	Throughput (per sec)	32	100	-
All Web Access	Error rate (%)	[illegible]	100	-
Transaction1	Avg. response (in ms)	[illegible]	-	-

For the services being monitored, this report displays the monitoring results for a period of one month, starting on November 1, 2012, for three items: the average response time, throughput, and error rate.

For example, from the table at the top, which displays the average value, the SLO compliance rate, and the previous month VS for each monitored item, you can conclude that the services were provided to users in November 2012 and that the service level was maintained because the SLO compliance rate was 100%. The change on one of the graphs (the graph that shows an upward trend) can be used to determine that whether the system needs to be enhanced.

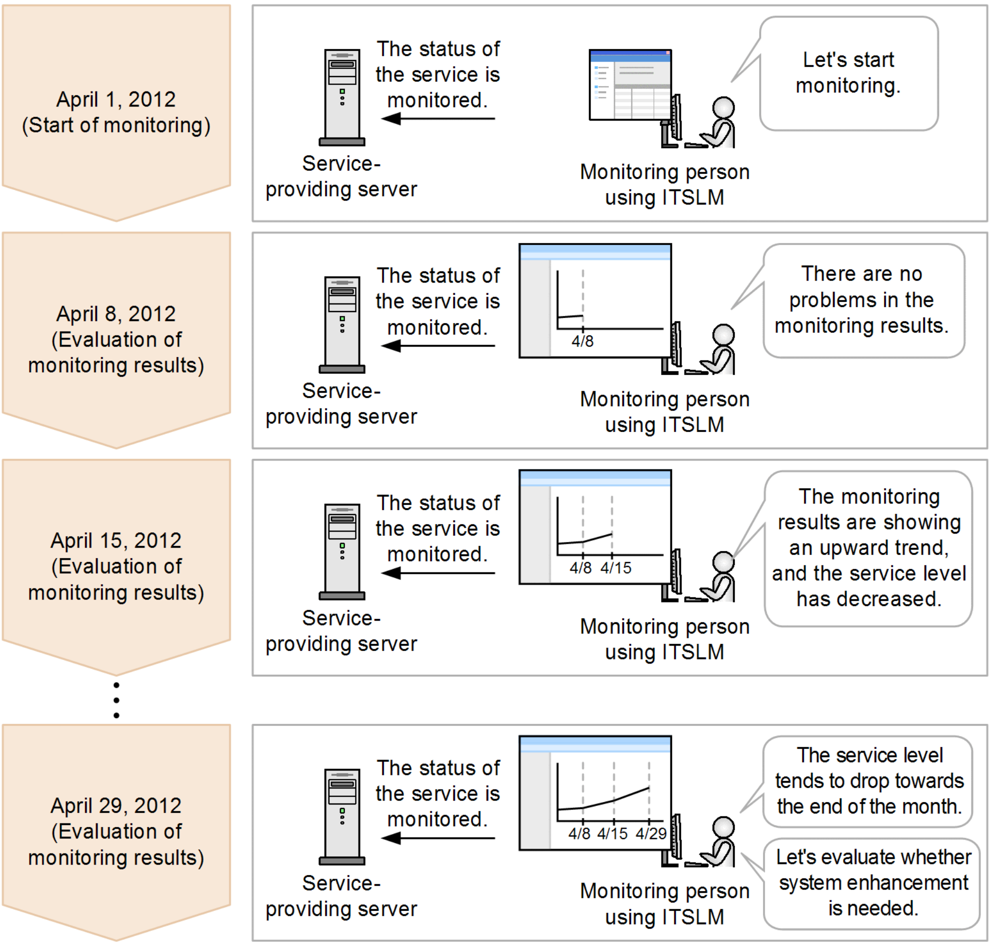
You can display reports by service and also by service process.

Example of periodic evaluation of monitored services

This subsection explains an example that evaluates the need for system enhancement by assessing periodically whether the service level is being maintained.

The following figure shows the general procedure for using ITSLM to check and evaluate the service level.

Figure 1–8: General procedure for using ITSLM to check and evaluate the service level


April 1, 2012
(Start of monitoring)
The status of the service is monitored.
Service-providing server
Monitoring person using ITSLM
Let's start monitoring.
April 8, 2012
(Evaluation of monitoring results)
The status of the service is monitored.
Service-providing server
4/8
Monitoring person using ITSLM
There are no problems in the monitoring results.
April 15, 2012
(Evaluation of monitoring results)
The status of the service is monitored.
Service-providing server
4/8 4/15
Monitoring person using ITSLM
The monitoring results are showing an upward trend, and the service level has decreased.
April 29, 2012
(Evaluation of monitoring results)
The status of the service is monitored.
Service-providing server
4/8 4/15 4/29
Monitoring person using ITSLM
The service level tends to drop towards the end of the month.
Let's evaluate whether system enhancement is needed.

On April 1, 2012, use of ITSLM to monitor service status began. Since then, the service level has been checked for any problems at the end of each week.

On April 8, 2012, no problems were seen, but a week later on April 15, 2012, monitoring detects a decrease in the service level, based on the trend shown on a graph of the monitoring results. On April 29, 2012, the last evaluation for the month, it becomes clear that the service level tends to drop toward the end of the month. As a result, the monitoring person who is using ITSLM evaluates whether some sort of system enhancement might be called for in order to increase the service users' sense of satisfaction.

As shown in this example, you can use ITSLM for periodic evaluation of service level and then use the monitoring results to improve the service users' sense of satisfaction.

For this example, an example of setting up the monitored items is explained in *3.3.4 Example of setup for periodic evaluation of the status of monitored services*, and an example of execution of monitoring is explained in *4.6.4 Example of execution for periodic evaluation of the status of monitored services*.

1.2 Linking with Performance Management to monitor service status (working with Performance Management)

ITSLM can monitor the status of hosts and middleware that provide monitored services and the availability of the monitored services. To achieve this, ITSLM must be linked with Performance Management. Linking with Performance Management is not required. We recommend that you evaluate your need to link with Performance Management, as necessary.

You can achieve the following monitoring by linking ITSLM with Performance Management:

- Monitoring the performance of hosts and middleware

  ITSLM acquires information collected by Performance Management's monitoring agents, thus enabling you to monitor the performance of hosts and middleware in an ITSLM window. Because ITSLM enables you to monitor the performance of hosts and middleware based on threshold values, if an unusual service status is detected, you can use the ITSLM window to check the status of the hosts and middleware during the period in question. Based on this information, you can investigate and determine whether the cause was in a host or middleware.

  This monitoring is supported when PFM - Agent or PFM - RM is used as the monitoring agent.

- Monitoring service availability

  By monitoring the availability of services, you can determine whether services are being provided without interruption. You can also obtain availability-related evaluation metrics (SLO) based on the monitored availability data and check the availability in an ITSLM window.

  This monitoring is supported when PFM - Agent for Service Response is used.

  Important note

  ITSLM does not support job monitoring.

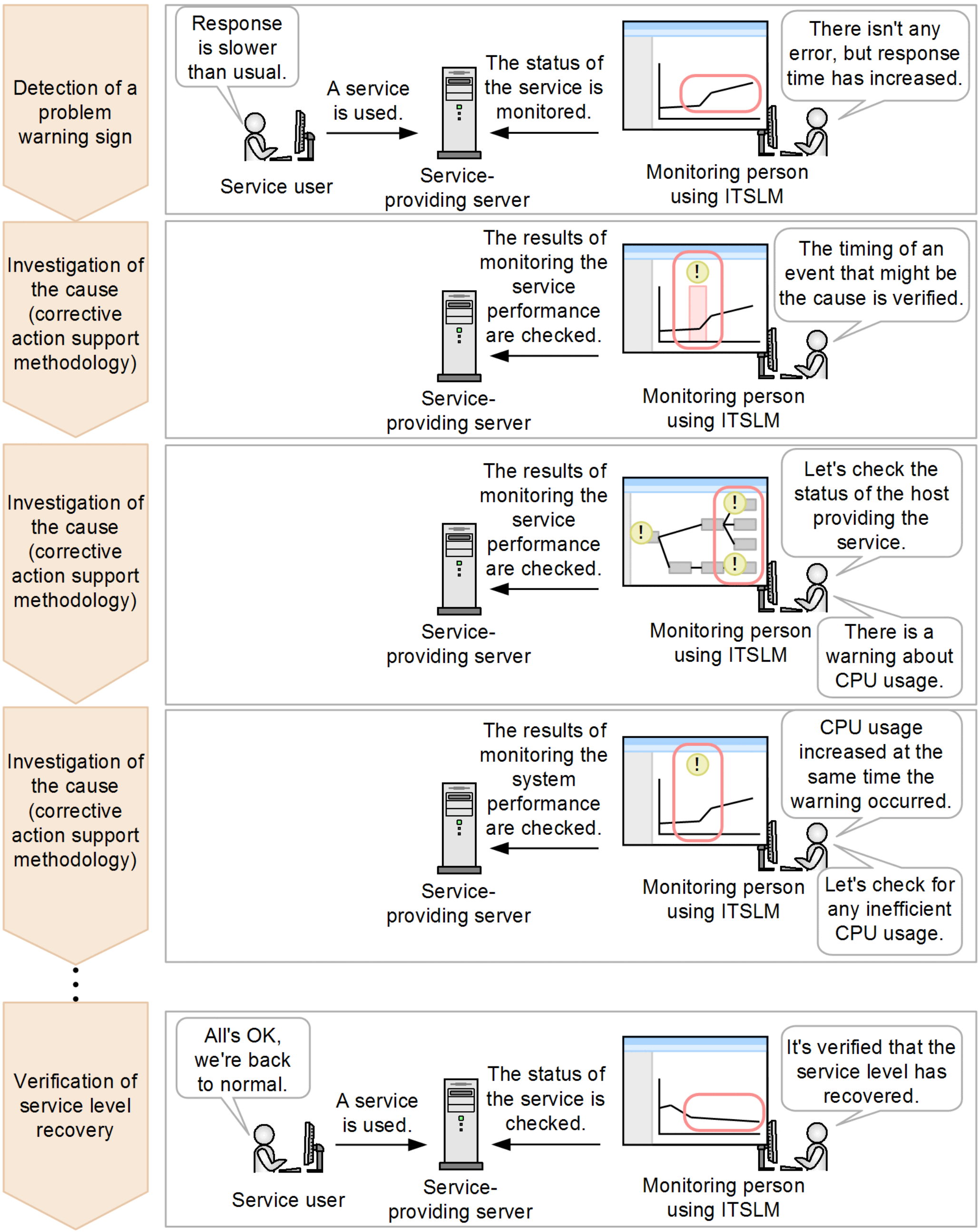
Example of predictive error detection in the performance of a monitored service and the investigative support methodology

This example uses the results obtained by monitoring hosts and middleware to determine the cause of a warning sign detected during monitoring of a service's performance.

This enterprise system has been using ITSLM to monitor service status. As the system has become increasingly complex, more and more time has been required to identify the causes of problems. Therefore, the current ITSLM monitoring system has been linked with Performance Management to monitor the status of hosts and middleware and to reduce the time required for identifying causes.

The following figure shows the general procedure for detecting a warning sign of an abnormality in the performance of a monitored service, and for taking an appropriate corrective action.

Figure 1–9: General procedure for detecting a warning sign of an abnormality in the performance of a monitored service, and for taking an appropriate corrective action by linking ITSLM and Performance Management


Detection of a problem warning sign
Response is slower than usual.
Service user
A service is used.
Service-providing server
The status of the service is monitored.
Monitoring person using ITSLM
There isn't any error, but response time has increased.
Investigation of the cause (corrective action support methodology)
The results of monitoring the service performance are checked.
Service-providing server
Monitoring person using ITSLM
The timing of an event that might be the cause is verified.
Investigation of the cause (corrective action support methodology)
The results of monitoring the service performance are checked.
Service-providing server
Monitoring person using ITSLM
Let's check the status of the host providing the service.
There is a warning about CPU usage.
Investigation of the cause (corrective action support methodology)
The results of monitoring the system performance are checked.
Service-providing server
Monitoring person using ITSLM
CPU usage increased at the same time the warning occurred.
Let's check for any inefficient CPU usage.
Verification of service level recovery
All's OK, we're back to normal.
Service user
A service is used.
Service-providing server
The status of the service is checked.
Monitoring person using ITSLM
It's verified that the service level has recovered.

First, use of ITSLM to monitor a service's status detects an increase in response time, which is a warning sign of an abnormality in service performance. Next, from ITSLM's past monitoring records, the timing of an event that might be the cause of the warning sign of an abnormality in service performance is checked. Then, the example checks the results of monitoring the host and middleware providing that service for any warning. If there is a warning, the example investigates further to determine the cause because that warning might have something to do with the change in service performance. For example, if CPU usage increased considerably at the time the warning sign of an abnormality in service performance was detected, the corresponding host's middleware information must be examined for any inefficient CPU usage in order to identify the cause.

If an appropriate corrective action was taken and ITSLM shows that the service level has recovered, the corrective action needed at the stage of the warning sign of an abnormality in the service performance is complete.

For this example, an example of setting up the monitored items is explained in *3.3.3 Example of setup for predictive error detection in the performance of systems running monitored services and the corrective action support* *methodology (working with Performance Management)*, and an example of execution of monitoring is explained in *4.6.3 Example of execution for predictive error detection in the performance of systems running monitored services and the corrective action support methodology (working with Performance Management)*.

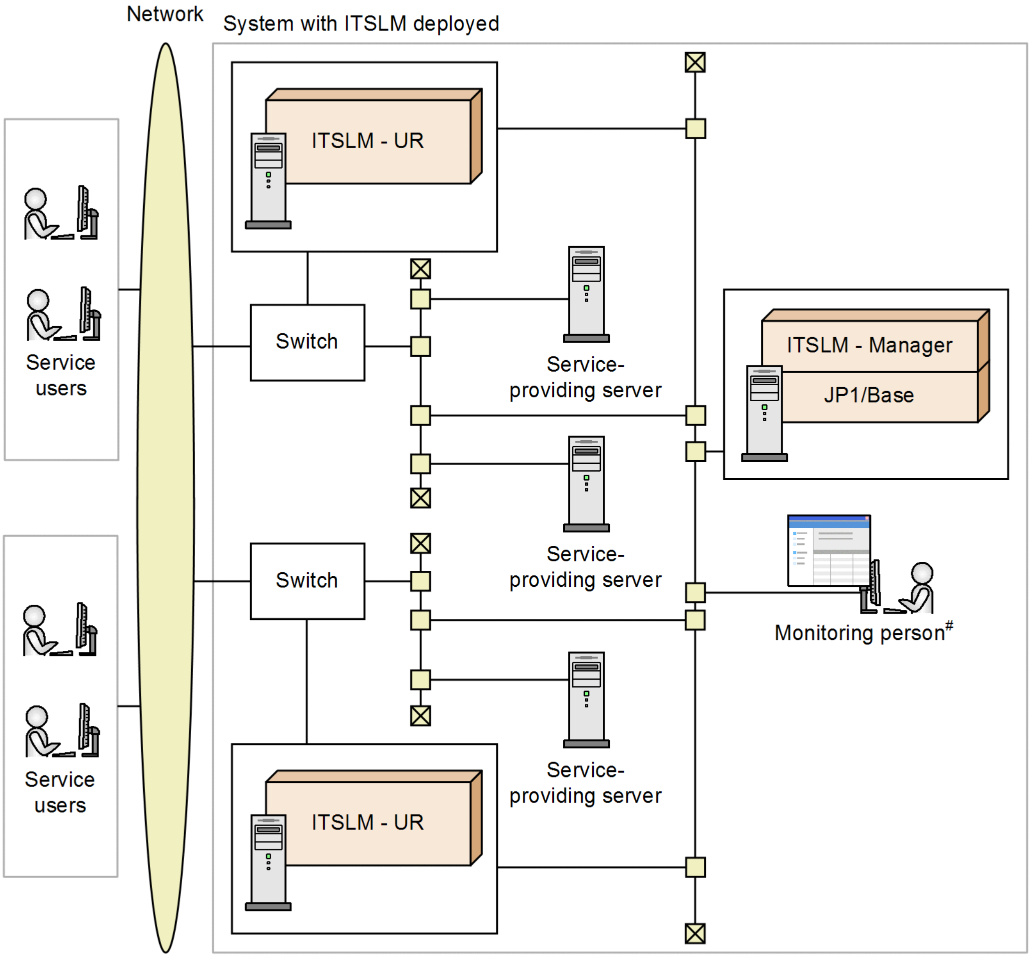
1.3 ITSLM system configuration

ITSLM consists of *ITSLM - UR*, which collects HTTP packets exchanged between service providing servers and users, and *ITSLM - Manager*, which monitors the service status based on the HTTP packets collected by ITSLM - UR.

A system configuration intended mainly for monitoring service status (service performance) is called a *service monitoring configuration*. The service monitoring configurations include a configuration for monitoring only service performance and a configuration for monitoring both service performance and system performance by linking ITSLM with Performance Management.

The following figure shows the system configuration for using ITSLM to monitor service performance only.

Figure 1–10: System configuration for monitoring service performance only



#

Internet Explorer and Flash Player must be installed on the monitoring person's computer.

Of the components shown in the figure, the roles of those that require explanation are described below.

ITSLM - Manager

Aggregates and analyzes the HTTP packets collected by ITSLM - UR and monitors the service status. The monitoring results can be displayed on the monitoring person's computer. They can also be saved to a file and used for creating reports.

Multiple ITSLM - URs can be connected to a single ITSLM - Manager.

ITSLM - UR

Collects HTTP packets of requests and responses that are exchanged between service users and service providing servers via switches. An ITSLM - UR is provided for each switch.

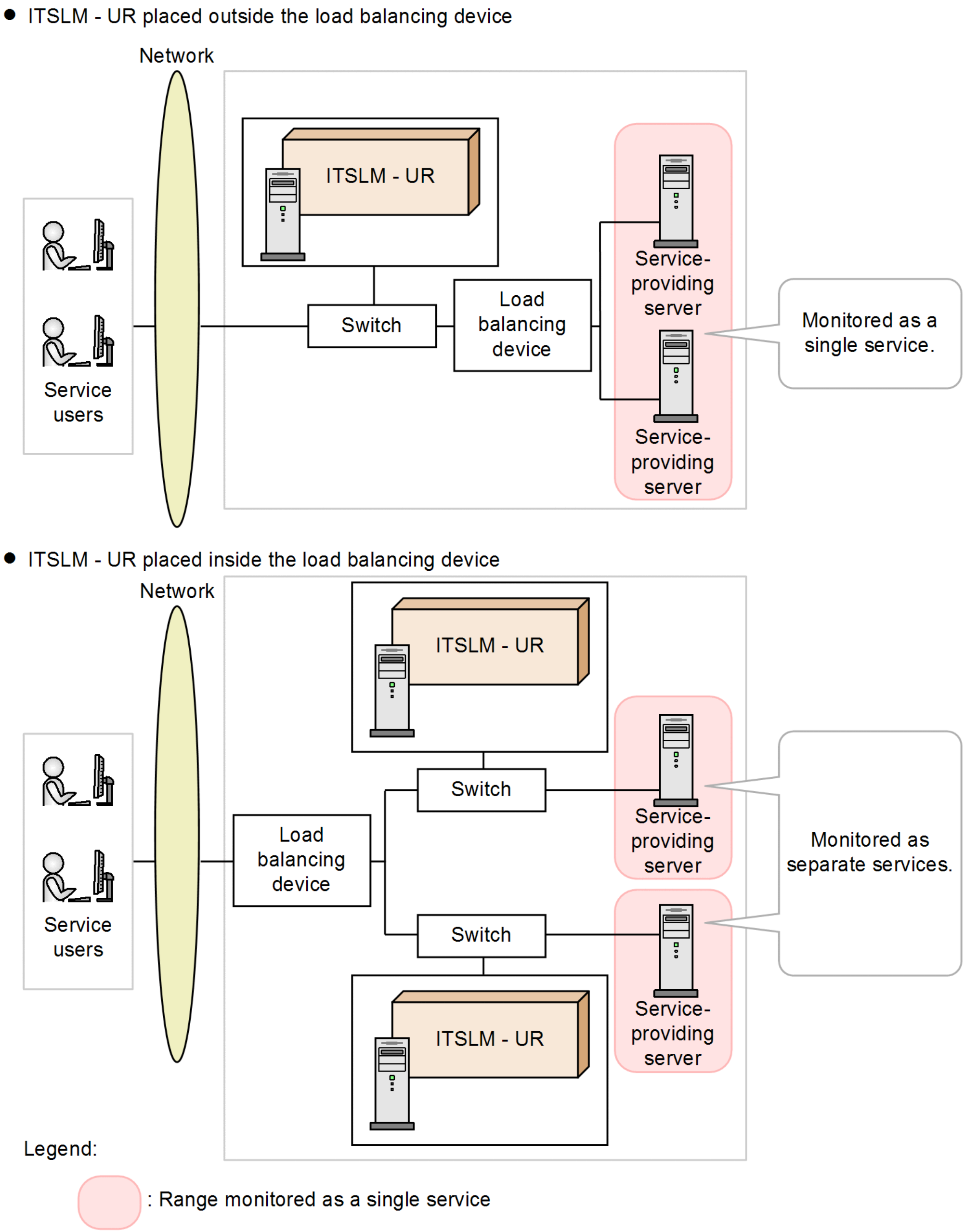
A single ITSLM - UR can monitor multiple services.

To reduce the network load, we recommend that you provide separate interfaces to connect to switches and to ITSLM - Manager, as shown in the system configuration here.

Notes

- ITSLM - UR uses two ports, one for monitoring services and one for communicating with ITSLM - Manager. If the mirrored ports do not support TCP/IP communications due to switch specifications, the port for monitoring services cannot be shared for communicating with ITSLM - Manager. In such a case, provide separate network interface cards, one for connecting switches and one for connecting ITSLM - Manager.
- If a load balancing device is used, the range monitored by an ITSLM - UR depends on its location within the system configuration. ITSLM placed outside the load balancing device monitors the services distributed by the load balancing device as a single service. ITSLM - UR placed inside the load balancing device within the system configuration monitors the services distributed by the load balancing device as separate services. The following figure shows the placement of ITSLM - UR and its monitoring range when a load balancing device is used.

Figure 1–11: Placement of ITSLM - UR and its monitoring range when a load balancing device is used



JP1/Base

Manages the users (JP1 users) who access ITSLM - Manager as the authentication server and performs monitoring.

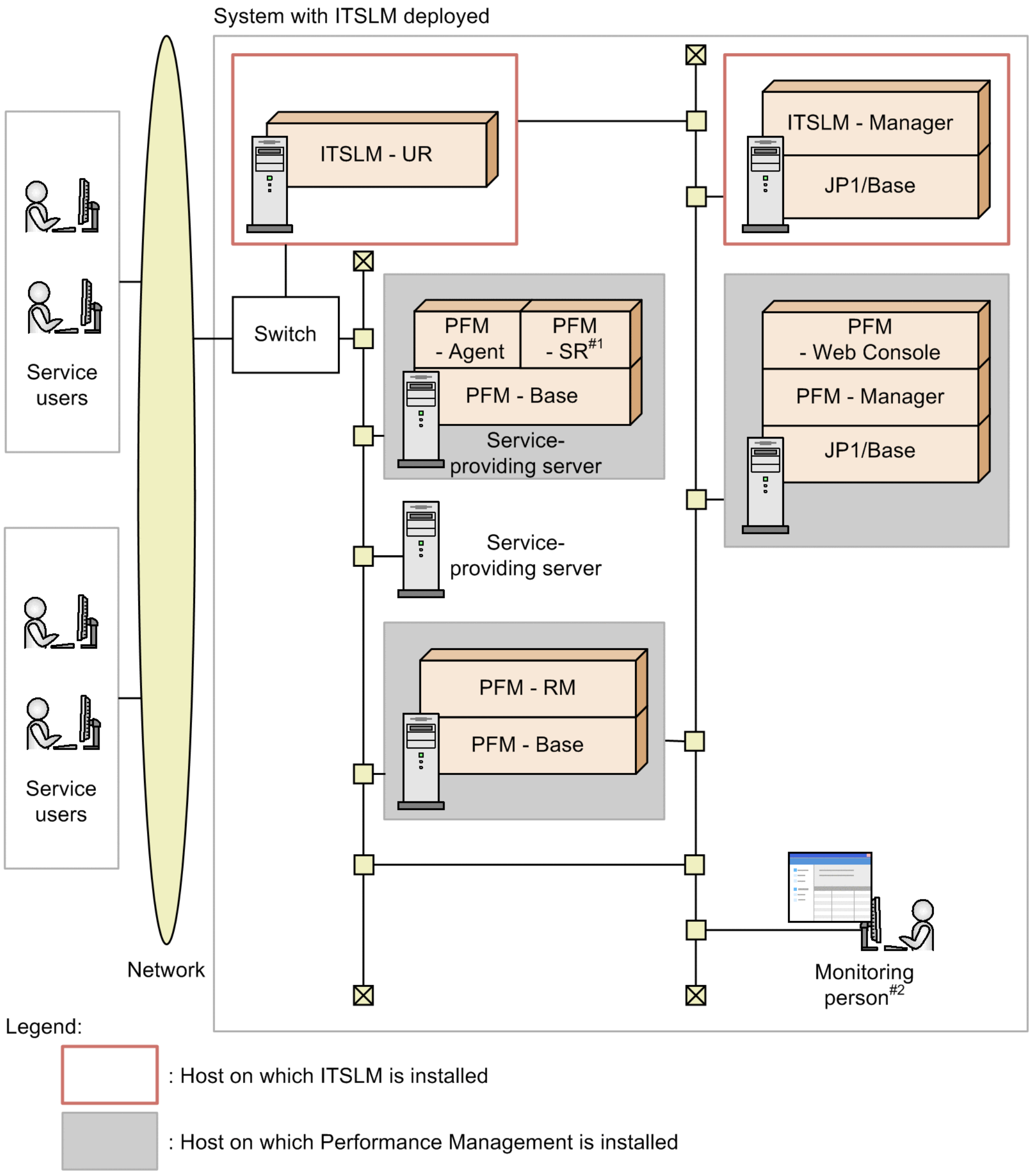
Switch

This is a network switch placed between external and internal networks. This network switch must have a port mirroring function.

If you link ITSLM with Performance Management to monitor system performance and availability, you must have Performance Management-related products.

The following shows an example of a system configuration when ITSLM is linked with Performance Management.

Figure 1–12: Example of a system configuration when ITSLM is linked with Performance Management



#1: In the figure, *PFM - SR* is an abbreviation for *PFM - Agent for Service Response*.

#2: Internet Explorer and Flash Player must be installed on the monitoring person's computer.

Of the components shown in the figure, the roles of the Performance Management products are explained below.

PFM - Base

Sends the data collected by PFM - Agent, PFM - Agent for Service Response, or PFM - RM to PFM - Manager and ITSLM - Manager.

PFM - Manager

Sends configuration information to ITSLM - Manager as requested by ITSLM - Manager. PFM - Manager also provides the functions of PFM - Base. If PFM - Agent, PFM - Agent for Service Response, and/or PFM - RM are running on the same host, data collected by these products is sent to ITSLM - Manager.

PFM - Agent

Provides functionality as a monitoring agent and monitors the system performance of a monitored host. PFM - Agent is installed on the monitored host.

PFM - RM

Provides functionality as monitoring agent and monitors the system performance of a monitored host. PFM - RM is installed on a host that is not the monitored host.

PFM - Agent for Service Response

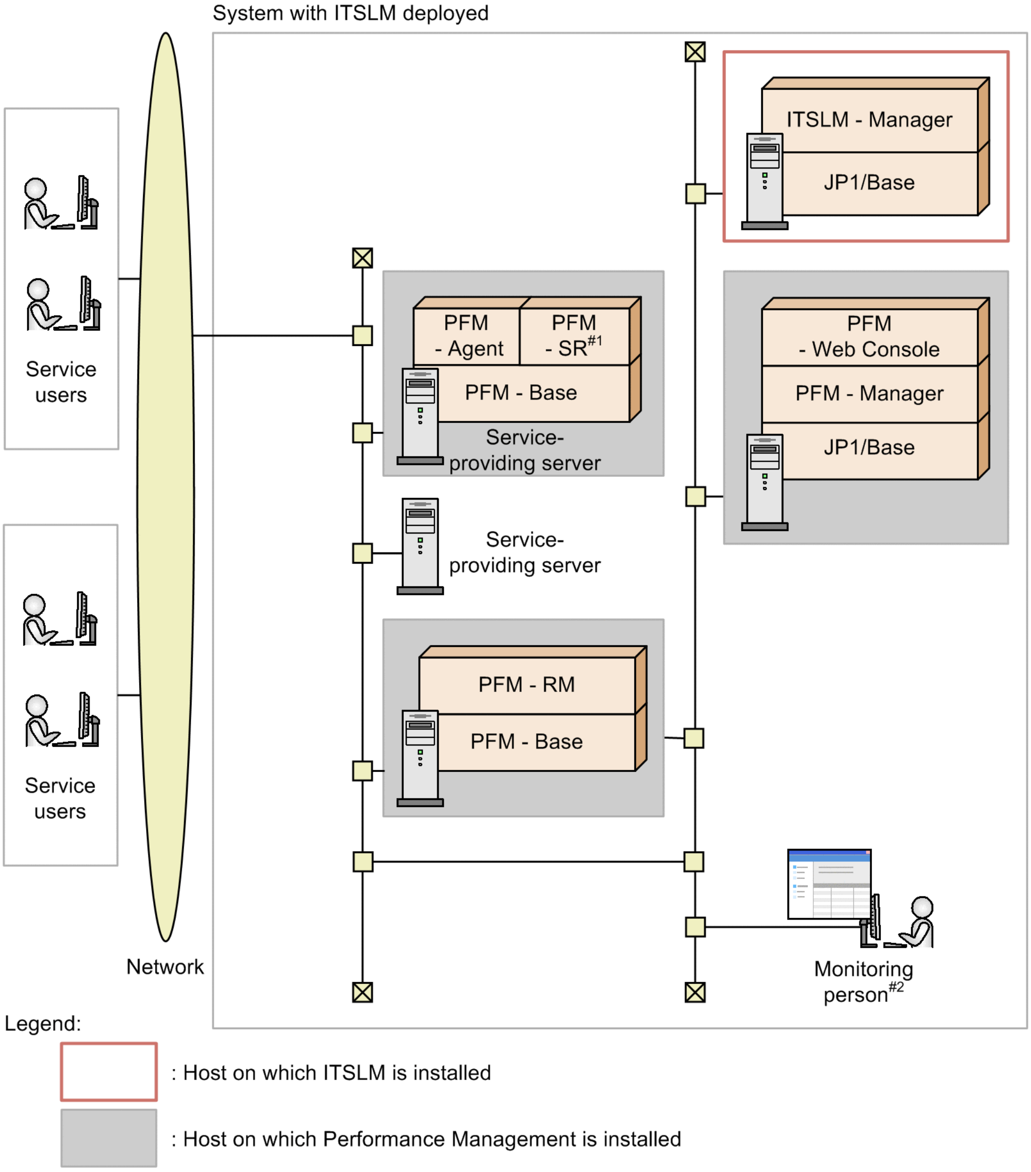
Provides functionality as a monitoring agent and collects operation data required for monitoring the availability of a monitored host.

PFM - Web Console

Provides windows for researching detailed system performance by using the Performance Management functions. When a warning sign of an error in monitored services is detected and the host in question is identified, PFM - Web Console is started from an ITSLM window.

A system configuration intended mainly for monitoring system performance is called a *system monitoring configuration*. Such a configuration is used to monitor system performance only. The following figure shows an example of a system monitoring configuration.

Figure 1–13: Example of a system configuration for monitoring only system performance



#1: In the figure, *PFM - SR* is an abbreviation for *PFM - Agent for Service Response*.

#2: Internet Explorer and Flash Player must be installed on the monitoring person's computer.

ITSLM - Manager and ITSLM - UR can be run in cluster systems. For the system configuration and components required when ITSLM - UR is run in a cluster system, see *6.1.2 ITSLM system configuration in a cluster system*.

1.4 Flow of a monitoring job and the timing of using ITSLM

This section explains by way of examples when ITSLM can be used in the flow of a monitoring job.

1.4.1 Assumed personnel

ITSLM assumes the following personnel and their responsibilities:

- Person who monitors all services

  This is the person in overall charge of monitoring. This person's responsibilities include monitoring setup, monitoring of monitored services, and periodic reporting of service status. This person can monitor all services. ITSLM assumes that this person is an expert with experience in monitoring.

  Of the tasks involved in *Check* in the PDCA cycle, this person is responsible for monitoring setup, monitoring, and periodic evaluation. In the event of a problem in ITSLM, this person checks the event and takes an appropriate corrective action. If the problem cannot be resolved, this person collects necessary data and contacts the maintenance service provider for the monitored service or the system administrator.

  The *person who monitors all services* is also responsible for the tasks performed by the *specific service monitors*.

- Monitor

  This person is a member of the monitoring staff who monitors designated services. A monitor receives instructions from the person who monitors all services and monitors such designated services as all newly installed services and services that have just been recovered. Of the tasks involved in *Check* in the PDCA cycle, a monitor is responsible for monitoring.

  A monitor performs monitoring according to instructions and past cases, not necessarily just on the basis of the monitor's own experience. If a monitor encounters a problem the monitor is not familiar with or discovers a problem warning sign while monitoring monitored services, it is the monitor's responsibility to report the matter to the *specific service monitor* for the applicable service.

- Specific service monitor

  This is a person who monitors a specific service. ITSLM assumes that this person is less experienced than the person who monitors all services.

  Of the tasks involved in *Check* in the PDCA cycle, a specific service monitor is responsible for monitoring.

  When notified by a monitor that a problem needs to be handled or a problem warning sign concerning the specific service monitor's service has been detected, the specific service monitor checks the nature of the event. If corrective action is needed, the specific service monitor notifies the person who monitors all services.

- Maintenance service provider for a monitored service

  This is a person who handles problems with the programs that constitute a monitored service. This person must be familiar with the monitored service (such as a developer of the monitored service).

- System operator

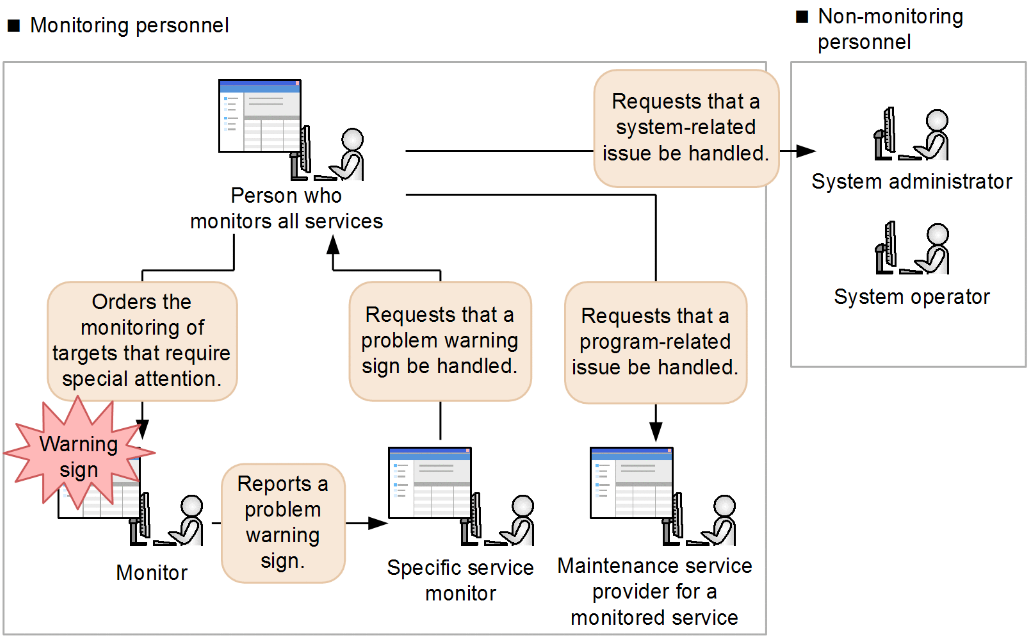
  This person runs IT equipment and networks and installs and sets up the products, including ITSLM, that are deployed in the company. This person is also a designer of the monitoring system that uses ITSLM and is responsible for monitoring setup and periodic evaluation of the tasks involved in *Check* in the PDCA cycle.

- System administrator

  This person manages the company's entire system and handles problems in ITSLM when notified by the person who monitors all services.

The following figure shows the relationships among these personnel.

Figure 1–14: Relationships among ITSLM personnel


■ Monitoring personnel
■ Non-monitoring personnel
Person who monitors all services
Requests that a system-related issue be handled.
System administrator
System operator
Orders the monitoring of targets that require special attention.
Requests that a problem warning sign be handled.
Requests that a program-related issue be handled.
Warning sign
Reports a problem warning sign.
Monitor
Specific service monitor
Maintenance service provider for a monitored service

Reference note

You must grant to the monitoring personnel JP1 permission levels that are appropriate to their ITSLM operation permissions. This manual assumes that the following permissions are granted to the individual personnel:

No.	Person	Assumed JP1 permission level
1	Person who monitors all services	`JP1_ITSLM_Admin`
2	Monitor	`JP1_ITSLM_User`
3	Specific service monitor	`JP1_ITSLM_User`
4	Maintenance service provider for a monitored service	`JP1_ITSLM_User`

For details about setting the operation permissions, see *5.2.3 Specifying operation permissions for each JP1 user*.

1.4.2 General procedure for detecting problem warning signs and the timing of using ITSLM

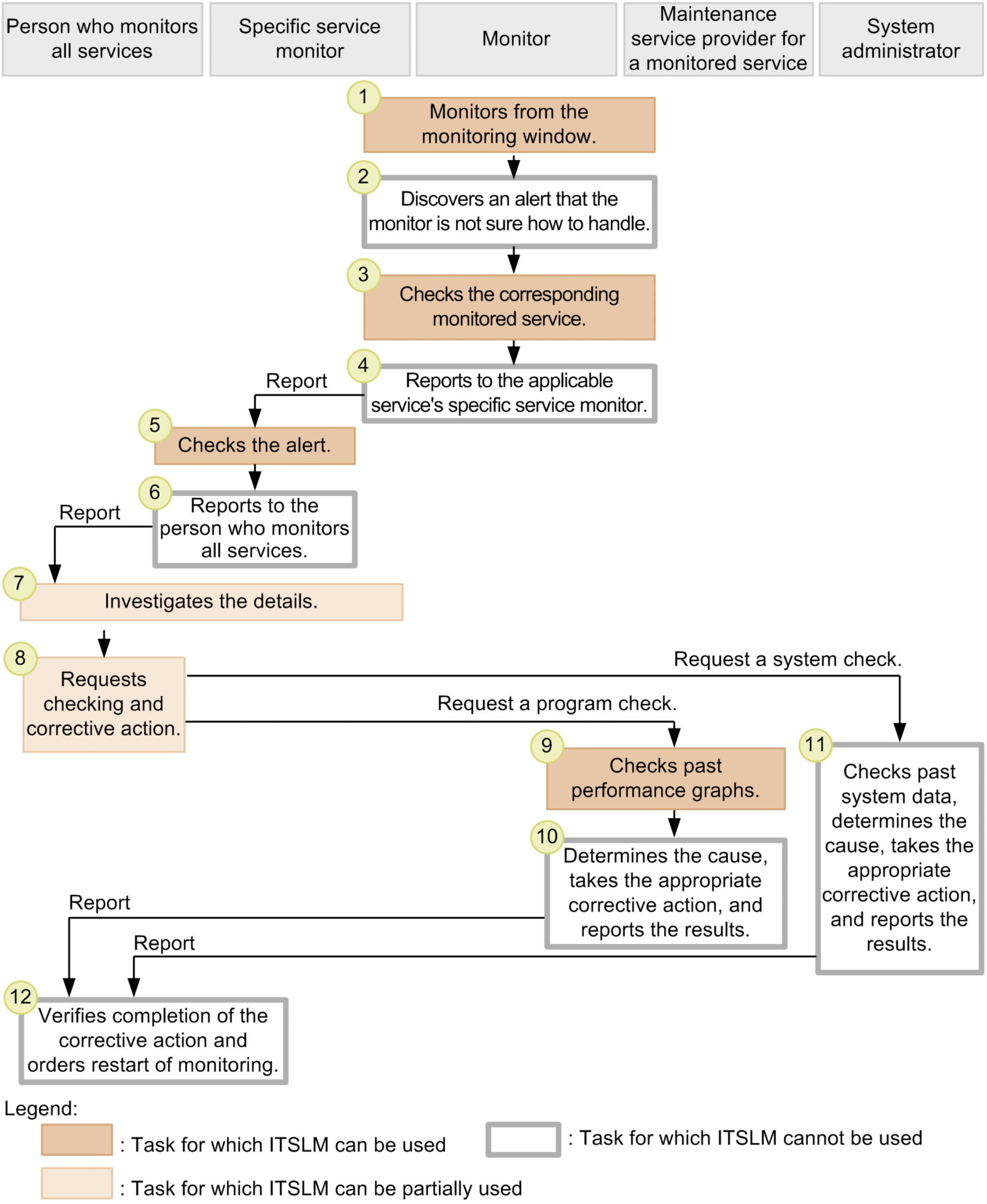
This subsection explains an example of the monitoring task procedure for detecting problem warning signs and when ITSLM can be used.

The following provides an overview of the task:

- A monitor discovers a problem warning sign and contacts the service's specific service monitor.
- The specific service monitor checks the situation and reports to the person who monitors all services and requests handling of the event.
- The person who monitors all services handles the warning sign in collaboration with the maintenance service provider for the monitored service or the system administrator.

The following shows an example procedure for detecting a problem warning sign.

Figure 1–15: Example procedure for detecting a problem warning sign


Person who monitors all services
Specific service monitor
Monitor
Maintenance service provider for a monitored service
System administrator
1
Monitors from the monitoring window.
2
Discovers an alert that the monitor is not sure how to handle.
3
Checks the corresponding monitored service.
4
Reports to the applicable service's specific service monitor.
Report
5
Checks the alert.
6
Reports to the person who monitors all services.
Report
7
Investigates the details.
8
Requests checking and corrective action.
Request a system check.
Request a program check.
9
Checks past performance graphs.
10
Determines the cause, takes the appropriate corrective action, and reports the results.
11
Checks past system data, determines the cause, takes the appropriate corrective action, and reports the results.
Report
Report
12
Verifies completion of the corrective action and orders restart of monitoring.
Legend:
: Task for which ITSLM can be used
: Task for which ITSLM cannot be used
: Task for which ITSLM can be partially used

The table below explains the flow of tasks shown in the figure. For the tasks for which ITSLM can be used, the section in which the task is explained is shown.

Table 1–1: Flow of tasks for detecting a problem warning sign and corresponding sections

No.	Task	What you can do with ITSLM	Section
1	The monitor uses ITSLM to monitor designated monitored services as instructed by the person who monitors all services. If an error or warning occurs during monitoring, the monitor takes an appropriate corrective action, if possible.	In the Home window, you can check the statuses of all monitored services that you are in charge of. Monitored services resulting in an error or warning are displayed in **Caution service**. You can view events that have been issued for services requiring attention in **Events in the last 7 days**.	*4.3.1*
2	The monitor detects an error or warning that the monitor is not sure how to handle using ITSLM.		

No.	Task	What you can do with ITSLM	Section
3	The monitor uses ITSLM to identify the monitored service resulting in the error or warning.	In the Home window, you can check the statuses of all monitored services that you are in charge of. Monitored services resulting in an error or warning are displayed in **Caution service**. You can view events that have been issued for services requiring attention in **Events in the last 7 days**.	*4.3.1*
4	The monitor notifies the specific service monitor about the error or warning by means such as telephone.	--	--
5	The notified specific service monitor uses ITSLM to verify the error or warning.	You can identify the corresponding error or warning displayed in the Home window based on such information as detection date and time, and view the details by displaying the Troubleshoot window from the **Details** column.	*4.4.1*
6	The specific service monitor reports the error or warning verification results to the person who monitors all services.	--	--
7	The person who monitors all services and the specific service monitor both use ITSLM to investigate past errors and warnings to determine the cause of the error or warning. They also check the operation logs before and after the past errors or warnings as well as the product logs and traces.	In the Troubleshoot window, you can check past service performance and identify the timing of the error or warning.	*4.3.2* *4.4.1*
8	The person who monitors all services requests verification from the maintenance service provider for the monitored service or the system administrator based on the results of the investigation of whether the cause is in the system or program.	If ITSLM is linked with Performance Management, you can display configuration information in the Troubleshoot window and locate the host providing the monitored service. You can also check system performance related to that host for any problem. This helps you determine whether the error or warning needs to be reported to the system administrator for verification.	*4.3.2* *4.4.1*
9	The maintenance service provider for the monitored service uses ITSLM to check past data, such as performance charts, to investigate the timing of warning signs and events that are likely related.	In the Troubleshoot window, you can check the past service performance and verify the status of the service and the system's performance when the error or warning occurred.	*4.3.2* *4.4.1*
10	If the cause has been determined, the maintenance service provider for the monitored service takes an appropriate corrective action. This person then reports the results to the person who monitors all services.	--	--
11	The system administrator checks past data related to the system. If Performance Management is deployed, its functions can be used for this check. If the cause has been determined, the system administrator takes an appropriate corrective action and reports the results to the person who monitors all services.	--	--
12	Upon receiving the results, the person who monitors all services verifies that the action has been completed. This person then orders the monitor to restart monitoring and also tells the	--	--

No.	Task	What you can do with ITSLM	Section
12	monitor how to handle a reoccurrence of the same error or warning.	--	--

Legend:

--: Not applicable

1.5 Organization of this manual and its relationship to the expected tasks

The following table describes the organization of this manual.

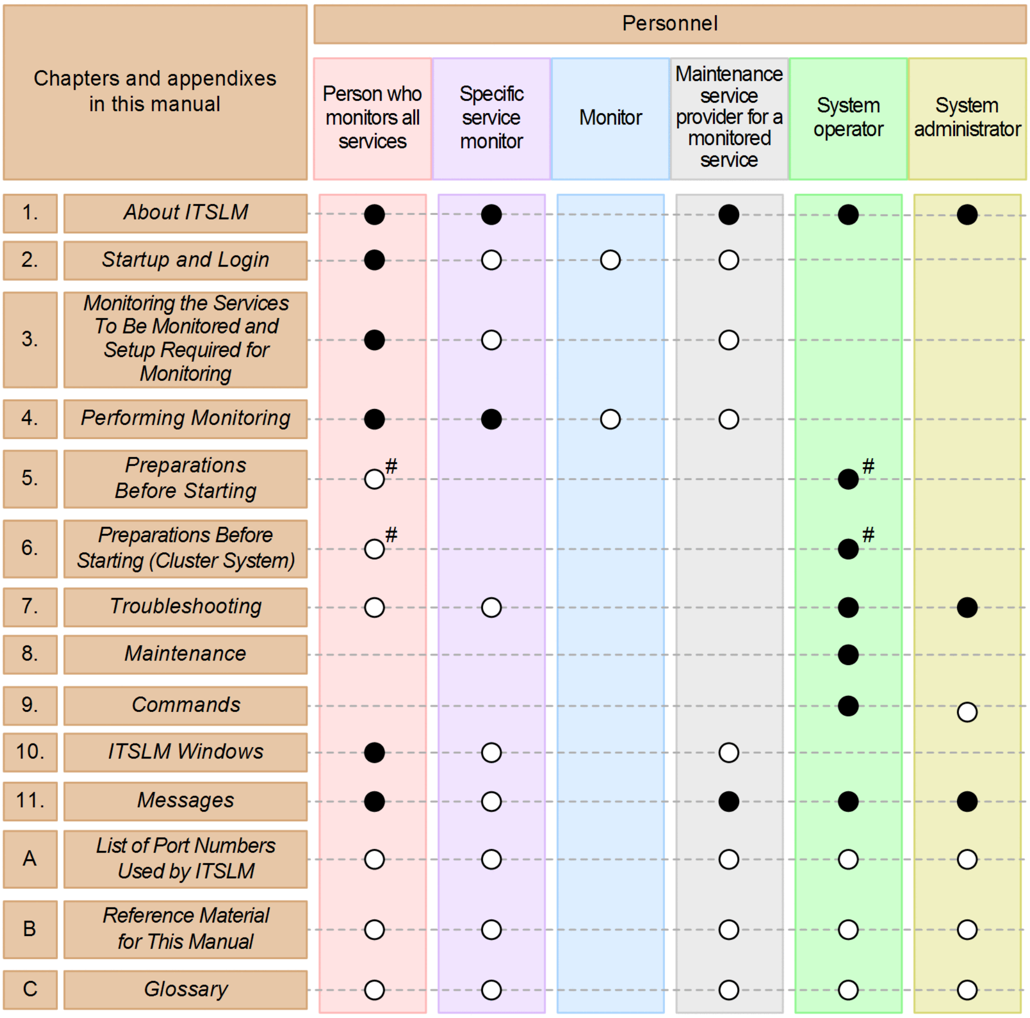
Table 1–2: Organization of this manual

Chapter or appendix	Contents
Chapter 1. About ITSLM	Provides an overview of ITSLM and explains the linkage with Performance Management for monitoring the status of hosts and middleware, the system configuration, the flow of monitoring jobs and the tasks that can be achieved by using ITSLM, and the relationship between the organization of this manual and the expected tasks.
Chapter 2. Startup and Login	Explains how to start and terminate ITSLM, how to log in and log out, and provides notes about the operations subsequent to login.
Chapter 3. Monitoring the Services to Be Monitored and Setup Required for Monitoring	Explains the different types of monitoring that can be achieved by using ITSLM. This chapter also explains how to register the services to be monitored and how to set up monitoring items for the services that are to be monitored.
Chapter 4. Performing Monitoring	Provides an overview of using ITSLM for monitoring and explains execution of monitoring. Execution of monitoring includes starting and stopping monitoring, monitoring the status of monitored services, the investigative support methodology for determining the cause when errors or warnings in monitored services are displayed, and creation of reports used for periodic reporting.
Chapter 5. Preparations Before Starting	Explains the preparations before starting ITSLM, including installation, setup, and user settings. This chapter also explains optional preparations, such as linking with JP1/IM to report monitoring results by a means such as email, linking with Performance Management to monitor hosts and middleware providing services, and editing system definition files (`jp1itslm.properties` or `jp1itslmur.properties`) to change ITSLM operations.
Chapter 6. Preparations Before Starting (Cluster System)	Explains the preparations before starting ITSLM in a cluster system, including installation, setup, and user settings. This chapter also explains optional preparations, such as linking with JP1/IM to report monitoring results by a means such as email, linking with Performance Management to monitor hosts and middleware providing services, and how to migrate to a cluster system.
Chapter 7. Troubleshooting	Explains how to troubleshoot problems with ITSLM.
Chapter 8. Maintenance	Explains ITSLM maintenance tasks, including backing up and restoring ITSLM definition files (system definition files and system configuration properties files) and databases, as well as migrating definition information and databases when computers are replaced.
Chapter 9. Commands	Explains the syntax of the ITSLM commands.
Chapter 10. ITSLM Windows	Explains the ITSLM windows.
Chapter 11. Messages	Explains the messages that are issued by ITSLM.
Appendix A. List of Port Numbers Used by ITSLM	Provides a list of the port numbers used in ITSLM.
Appendix B. ITSLM Communication	Explains the port numbers used in ITSLM communication and the direction in which data passes through a firewall.
Appendix C. Version Changes	Explains the changes in each version.
Appendix D. Reference Material for This Manual	Provides reference material for this manual.
Appendix E. Glossary	Defines terms used in this manual.

The tasks when ITSLM is used to manage the service level are broken down by the person in charge.

This manual is organized in such a manner that each person involved in monitoring can read the chapters appropriate to that person's tasks. The following figure shows the correspondence between chapters and the personnel described in *1.4.1 Assumed personnel*.

Figure 1–16: Correspondence between chapters in the manual and assumed personnel



Chapters and appendixes in this manual		Personnel					
		Person who monitors all services	Specific service monitor	Monitor	Maintenance service provider for a monitored service	System operator	System administrator
1.	*About ITSLM*	●	●		●	●	●
2.	*Startup and Login*	●	○	○	○		
3.	*Monitoring the Services To Be Monitored and Setup Required for Monitoring*	●	○		○		
4.	*Performing Monitoring*	●	●	○	○		
5.	*Preparations Before Starting*	○#				●#	
6.	*Preparations Before Starting (Cluster System)*	○#				●#	
7.	*Troubleshooting*	○	○			●	●
8.	*Maintenance*					●	
9.	*Commands*					●	○
10.	*ITSLM Windows*	●	○		○		
11.	*Messages*	●	○		●	●	●
A	*List of Port Numbers Used by ITSLM*	○	○		○	○	○
B	*Reference Material for This Manual*	○	○		○	○	○
C	*Glossary*	○	○		○	○	○

Legend:

●: See the corresponding chapter.

○: See the corresponding character or appendix as needed.

#: See either Chapter *5* or *6*, as appropriate to your environment.

Reference note

We recommend that a person who will serve both as the person who monitors all services and as a system operator read the chapters in this manual in the following order when ITSLM is deployed:

For a non-cluster system:

1. *1. About ITSLM*
2. *5. Preparations Before Starting*
3. *2. Startup and Login*

4. *3. Monitoring the Services to Be Monitored and Setup Required for Monitoring*
5. *4. Performing Monitoring*

For a cluster system:

1. *1. About ITSLM*
2. *6. Preparations Before Starting (Cluster System)*
3. *2. Startup and Login*
4. *3. Monitoring the Services to Be Monitored and Setup Required for Monitoring*
5. *4. Performing Monitoring*

2 Startup and Login

This chapter explains how to start and terminate ITSLM, how to log in and log out, and provides notes about the operations subsequent to login.

Read this chapter after you have finished installing ITSLM. For details about installing ITSLM, see *5. Preparations Before Starting* or *6. Preparations Before Starting (Cluster System)*.

2.1 Starting and terminating ITSLM

ITSLM requires that ITSLM - Manager and ITSLM - UR be started and terminated in a specific order.

When you start ITSLM, you must start ITSLM - Manager before you start ITSLM - UR. When you terminate ITSLM, you must terminate ITSLM - UR before you terminate ITSLM - Manager.

2.1.1 Starting ITSLM - Manager

To start ITSLM - Manager, start the services that comprise ITSLM - Manager and set their service status to **Start**.

You can have the ITSLM - Manager services start automatically when the OS starts. In such a case, you must use JP1/Base's startup control to set the order in which the services are to be started. If the services start automatically when the OS starts without setting the order, logging in to ITSLM or issuing JP1 events might fail. If ITSLM - Manager and ITSLM - UR are installed on the same host and you want to start the services automatically, you must use JP1/Base's startup control to set the ITSLM - Manager services to start first when the OS starts. For details about using JP1/Base for startup control, see the *Job Management Partner 1/Base User's Guide*.

If you have not set up the services to start automatically or when you are restarting ITSLM - Manager, you must start ITSLM - Manager by starting the services manually.

This subsection explains how to start ITSLM - Manager manually. If you run ITSLM - Manager in a cluster system, use the cluster software to start ITSLM - Manager; for details about the services to be started by the cluster software, see *(3) Supplementary information*.

(1) Before you start

- Verify that JP1/Base is running.
  For details about how to start JP1/Base, see the *Job Management Partner 1/Base User's Guide*.
- Verify that ITSLM - Manager has been set up.
  For details about how to set up ITSLM - Manager, see *5.1.6 Setting up ITSLM - Manager*.
- Verify that ITSLM - UR is not running.
- If you link your ITSLM with Performance Management, verify that the necessary linkage information has been defined in a system definition file. For details about how to define the necessary linkage information, see *5.4.1 Setting up the linkage between ITSLM and Performance Management (working with Performance Management)*.
- If you link your ITSLM with Performance Management, start each monitoring agent of the linked Performance Management and PFM - Manager. It doesn't matter whether you start ITSLM - Manager first or Performance Management first.
- If you link your ITSLM with JP1/IM, verify that the necessary linkage information has been defined in a system definition file. For details about how to define the necessary linkage information, see *5.5.1 Linking with JP1/IM*.

(2) Procedure

To start ITSLM - Manager:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

2. Start the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

3. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).

4. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).

Once the status of all three services is set to **Start** and in the above order, ITSLM - Manager has started.

(3) Supplementary information

- If you run ITSLM in a cluster system, use the cluster software to start the following services in the order shown below:
  1. Start the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).
  2. Start the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`).
  3. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).
  4. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).
- To restart ITSLM - Manager, perform *(2) Procedure* after ITSLM - Manager has terminated.
- When you start ITSLM - Manager and ITSLM - UR, if you perform the following steps in this order, you might not be able to log in to ITSLM - Manager for about two minutes because it takes time for ITSLM - Manager to initialize:
  1. Terminate ITSLM - Manager.
  2. Terminate ITSLM - UR.
  3. Start ITSLM - Manager.
- If you restart ITSLM - Manager while you are logged in to ITSLM - Manager, you must log in to ITSLM - Manager again because the logged-in session becomes invalid.

  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- The services that comprise ITSLM - Manager are dependent on each other. If you start **JP1/ITSLM - Manager Service** before starting **JP1/ITSLM - Manager DB Service**, **JP1/ITSLM - Manager DB Service** starts automatically. Similarly, if you start **JP1/ITSLM - Manager Web Service** before starting **JP1/ITSLM - Manager Service**, **JP1/ITSLM - Manager Service** starts automatically.
- If you have changed the system configuration (including when you restore the system configuration after a change) while ITSLM - Manager is running, you must restart ITSLM - Manager.
- If you link your ITSLM with Performance Management, information about the linkage with Performance Management that is defined in a system definition file takes effect when ITSLM - Manager is started. Therefore, if you want to edit the system definition file while ITSLM - Manager is running, first terminate ITSLM - Manager, edit the system definition file, and then restart ITSLM - Manager.
- If ITSLM - Manager is terminated after service detection of monitored services has started, service detection of monitored services will remain stopped the next time ITSLM - Manager is started.
- If ITSLM - Manager is terminated after monitoring of monitored services has started, the following processing takes place, depending on the `managerStartMode` value in ITSLM - Manager's system definition file (`jp1itslm.properties`):
  - When the `managerStartMode` property is omitted or **normal** is specified:

Monitoring of all monitored services whose monitoring had already started at the time of the previous termination processing is stopped.

- When **restart** is specified for the `managerStartMode` property:

  Monitoring of all monitored services whose monitoring had already started at the time of the previous termination processing is restarted in the normal status.

  If you specify **restart** for the `managerStartMode` property and you restart monitoring of the monitored services, the monitoring of inactive ITSLM - UR's monitored services is also placed in started status, but collection of service performance information is restarted after the corresponding ITSLM - UR is started.

(4) Next task

- *2.1.2 Starting ITSLM - UR*

(5) Related topics

- *2.1.4 Terminating ITSLM - Manager*

2.1.2 Starting ITSLM - UR

To start ITSLM - UR, start the ITSLM - UR service and set its service status to **Start**.

You can have the ITSLM - UR service start automatically when the OS starts if you set it up in the OS to start automatically. If ITSLM - Manager and ITSLM - UR are installed on the same host and you want to start the service automatically, you must use JP1/Base's startup control to set the ITSLM - Manager services to start first when the OS starts. For details about using JP1/Base for startup control, see the *Job Management Partner 1/Base User's Guide*.

If you have not set up the service to start automatically or when you are restarting ITSLM - UR, you must start ITSLM - UR by starting the service manually.

This subsection explains how to start ITSLM - UR manually. If you run ITSLM - UR in a cluster system, use the cluster software to start ITSLM - UR.

(1) Before you start

- Verify that ITSLM - UR has been set up.

  For details about how to set up ITSLM - UR, see *5.1.7 Setting up ITSLM - UR*.
- Verify that ITSLM - Manager is running.

  For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

(2) Procedure

To start ITSLM - UR:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

2. Start the ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`).

Once the status of the service is set to **Start**, ITSLM - UR has started.

(3) Supplementary information

- To restart ITSLM - UR, perform *(2) Procedure* after ITSLM - UR has terminated.
- If you restart ITSLM - UR while monitored services are being monitored, the restarted ITSLM - UR starts monitoring automatically.

  For details about starting monitoring, see *4.2.1 Starting monitoring*.
- If you have changed the system configuration (including when you restore the system configuration after a change) while ITSLM - UR is running, you must restart ITSLM - UR.

(4) Next task

- *2.2.1 Logging in to ITSLM - Manager*

(5) Related topics

- *2.1.3 Terminating ITSLM - UR*

2.1.3 Terminating ITSLM - UR

To terminate ITSLM - UR, stop the ITSLM - UR service and set its service status to **Stop**.

To restart ITSLM - UR, you must first terminate ITSLM - UR by stopping its service manually.

This subsection explains how to terminate ITSLM - UR manually. If you run ITSLM - UR in a cluster system, use the cluster software to terminate ITSLM - UR.

(1) Procedure

To terminate ITSLM - UR:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
2. Stop the ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`).

Once the service status is set to **Stop**, ITSLM - UR has terminated.

(2) Supplementary information

- If you use JP1/Base's startup control, the services are stopped when the OS is terminated in the reverse order from when they were started. You do not need to be concerned with the order in which services are stopped, even when ITSLM - Manager and ITSLM - UR are installed on the same host.

(3) Related topics

- *2.1.4 Terminating ITSLM - Manager*

2.1.4 Terminating ITSLM - Manager

To terminate ITSLM - Manager, stop the ITSLM - Manager services and set their service status to **Stop**.

If you do not use JP1/Base's startup control or if you want to restart ITSLM - Manager, you must first terminate ITSLM - Manager by stopping its services manually.

This subsection explains how to terminate ITSLM - Manager manually. If you run ITSLM - Manager in a cluster system, use the cluster software to terminate ITSLM - Manager. For details about the services to be stopped by using the cluster software, see *(2) Supplementary information*.

(1) Procedure

To terminate ITSLM - Manager:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
2. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).
3. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).
4. Stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

Once the status of all three services is set to **Stop** in the above order, ITSLM - Manager has terminated.

(2) Supplementary information

- If you run your ITSLM in a cluster system, use the cluster software to stop the following services in the order shown below:
    1. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).
    2. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).
    3. Stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`).
    4. Stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).
- Terminating ITSLM - Manager does not terminate the ITSLM - UR that is connected to ITSLM - Manager.

  For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.
- The services that comprise ITSLM - Manager are dependent on each other. If you attempt to stop **JP1/ITSLM - Manager Service** while **JP1/ITSLM - Manager Web Service** is running, the OS's Stop Other Services dialog box will be displayed. Similarly, if you attempt to stop **JP1/ITSLM - Manager DB Service** while **JP1/ITSLM - Manager Service** is running, the OS's Stop Other Services dialog box will be displayed.
- If you use JP1/Base's startup control, the services are stopped when the OS is terminated in the reverse order from when they were started. You do not need to be concerned with the order in which services are stopped, even when ITSLM - Manager and ITSLM - UR are installed on the same host.
- If ITSLM - Manager is terminated after monitoring of monitored services has started, accumulation of service performance information during the termination processing might be interrupted for several to several dozens of seconds. For this reason, we recommend that you stop monitoring of monitored services before you terminate ITSLM - Manager.

- If ITSLM - Manager is terminated after service detection of monitored services has started, service detection of monitored services remains stopped the next time ITSLM - Manager is started.
- If you link your ITSLM with Performance Management, terminate each agent of Performance Management and PFM - Manager as needed. There is no rule for the order in which ITSLM - Manager and Performance Management must be terminated.

2.2 Logging in to and out of ITSLM - Manager

To set up and perform monitoring, you must first start Internet Explorer (the *browser*) and log in to ITSLM - Manager.

2.2.1 Logging in to ITSLM - Manager

This subsection explains how to log in to ITSLM - Manager.

(1) Before you start

- Verify that JP1/Base has been used to set JP1 user operation permissions for the user who will be logging in to ITSLM - Manager.

  For details about setting JP1 user operation permissions, see *5.2.3 Specifying operation permissions for each JP1 user*.
- Verify that the target ITSLM - Manager is running.

  For details about starting ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

If you are performing monitoring, the ITSLM - UR connected to the login target ITSLM - Manager must also be running in addition to the above conditions. For details about starting ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

(2) Procedure

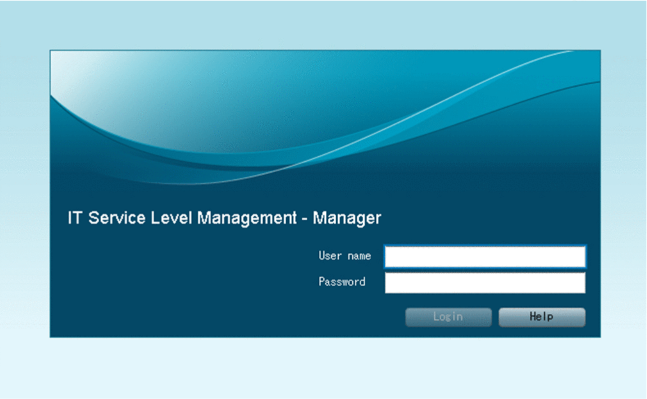
To log in to ITSLM - Manager:

1. Display the following access destination in the browser:

```
http://IP-address-of-ITSLM-Manager's-Web-server:listen-port-number-of-
ITSLM-Manager's-Web-server/jp1itslm/jp1itslm.jsp
```

   Do not specify a loopback address for *IP-address-of-ITSLM-Manager's-Web-server*.

   If the access destination is correct, the following window appears:



2. Enter your user name and password.

   The entered user name and password must be of a JP1 user.

3. Click the **Login** button.

If the ITSLM - Manager window is displayed, you have successfully logged in to ITSLM - Manager.

(3) Supplementary information

- *listen-port-number-of-ITSLM-Manager's-Web-server* is the value of the `psb_Listen` definition item in the options file that you specified when you set up ITSLM - Manager. By default, `20900` is set.
- If the entered user name or password is invalid, an error message is displayed. In such a case, the entered password is cleared.
- The **Login** button becomes clickable only when the entered user name and password are valid. If no user name or password is entered or if the entered information is not valid, the **Login** button does not become clickable.
- Multiple users can log in using the same user name.
- If login fails a specific number of times, the user name and password fields and the **Login** button are disabled and the window is locked. If the window has been locked, you must reload it by pressing the **F5** key on the keyboard or by selecting the browser's **Refresh** button. This will reset the login errors count.

  Use the `loginFailedLimit` property in the system definition file (`jp1itslm.properties`) to specify the login errors count that will result in a locked window.
- Do not drag any draggable window, such as a dialog box that is displayed in the event of an error, outside the browser's window. If a draggable window is dragged outside the browser's window, buttons in the window will no longer be selectable with the mouse. If this happens, you must reload the window by pressing the **F5** key on the keyboard or by selecting the browser's **Refresh** button. Note that after the window has been reloaded, the login window is displayed again. If you dragged an error dialog box outside the browser's window, check the log files for details of the error.

  For details about the log files, see *7.2 Log files*.
- If you are running ITSLM in a cluster system and failover has occurred in ITSLM - Manager, a message is displayed or a server's internal error is displayed; any attempt to log in to ITSLM - Manager will fail. In such a case, window operations are all disabled until the ITSLM - Manager failover has been completed. After the ITSLM - Manager failover has been completed, you must log in and perform necessary operations again.

  If failover has occurred in ITSLM - UR, you can still perform window operations. However, you cannot start or stop detection of monitored services or start or stop monitoring during failover until you can use another ITSLM - UR. If this happens, an error occurs and the error message is displayed in the window. Re-execute the operation after ITSLM - UR failover has been completed.
- If a firewall has been set up on a host from which you access ITSLM - Manager via a browser, you need to configure the firewall to release ephemeral ports used for communication between the browser and ITSLM - Manager.

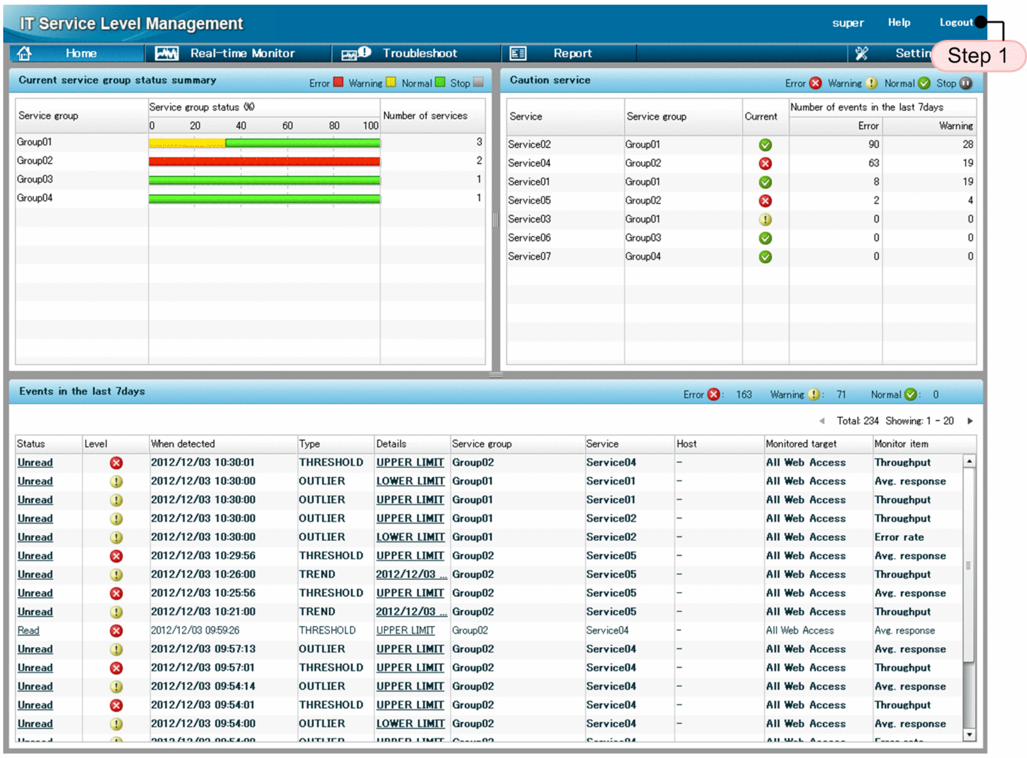
(4) Related topics

- *2.2.2 Logging out of ITSLM - Manager*
- *8.5.4 Changing the listen port number of the ITSLM - Manager embedded Web server*
- *A. List of Port Numbers Used by ITSLM*

2.2.2 Logging out of ITSLM - Manager

This subsection explains how to log out of ITSLM - Manager.

The following window is used in this task:



Current service group status summary Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%) 0 20 40 60 80 100	Number of services
Group01	🟨🟩	3
Group02	🟥	2
Group03	🟩	1
Group04	🟩	1

Caution service Error ✖ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service02	Group01	✓	90	28
Service04	Group02	✖	63	19
Service01	Group01	✓	8	19
Service05	Group02	✖	2	4
Service03	Group01	!	0	0
Service06	Group03	✓	0	0
Service07	Group04	✓	0	0

Events in the last 7days Error ✖: 163 Warning !: 71 Normal ✓: 0

◀ Total: 234 Showing: 1 - 20 ▶

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	✖	2012/12/03 10:30:01	THRESHOLD	UPPER LIMIT	Group02	Service04	-	All Web Access	Throughput
Unread	!	2012/12/03 10:30:00	OUTLIER	LOWER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	!	2012/12/03 10:30:00	OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!	2012/12/03 10:30:00	OUTLIER	UPPER LIMIT	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/03 10:30:00	OUTLIER	LOWER LIMIT	Group01	Service02	-	All Web Access	Error rate
Unread	✖	2012/12/03 10:29:56	THRESHOLD	UPPER LIMIT	Group02	Service05	-	All Web Access	Avg. response
Unread	!	2012/12/03 10:26:00	TREND	2012/12/03 ...	Group02	Service05	-	All Web Access	Throughput
Unread	✖	2012/12/03 10:25:56	THRESHOLD	UPPER LIMIT	Group02	Service05	-	All Web Access	Avg. response
Unread	!	2012/12/03 10:21:00	TREND	2012/12/03 ...	Group02	Service05	-	All Web Access	Throughput
Read	✖	2012/12/03 09:59:26	THRESHOLD	UPPER LIMIT	Group02	Service04	-	All Web Access	Avg. response
Unread	!	2012/12/03 09:57:13	OUTLIER	UPPER LIMIT	Group02	Service04	-	All Web Access	Avg. response
Unread	✖	2012/12/03 09:57:01	THRESHOLD	UPPER LIMIT	Group02	Service04	-	All Web Access	Throughput
Unread	!	2012/12/03 09:54:14	OUTLIER	UPPER LIMIT	Group02	Service04	-	All Web Access	Avg. response
Unread	✖	2012/12/03 09:54:01	THRESHOLD	UPPER LIMIT	Group02	Service04	-	All Web Access	Throughput
Unread	!	2012/12/03 09:54:00	OUTLIER	LOWER LIMIT	Group02	Service04	-	All Web Access	Avg. response

1. Click **Logout** in the upper right corner of the window.
   In ITSLM, all windows except the login window have a **Logout** button in the upper right corner.

2. In the dialog box for confirming logout, click the **OK** button.

If the login window is displayed next, you have logged out successfully. When you click the **OK** button, window operations become disabled until logout is completed.

2.3 Notes about operations after login to ITSLM - Manager

- If you refresh the window by pressing the **F5** key on the keyboard or by selecting the browser's **Refresh** button, the login window is displayed.
- Once you log in to ITSLM - Manager, the browser's **Back** and **Forward** buttons cannot be used to move from one window to another. Clicking the browser's **Back** button will display the Web page that was being displayed before the login window was displayed. If you click the **Forward** button after that, the login window will be displayed.
- If, while a window that follows ITSLM - Manager's login window is being displayed, you attempt to display that window in another browser by copying the browser's URL, the login window will be displayed.
- The current login session will expire if communication with ITSLM - Manager is interrupted for one minute. You must re-log in.

  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Do not drag any draggable window, such as a dialog box that is displayed in the event of an error, outside the browser's window. If a draggable window is dragged outside the browser's window, buttons in the window will no longer be selectable with the mouse. If this happens, you must reload the window by pressing the **F5** key on the keyboard or by selecting the browser's **Refresh** button. Note that after the window has been reloaded, the login window is displayed again. If you dragged an error dialog box outside the browser's window, check the log files for details of the error.

  For details about the log files, see *7.2 Log files*.
- The browser's zoom functions cannot be used to zoom the display.
- The login window is displayed automatically in the following cases:
  - When an error has occurred in the embedded database.
  - When a non-resumable error has occurred.
  - When a memory shortage has occurred.
  - When servlet initialization has failed.
  - When the session has expired.
- Do not change PFM-related permissions while you are logged in to ITSLM. The following explains what happens if permissions are changed while you are logged in:
  - If business group access permissions are changed while you are logged in, the change does not take effect until the next time you attempt to log in. If access permissions have been changed, log in again and then click the **Refresh configuration information** button in the **Configuration information settings** area of the Settings window.
  - If a JP1 resource group to which the `JP1_PFM_Operator` permission has been granted is added or deleted while you are logged in, the change will not take effect until the next time you log in. To effect the change, log in again when such a resource group is added or deleted.

3 Monitoring the Services to Be Monitored and Setup Required for Monitoring

This chapter explains the different types of monitoring that can be achieved by using ITSLM. This chapter also explains how to register the services to be monitored and how to set up the monitoring items for the monitored services.

3.1 Monitoring supported by ITSLM

ITSLM monitors the following three monitoring items based on actual accesses from users to the monitored services:

- Average response time
- Throughput
- Error rate

The data obtained by monitoring the monitoring items (average response time, throughput, and error rate) is characterized as the *service performance*. Service performance represents one second's worth of data, which means that service performance is measured 60 times per minute.

ITSLM enables you to perform out-of-range value detection and SLO monitoring on the basis of the monitoring items. The following table describes out-of-range value detection and SLO monitoring.

Table 3–1: Out-of-range value detection and SLO monitoring

No.	Monitoring (detection) type		Description
1	Out-of-range value detection		If the performance of a monitored service varies significantly from what is typical, this monitoring method regards such a condition as an early warning sign of a potential service performance error.
2	SLO monitoring	Trend monitoring	This monitoring method determines trends in the performance of a monitored service and uses the trends to predict overages of a service performance threshold.
		Threshold value monitoring	This monitoring method detects an overage of a service performance threshold for a monitored service.

When out-of-range value detection, trend monitoring, and threshold value monitoring are all performed, a warning is displayed by out-of-range value detection and trend monitoring whenever the possibility of a service performance error in a monitored service is suspected. If you take an appropriate corrective action at this early stage, you can prevent the service performance error from occurring. Once a service performance error has occurred, it is displayed by threshold value monitoring. In such a case, immediate corrective action is assumed to be called for.

If you link ITSLM with Performance Management, you can monitor the hosts and middleware that provide the monitored services. The monitoring items are set in Performance Management beforehand. The performance data monitored by Performance Management is called *system performance*. Out-of-range value detection and SLO monitoring are also applicable to system performance, similarly to service performance.

In addition, by linking ITSLM with Performance Management, you can monitor the availability of monitored services. *Availability monitoring* detects monitored services that have stopped as a result of an error. You can obtain the following evaluation metrics (SLOs) on the basis of the availability information acquired by availability monitoring:

- Service availability
- Mean time to recovery
- Mean time between failures

3.1.1 ITSLM's monitoring methods and types of monitored targets

A *Web access* covers the period from when a request was initiated by a user being monitored by ITSLM until the response to that request is completed.

ITSLM enables you to use two methods to monitor Web accesses:

- Monitoring all Web accesses (All Web Access monitoring)
  This method monitors Web accesses for all monitored services. In this method, the monitored target is called *All Web Access*.
- Monitoring specific Web accesses (Web transaction monitoring)
  This method monitors the Web accesses that are related to specific processing in the monitored services. In this method, a monitored target is called a *Web transaction*.

If you link ITSLM with Performance Management, you can also monitor system performance.

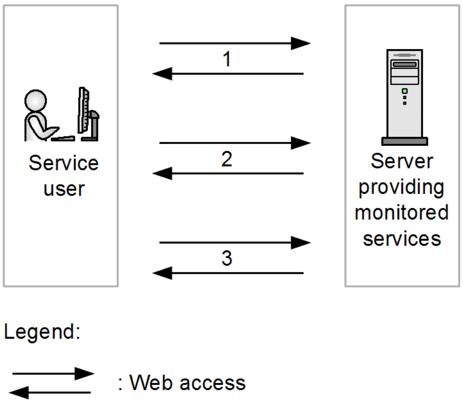
This subsection explains how monitoring of All Web Access, monitoring of Web transactions, and monitoring linked with Performance Management work and their respective monitoring items.

(1) Monitoring all Web accesses (All Web Access monitoring)

This method monitors all Web accesses to monitored services. When this method is used, **All Web Access** is displayed as the monitored target in the window.

The following figure shows the monitored target range when all Web accesses are monitored.

Figure 3–1: Range of monitored target when all Web accesses are monitored

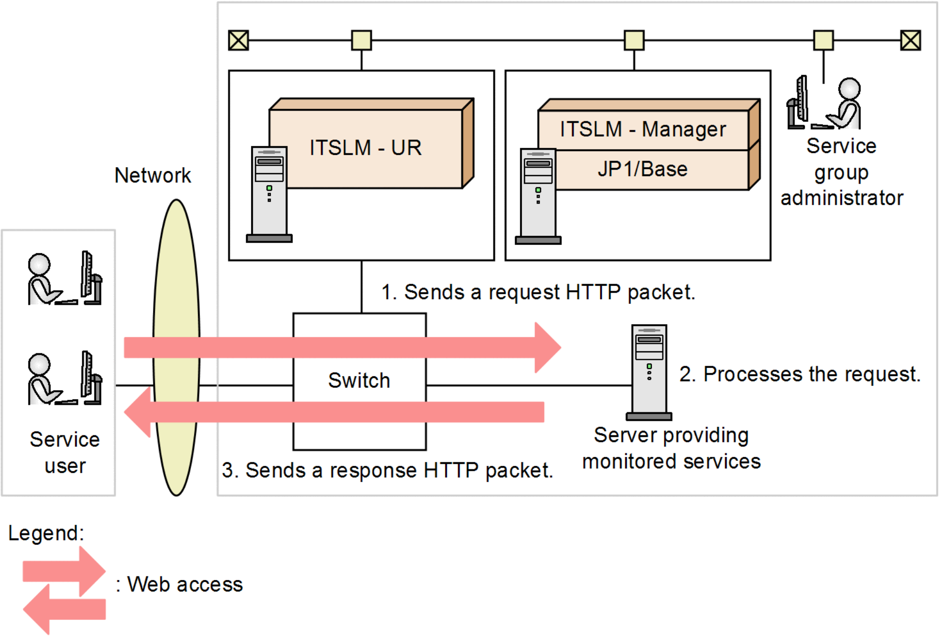


In this example, Web accesses 1 through 3 have occurred from the service user to monitored services. With this monitoring method, the averages or the totals of Web accesses 1 through 3 constitute the service performance of the monitoring items.

(2) Monitoring items for All Web Access

The following shows the relationship among the three monitoring items when monitoring of All Web Access is performed.

Figure 3–2: Relationship among monitoring items (for All Web Access)



ITSLM - UR
ITSLM - Manager
JP1/Base
Service group administrator
Network
1. Sends a request HTTP packet.
Switch
2. Processes the request.
Server providing monitored services
Service user
3. Sends a response HTTP packet.
Legend:
: Web access

- Average response time (milliseconds)

  This is the average time required for 1 through 3 in the figure to be completed. Responses include error responses.#

- Throughput (per second)

  This is a count of the number of times 1 through 3 in the figure occurred in one second. Responses include error responses.# Note that requests resulting in a timeout during request collection by ITSLM - UR are not included. Each set of the events identified as 1 through 3 is counted as one when the set is completed.

- Error rate (%)

  This is the percentage of the event 1 items in the figure that end up as event 3 error responses# or as timeouts during request collection by ITSLM - UR.

#

These are the responses whose HTTP status is error `400` to `599`.

The HTTP packets for requests and responses are collected by ITSLM - UR when they pass the switch.

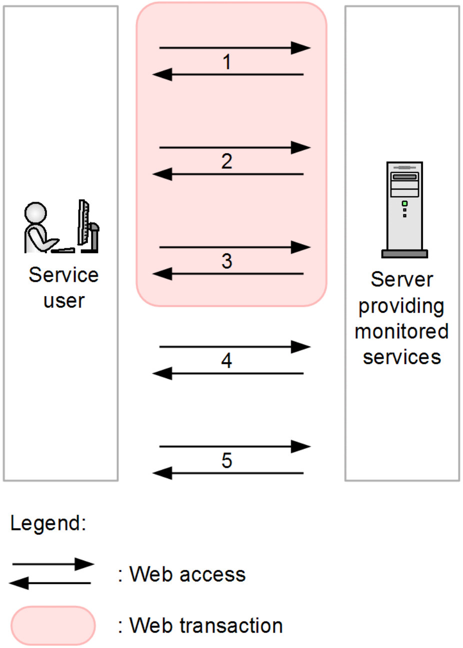
(3) Monitoring specific Web accesses (Web transaction monitoring)

Among all Web accesses to the monitored services, this method monitors only those Web accesses that constitute a series of processes that satisfy a specified condition. Such a series of processes that is subject to monitoring is called a Web transaction. Because this method enables you to determine the status of specific processes contained in a monitored service individually, you can promptly identify a process that might adversely affect service performance. You can set multiple Web transactions for a single monitored service. A condition for identifying the Web accesses to be treated as a Web transaction is called a *Web access condition*.

You can monitor Web transactions if your ITSLM - Manager and ITSLM - UR versions are 09-51 or later.

The following figure illustrates the range of a monitored target when specific Web accesses are monitored.

Figure 3–3: Range of monitored target when specific Web accesses are monitored



In this example, Web accesses 1 through 5 have occurred from the service user to the monitored service. Whenever Web accesses 1 through 3 all satisfy a pre-registered Web access condition, that series of Web accesses is monitored as a Web transaction.

In the monitoring of a Web transaction, the average or the total of the results of monitoring the transmissions of the first request (1 in the figure) through the last response (3 in the figure) of the Web transaction constitutes the monitoring item's service performance.

ITSLM monitors only those Web accesses that occur in an order specified for the Web access condition. A Web access whose order of occurrence is undetermined cannot be included in a Web transaction.

Whether Web accesses are included in a target Web transaction is determined as follows:

1. Each time a Web access occurs, whether that Web access satisfies a Web access condition is checked in the order of the Web access conditions.

   When a Web access that satisfies the first Web access condition is detected, any subsequent Web access is checked to determine whether it satisfies the second Web access condition.

   Note that once a Web access satisfies one of the Web access conditions, it is no longer checked against any subsequent Web access conditions. For example, a Web access satisfying the first Web access condition is treated as satisfying only the first Web access condition even if it would also satisfy the second Web access condition.
2. When a Web access satisfying the last Web access condition is detected, the series of Web accesses is identified as a Web transaction.

If another Web access satisfying the first Web access condition is detected in the same Web transaction before a Web access satisfying the last Web access condition is detected, the current check processing is placed in the status in which a Web access satisfying only the first Web access condition has been detected.

Examples are shown below. For these examples, the Web access conditions for a Web transaction are set in the order of Web access condition 1 ➜ Web access condition 2 ➜ Web access condition 3.

Example of Web accesses that are treated as a Web transaction

- Web accesses that occurred in the order of Web access 1 ➜ Web access 2 ➜ Web access 3

- Web accesses that occurred in the order of Web access 1 ➜ Web access 2 ➜ Web access 4 ➜ Web access 3 (Web access 4 is not used in the calculation of the error rate monitoring item for the Web transaction)
- Web accesses that occurred in the order of Web access 1 ➜ Web access 2 ➜ Web access 2 ➜ Web access 3 (the second Web access 2 is not used in the calculation of the error rate monitoring item for the Web transaction)

Examples of Web accesses that are not treated as a Web transaction

- Web accesses that occurred in the order of Web access 1 ➜ Web access 2 ➜ Web access 1 ➜ Web access 3

  In this case, when the second Web access 1 was detected, the existing record for the order Web access 1 ➜ Web access 2 was discarded. The subsequent Web accesses are not treated as a Web transaction because they occurred in the order of Web access 1 ➜ Web access 3.
- Web accesses that occurred in the order of Web access 1 ➜ Web access 2 ➜ Web access 3 ➜ Web access 3

  The same Web access cannot be monitored more than once in the same Web transaction. Monitor this example as Web access 1 ➜ Web access 2 ➜ Web access 3. Note that the Web accesses that can be monitored are Web access 1 ➜ Web access 2 ➜ Web access 3 (first one). Web access 1 ➜ Web access 2 ➜ Web access 3 (second one) cannot be monitored.

(4) Components of a Web access condition for a Web transaction

A web access condition consists of the URI and cookie contained in the Web access. For a URI, only path and query information can be specified as Web access condition components.

The following examples illustrate the structure of a URI and cookie contained in a Web access.

URI

`http://`*host*`:`*port*`/`*path*`?`*query*

- Example 1: `http://hitachi.`*XXX*`:1234/`*YYY*`/`*ZZZ*`.html`
- Example 2: `http://hitachi.`*XXX*`?division=1&section=2`

Cookie

key=value

- Example 1: `year=2011`
- Example 2: `month=08`

A Web access satisfying the specified Web access condition becomes a Web transaction. If multiple Web access conditions are specified, the set of Web accesses that satisfy all the specified Web access conditions becomes a Web transaction.

If multiple Web accesses satisfy the same Web access condition, they are treated as being the same Web transaction.

Suppose Web transaction X is defined as follows:

Definition of Web transaction X

- Web accesses are to occur in the order of Web access 1 ➜ Web access 2 ➜ Web access 3.
- The Web access conditions are defined as follows:

Web access condition	Path	Query condition	Cookie condition
Web access condition 1	`/top.html`	`a=1`	Not specified.
Web access condition 2	`/middle.html`	`b=.*`	Not specified.
Web access condition 3	`/bottom.html`	`c=3`	Not specified.

Combinations of Web accesses monitored as Web transaction X

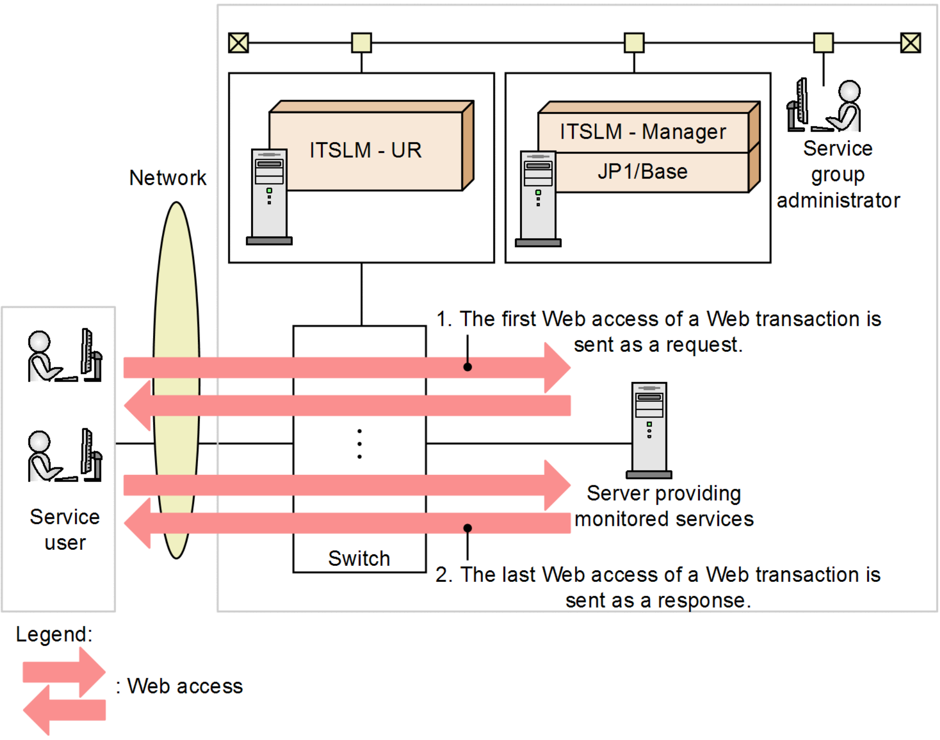
Both of the following combinations of Web accesses are monitored as Web transaction X:

- Web accesses occurring in the order of *path*: `/top.html` *query*: `a=1`, *path*: `/middle.html` *query*: `b=2`, and *path*: `/bottom.html` *query*: `c=3`
- Web accesses occurring in the order of *path*: `/top.html` *query*: `a=1`, *path*: `/middle.html` *query*: `b=4`, and *path*: `/bottom.html` *query*: `c=3`

(5) Monitoring items for Web transactions

The following figure shows the relationship among three monitoring items when Web transactions are monitored.

Figure 3–4: Relationship among monitoring items (for Web transactions)


ITSLM - UR
ITSLM - Manager
JP1/Base
Service group administrator
Network
1. The first Web access of a Web transaction is sent as a request.
Server providing monitored services
Service user
Switch
2. The last Web access of a Web transaction is sent as a response.
Legend:
: Web access

- Average response time (milliseconds)

  This is the average time required for the last Web access (*2* in the figure) of the Web transaction to be sent as a response since the first Web access (*1* in the figure) was sent as a request. Responses include error responses.#

- Throughput (per second)

  This is the number of times *1* through *2* occurred in one second, beginning with transmission of the first Web access (*1* in the figure) of the Web transaction as a request through the last Web access (*2* in the figure) as a response. Responses include error responses.# Note that requests resulting in a timeout during request collection by ITSLM - UR are not included. From the transmission of the first Web access (*1* in the figure) of the Web transaction as a request through the transmission of the last Web access (*2* in the figure) as a response is counted as one when the set is completed.

- Error rate (%)

  This is the percentage of the number of Web accesses (*1* to *2* in the figure) in the Web transaction sent as requests that ended up as error responses# or as timeouts during request collection by ITSLM - UR.

#

These are the responses whose HTTP status is error `400` to `599`.

The HTTP packets for requests and responses are collected by ITSLM - UR when they pass the switch.

(6) Monitoring system performance (by linking with Performance Management)

If you link your ITSLM with Performance Management, you can monitor system performance.

System performance is monitored based on performance data collected for each Performance Management monitoring agent assigned to a monitored service. Each monitoring agent that collects data is displayed in the ITSLM window at a separate hierarchical level and the results are reported by hierarchical level.

(7) Monitoring items for system performance

There are two types of monitoring items for system performance:

- Default monitoring items provided by Performance Management
- Monitoring items defined by the user of Performance Management

ITSLM enables you to monitor both types of monitoring items together.

For details about the monitoring items for system performance, see the description of monitoring items in the *Job Management Partner 1/Performance Management User's Guide*.

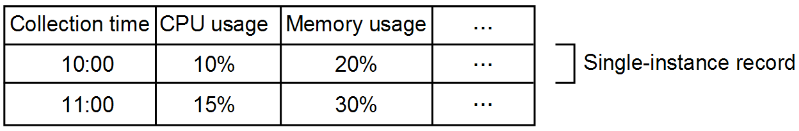
System performance data is collected in units called *records*. There are two types of records depending on the monitoring item:

- Single-instance records
- Multi-instance records

Single-instance records

A single-instance record consists of one row of data that is collected at a single point of data collection.

The following shows an example of single-instance records:



Collection time	CPU usage	Memory usage	...
10:00	10%	20%	...
11:00	15%	30%	...

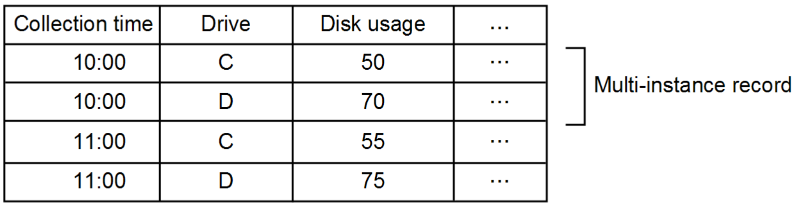
Single-instance record

Each row (record) contains performance data for a specific time. This record stores performance data, such as the CPU usage and memory usage at the monitored host.

Multi-instance record

A multi-instance record consists of multiple rows of data that are collected at a single point of data collection.

The following shows an example of multi-instance records:



Collection time	Drive	Disk usage	...
10:00	C	50	...
10:00	D	70	...
11:00	C	55	...
11:00	D	75	...

Multi-instance record

This example collects performance data for drives C and D in separate rows at each collection time. Therefore, to search for specific performance data at a particular time, you must specify both the collection time and the drive.

For details about instance records, see the description of performance data in the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

(8) Supplementary information

- When a Web transaction is monitored, the Web accesses constituting the Web transaction must be within the monitoring range of the ITSLM - UR that monitors the target service for which the Web transaction is defined. If you want to monitor Web accesses outside the monitoring range, you must monitor them as Web accesses of a Web transaction of a monitored service whose Web accesses fall within the desired monitoring range.
- If you monitor a Web transaction and want to identify whether each Web access is from the same user, specify a session condition for the Web transaction. For a session condition, specify a query and a cookie key. Web accesses with the specified query and cookie key values are treated as Web accesses from the same user.
- The maximum length of an HTTP packet that ITSLM can monitor is 1,500 bytes including the IP and TCP headers. If a packet is longer than 1,500 bytes but contains the information to be monitored in the first 1,500 bytes, ITSLM can monitor it successfully. Any data following byte 1,500 is discarded.

(9) Related topics

- *3.1.2 Using out-of-range value detection for detection of unusual status in monitored services*
- *3.1.3 Using trend monitoring for detection in advance of threshold overages*
- *3.1.4 Using threshold value monitoring for detection of threshold overages*
- *3.2.3 Setting up the Web transactions to be monitored*
- *3.2.7 Setting up the monitoring items for service performance*

3.1.2 Using out-of-range value detection for detection of unusual status in monitored services

Out-of-range value detection is performed for each monitoring item. You can also combine multiple monitoring items and monitor them as a set. For details about the monitoring items, see *3.1.1 ITSLM's monitoring methods and types of monitored targets*.

This subsection provides an overview of out-of-range value detection and how to obtain the base line, upper-limit value, and lower-limit value.

(1) About out-of-range value detection

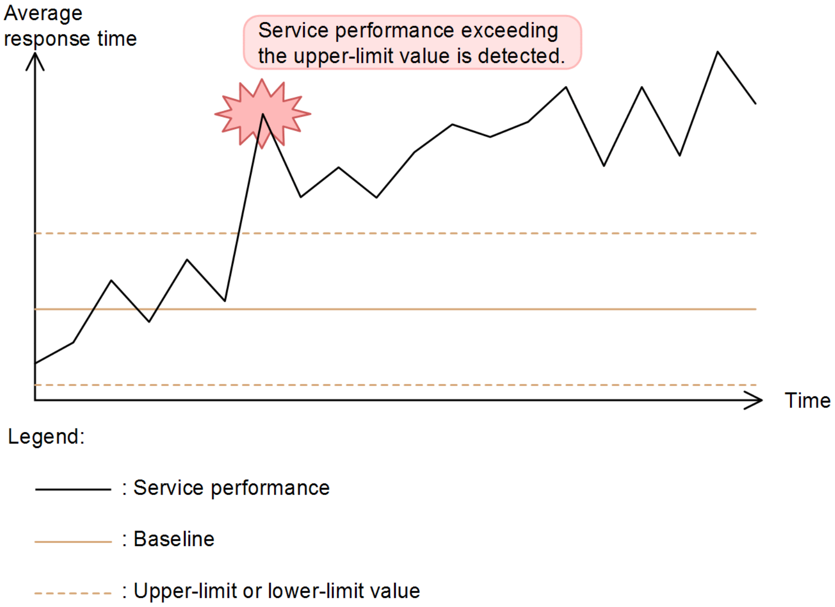
If the performance of a monitored service becomes noticeably poor, this monitoring method regards this change as an early warning sign of a potential service performance error. The method obtains an average value from accumulated past service performance data and detects any value that differs significantly from this average as constituting an *out-of-range value*. The average value obtained from accumulated past service performance data is called the *baseline*.

In out-of-range value detection, some upper margin from the baseline and some lower margin from the baseline are used as *upper-limit and lower-limit values*. This detection method checks whether the current service performance is veering significantly away from the baseline (that is, differs significantly from the usual service performance) and determines the current service performance to constitute an out-of-range value when it falls beyond the upper-limit or lower-limit value. The baseline and the upper-limit and lower-limit values are updated every 60 seconds.

Outlier detection is based on statistics using standard deviation. For the baseline, the average of the service performance data collected in the past is used. The upper and lower limits are calculated based on that average and standard deviation.

The following figure shows an example in which unusual service performance is detected by out-of-range value detection.

Figure 3–5: Example in which unusual service performance is detected by out-of-range value detection



This example monitors the average response time. The service performance value increased as time went by and an out-of-range value was detected when it exceeded the upper-limit value.

The upper-limit and lower-limit values are determined by setting a *sensitivity* that determines a distance from the baseline, beyond which point the performance of a monitored service is to be detected as an out-of-range value. The sensitivity setting determines the sensitivity of detection.

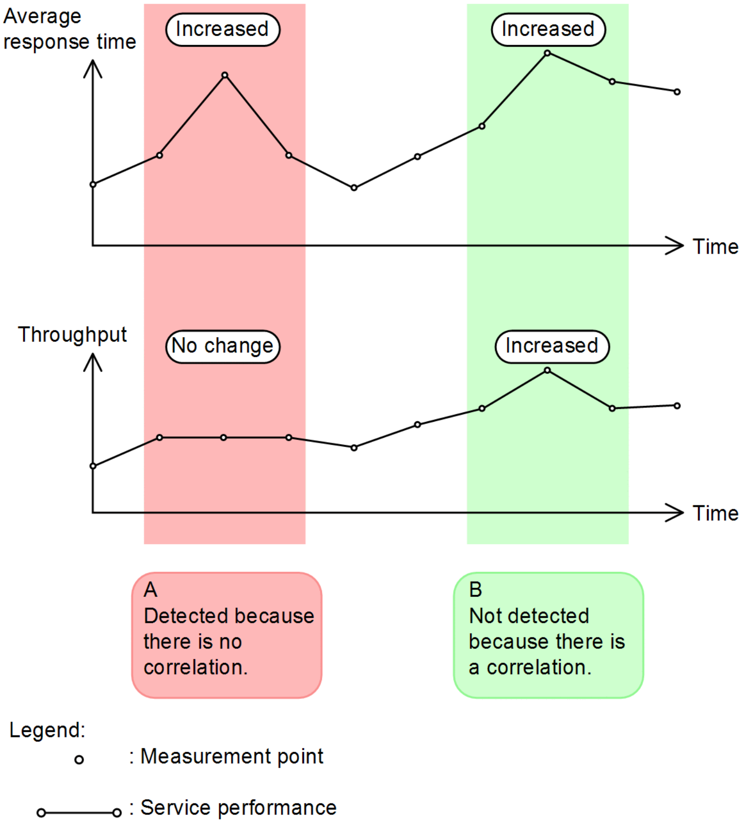
In out-of-range value detection, you can combine multiple monitoring items together as a set.

By combining multiple monitoring items, you can improve the precision of predictive error detection in service performance by taking into account a correlation among monitoring items. The two monitoring items that can be combined are average response time and throughput.

When these two monitoring items are correlated, one of them might seem abnormal, but it might not appear to be abnormal when the correlation is taken into account. For example, if the average response time is increasing but this is the result of an increase in throughput due to an increase in the number of users using the monitored service, this increase in average response time might be treated as a normal change in service performance due to the increased system load. In out-of-range value detection using a combination of multiple monitoring items, you can improve detection precision by treating a change in service performance caused by such a correlation as normal and not detecting it.

The following provides an example in which unusual service performance is detected by out-of-range value detection with a combination of multiple monitoring items.

Figure 3–6: Example in which unusual service performance is detected by out-of-range value detection with a combination of multiple monitoring items



In *A* in the figure, an unusual increase either in average response time or in throughput in the same period would be detected as a warning sign of a service performance error. However, in *B* in the figure, the increases in both response time and throughput in the same period are treated as being normal due to their correlation and they are not detected.

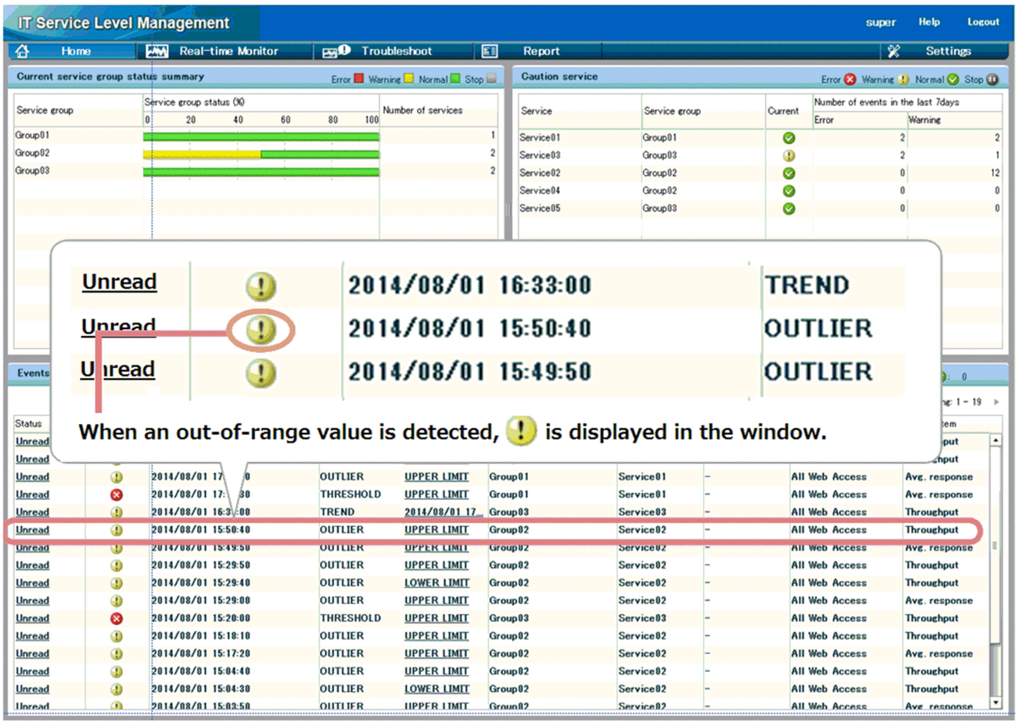
In out-of-range value detection with a combination of multiple monitoring items, the correlation of the two service performance items is taken into account in determining the baseline. When service performance falls beyond the upper-limit or lower-limit value that has been determined based on this baseline, the correlation is treated as not being the cause and a warning sign is detected.

In out-of-range value detection with a combination of multiple monitoring items, the baseline and the upper-limit and lower-limit values are updated every hour.

A detected out-of-range value is displayed in the window as a warning.

The following shows an example of a window in which a warning is displayed.

Figure 3–7: Example of window with a warning displayed (out-of-range value detection)



Current service group status summary

Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%)	Number of services
Group01		1
Group02		2
Group03		2

Caution service

Error ✖ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
Service05	Group03	✓	0	0

Unread	!	2014/08/01 16:33:00	TREND
Unread	!	2014/08/01 15:50:40	OUTLIER
Unread	!	2014/08/01 15:49:50	OUTLIER

When an out-of-range value is detected, ! is displayed in the window.

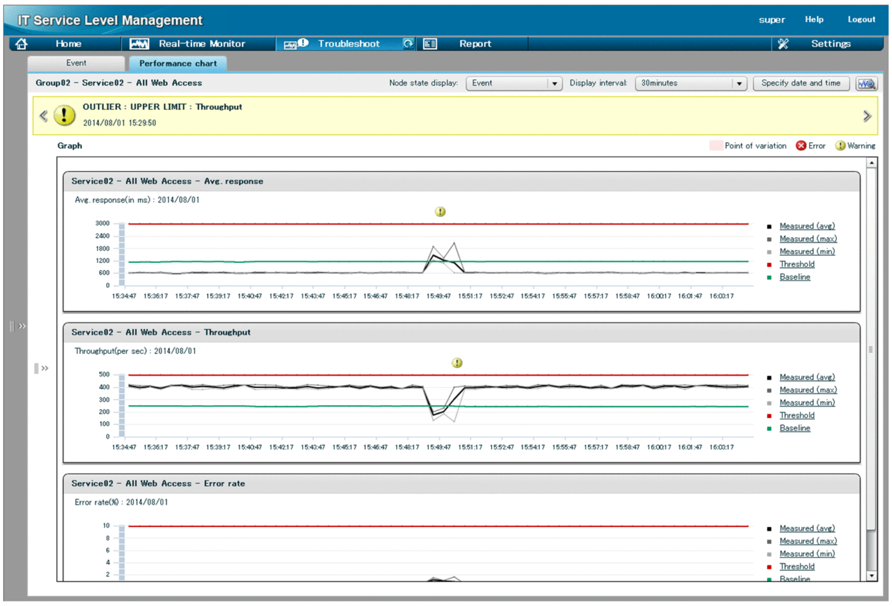
Status									
Unread									put
Unread									hput
Unread	!	2014/08/01 17: 0	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	✖	2014/08/01 17: 30	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2014/08/01 16:3 :00	TREND	2014/08/01 17...	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	✖	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response

zu030370.vsd／J:¥Hitachi¥2014Jobs¥490911_311¥60_DTP¥VSD¥／／2014/10/29／2:08／

The information displayed in the window for a warning includes a warning icon, the detection date and time, the name of the service group detected for the warning, and the service name. If service performance continues to exceed the upper-limit value or continues to be lower than the lower-limit value, only the first warning detected is displayed. You can view the service performance leading up to and following the point of the warning as a graph.

The following shows an example of a graph.

Figure 3–8: Example of a graph (out-of-range value detection)



OUTLIER : UPPER LIMIT : Throughput
2014/08/01 15:29:50

In the graph, a warning icon indicates the time the service performance exceeded the upper-limit value or dropped below the lower-limit value and a colored belt indicates the time period during which the event resulting in the out-of-range value is suspected to have occurred.

To perform out-of-range value detection, you must specify the following items in the Settings window:

- **Days till start**
- **Days in baseline calculation**
- **Sensitivity**

Days till start

Specifies the number of days for which service performance data is to be accumulated before out-of-range value detection is to be started. Out-of-range value detection requires that service performance data be accumulated from the monitored service running in the actual operating environment before a baseline can be calculated. If service performance data is accumulated for at least one day, out-of-range value detection can be performed. However, if the number of days specified for accumulation of service performance data is less than the number of days to be used in the baseline calculation, the obtained baseline might be unrealistic because there is not enough data to calculate it. For **Days till start**, we recommend that you specify a value that is at least equal to the number of days to be used in the baseline calculation.

Days in baseline calculation

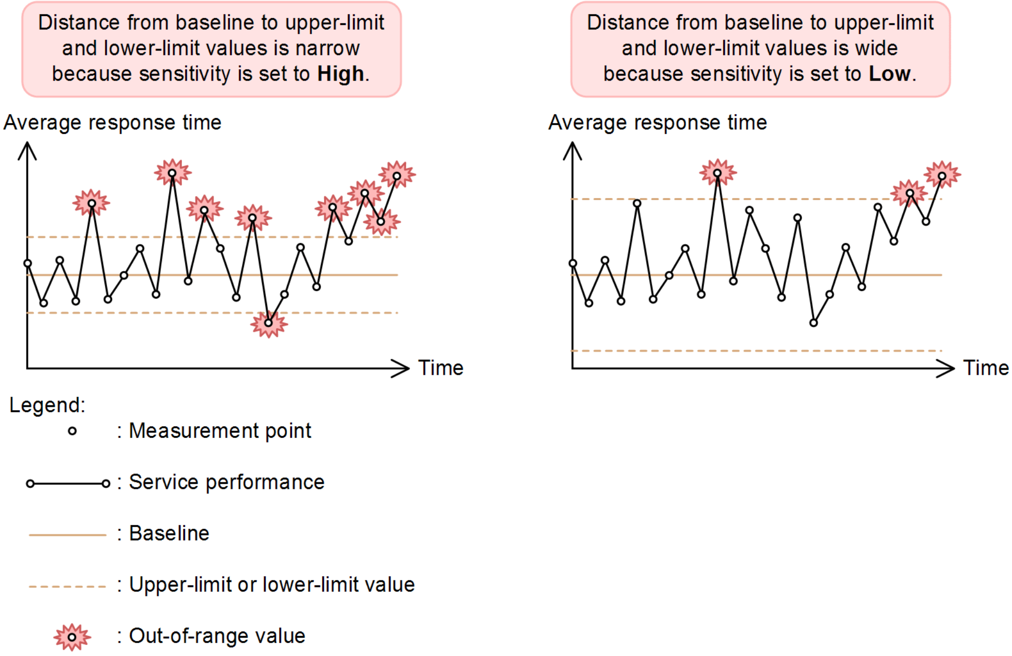
Specifies the number of days' worth of accumulated past service performance data that are to be used for calculation of the baseline.

Sensitivity

Specifies a sensitivity setting for out-of-range value detection that is to be used to determine the distance from the baseline to the upper-limit and lower-limit values. You can select **High**, **Middle**, or **Low** for the sensitivity setting. High sensitivity reduces the distance from the baseline to the upper-limit and lower-limit values, making service performance anomalies more likely to be detected. Low sensitivity increases the distance from the baseline to the upper-limit and lower-limit values, making service performance anomalies less likely to be detected. For **High**, the distance is half of the distance for **Middle**; for **Low**, the distance is 1.5 times the distance for **Middle**.

The following shows examples in which the distance from the baseline to the upper-limit and lower-limit values is narrowed or widened depending on the sensitivity.

Figure 3–9: Examples in which the distance from the baseline to the upper-limit and lower-limit values is narrowed or widened



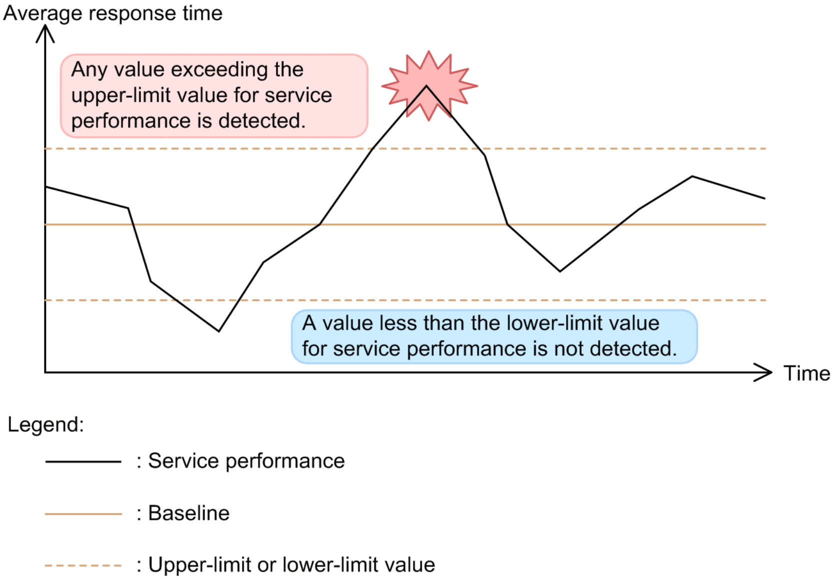
This example monitors the average response time. The service performance is the same in both graphs. However, when the distance from the baseline to the upper-limit and lower-limit values is narrow, as in the graph on the left, more out-of-range values in service performance are detected than when the distance from the baseline to the upper-limit and lower-limit values is wide, as in the graph on the right.

Setting the upper-limit and lower-limit values for out-of-range value detection

Use the `serviceBaselineExclusion` property in ITSLM - Manager's system definition file (`jp1itslm.properties`) to set upper-limit and lower-limit values for out-of-range value detection.

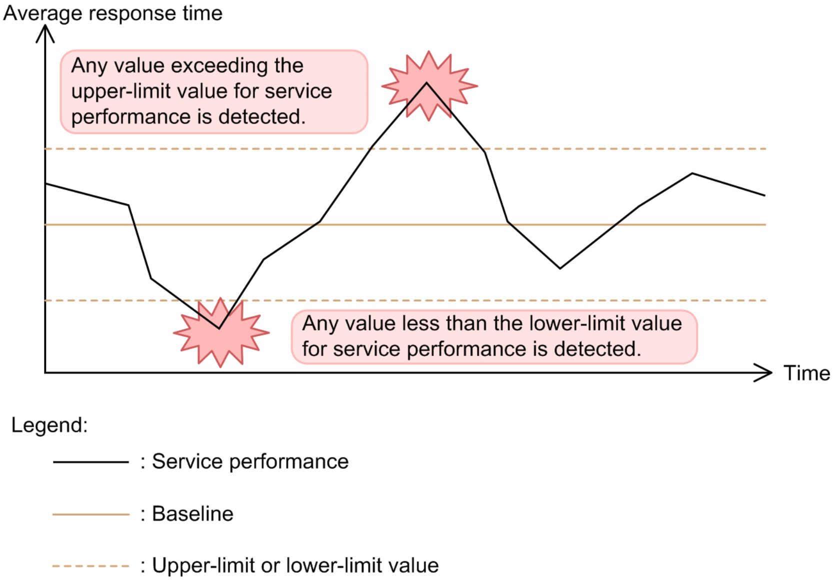
When this property is set to `true`: ITSLM detects only values that exceed the upper-limit value from the baseline.

Figure 3–10: Example of detecting only values that exceed the upper-limit value



When this property is set to `false`: ITSLM detects any value exceeding the upper-limit value or dropping below the lower-limit value from the baseline.

Figure 3–11: Example of detecting any value exceeding the upper-limit value or dropping below the lower-limit value



For details about how to edit system definition files, see *5.6.1 Editing the system definition files*.

When linking with Performance Management

If you link ITSLM with Performance Management, you can also perform out-of-range value detection in system performance. However, when system performance is monitored, out-of-range value detection using a combination of multiple monitoring items is not supported.

Use the `systemBaselineExclusion` property in ITSLM - Manager's system definition file (`jp1itslm.properties`) to set upper-limit and lower-limit values for out-of-range value detection for system performance. For details about how to edit system definition files, see *5.6.1 Editing the system definition files*.

(2) How to obtain the baseline and upper-limit and lower-limit values

The baseline used as the criterion for determining out-of-range values is obtained as follows:

For a service monitoring configuration

1. The average throughput service performance (average processing count) for the monitored service over the past one hour is determined.
2. From the accumulated service performance data (over a maximum of 60 days), the service performances whose averaged processing counts for the same period are the closest to the past hour's average processing count are selected.
3. From the service performances for the selected dates, an average value (baseline) up to one hour ahead from the current time is calculated every minute for each monitoring item.

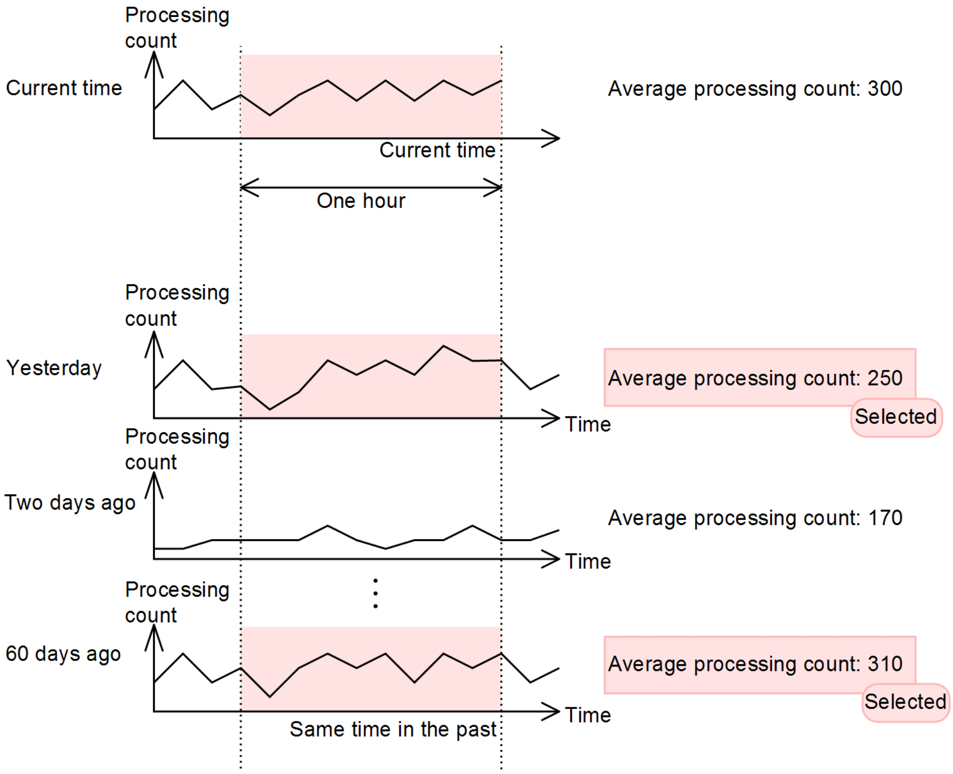
For a system monitoring configuration

1. The average of the system values measured during the past hour for the selected monitored target is calculated.
2. From the accumulated system performance data (over a maximum of 60 days), the dates whose average system performance for the same period is the closest to the current average value are selected.
3. For each monitoring item, based on the system performance data for the selected dates, the average of the values from the present time to an hour later (the baseline) is calculated every minute.

For example, if service performance for the same time period differs greatly depending on the day of the week, such as a monitored service whose processing counts for regular business days differ considerably from the processing counts for weekends and holidays, a realistic baseline can be obtained by calculating it based on past service performance that takes into account regular business days and weekends and holidays.

The following example selects the past service performance for baseline calculation from the service performance data accumulated for the past 60 days and using the days whose average processing counts are closest to the past hour's average processing count.

Figure 3–12: Example of selecting the past service performance for baseline calculation from the service performance data accumulated for the past 60 days and using the days whose average processing counts are closest to the past hour's average processing count



The service performances for the days whose average processing counts are the closest to the average processing count for the past hour are selected from the accumulated past service performance data. In this example, the past hour's average processing count is 300. Therefore, the service performance from yesterday and from 60 days ago, which have the closest average processing counts, are selected from all the service performance over the past 60 days. The service performance from two days ago is not selected because its average processing count is quite different from the past hour's average processing count. As many service performance values are selected from the past service performance data as the number of days specified for **Days in baseline calculation** in the Settings window.

The following rules apply to selection of past service performance:

- If there are multiple days with the same average processing count, the day that is closest to the current date is selected.
- When a day whose service performance will be used is selected, the number of times service performance was collected that day is not considered. However, a day when no service performance data was collected will not be selected.
- In cases such as immediately after monitoring is stopped and then restarted, there might not be an average processing count for the past hour. In such cases, the first day that qualifies is selected by checking days in reverse order starting from the previous day.

According to these rules, past service performance over as many days as specified for **Days in baseline calculation** under **Error Predict. settings** is used (or past service performance over the number of days for which data has been accumulated is used). This selection of past service performance occurs once an hour on the hour.

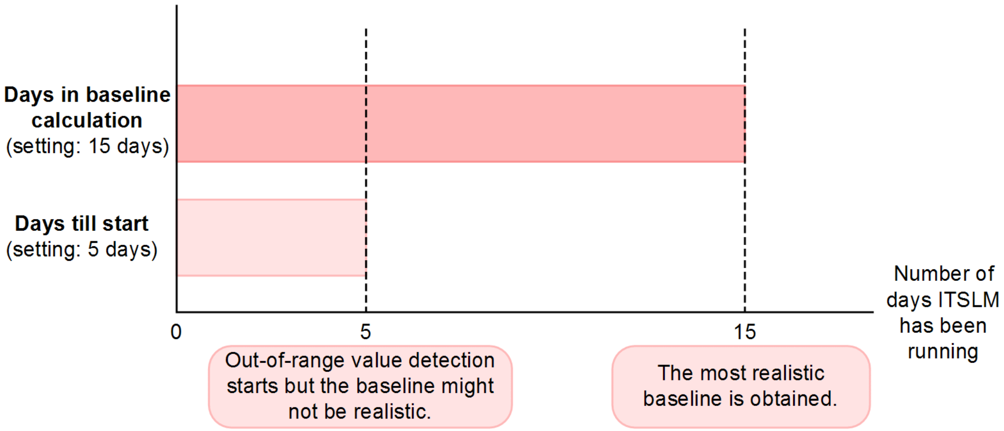
The baseline is calculated after selection of the days to be used, in order of priority, from the oldest data that is entered.

You can start out-of-range value detection if one day's worth of service performance data has been accumulated. However, the baseline might not be realistic until as many days' worth of service performance data as needed for baseline calculation has accumulated. To obtain a realistic baseline, we recommend that you do not start out-of-range value detection until enough service performance data for the baseline calculation has accumulated.

For **Days till start** in the Settings window, specify the number of days service performance data is to be accumulated before out-of-range value detection is started.

The following figure shows the relationship between the number of days used for baseline calculation (**Days in baseline calculation**) and the number of days before out-of-range value detection is started (**Days till start**).

Figure 3–13: Relationship between the number of days used for baseline calculation (Days in baseline calculation) and the number of days before out-of-range value detection is started (Days till start)



Days in baseline calculation
(setting: 15 days)
Days till start
(setting: 5 days)
0
5
15
Number of days ITSLM has been running
Out-of-range value detection starts but the baseline might not be realistic.
The most realistic baseline is obtained.

This example specifies 15 days for **Days in baseline calculation** and 5 days for **Days till start**.

In this example, out-of-range value detection starts five days after ITSLM operation began. The baseline is calculated from the past five days' worth of service performance. Because this value is less than the number of days set for baseline calculation, the resulting baseline might not be realistic. The most realistic baseline is obtained on the 15th day of ITSLM operation, because as many days' worth of service performance data as needed for baseline calculation has been accumulated.

When multiple monitoring items are combined, there are some differences in the baseline calculation method.

When out-of-range value detection is performed with multiple monitoring items combined, past service performance is based on average throughput (average processing count), and then the average correlation between average response time and throughput is obtained for the selected days, and finally the baseline is calculated.

Because the baseline used for detection is different, an out-of-range value in out-of-range value detection with multiple monitoring items combined differs as indicated below from the out-of-range value in normal out-of-range value detection:

- Out-of-range value in normal out-of-range value detection

  Indicates that the current service performance differs significantly from the usual service performance.

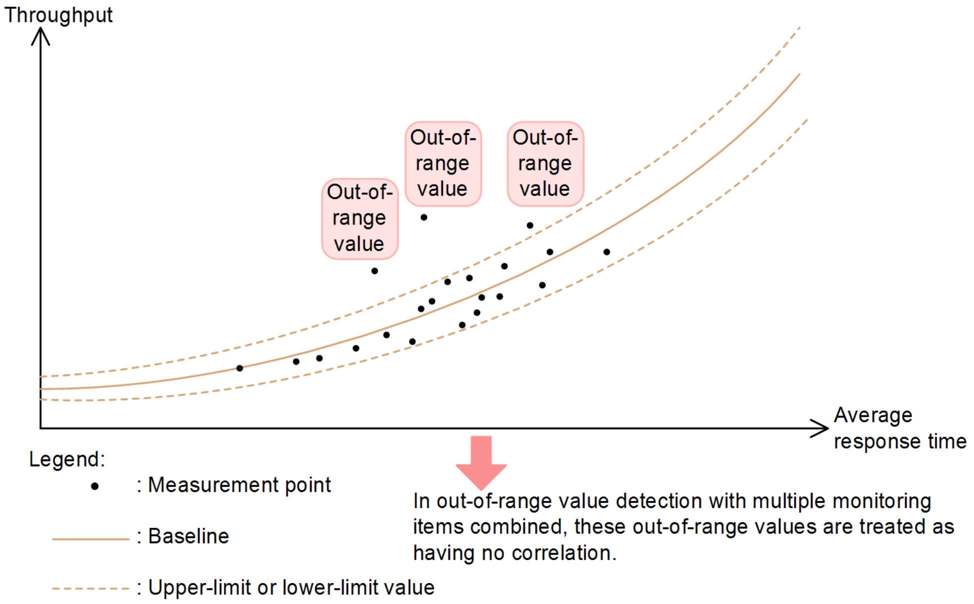
- Out-of-range value in out-of-range value detection with multiple monitoring items combined

  Indicates that in the current service performance, there is no correlation at this time between the multiple monitoring items.

Therefore, an out-of-range value exceeding the upper-limit value in normal out-of-range value detection might be less than the lower-limit value in out-of-range value detection with multiple monitoring items combined. Conversely, an out-of-range value that is less than the lower-limit value in normal out-of-range value detection might exceed the upper-limit value in out-of-range value detection with multiple monitoring items combined.

The following figure shows an example in which out-of-range values are detected in out-of-range value detection with multiple monitoring items combined.

Figure 3–14: Example in which out-of-range values are detected in out-of-range value detection with multiple monitoring items combined



In out-of-range value detection with multiple monitoring items combined, these out-of-range values are treated as having no correlation.

This example monitors average response time and throughput. The baseline is calculated on a graph containing both monitoring items. Any value exceeding the upper-limit value or less than the lower-limit value is detected as an out-of-range value, and the monitoring items are treated as having no correlation.

The upper-limit and lower-limit values for out-of-range value detection or for out-of-range value detection with multiple monitoring items combined are determined by irregularity from the past service performance selected for the baseline calculation and the sensitivity that has been set for tuning detectability.

When linking with Performance Management

The baseline used for monitoring system performance is calculated from system performance data that is selected using the same criteria as for monitoring service performance. If a day has the highest priority in one monitoring item but no system performance was collected, that day is not selected; the day with the next highest priority is selected. Therefore, the days used for baseline calculation might depend on the monitoring items.

When you monitor system performance, you can specify separately for each monitoring item the number of days to be used for baseline calculation.

(3) Detection criteria

In out-of-range value detection, out-of-range values are detected only when they occur consecutively so as to avoid detecting transient out-of-range values.

This subsection explains the criteria for detecting out-of-range values when service performance is monitored and when system performance is monitored.

When service performance is monitored

The detection criteria depend on the service performance measurement count per 60 seconds and the `outlierRate` property value specified in ITSLM - Manager's system definition file (`jp1itslm.properties`). The `outlierRate` property value is applied to out-of-range value detection for all monitored services.

For details about editing the system definition file, see *5.6.1 Editing the system definition files*.

The following table describes the relationship between the `outlierRate` property value and the behavior of out-of-range value detection.

Table 3–2: Relationship between outlierRate property value and the behavior of out-of-range value detection

No.	outlierRate property value (n)	Behavior of out-of-range value detection
1	`1`	An out-of-range value is detected when service performance exceeds the upper-limit value or drops below the lower-limit value even once. When service performance does not exceed the upper-limit value or drop below the lower-limit value over the next 60 seconds, it is determined to have returned to normal.
2	`2` to `98`	An out-of-range value is detected when service performance exceeds the upper-limit value or drops below the lower-limit value $S \times n \div 100$ times (rounded up) in 60 seconds. When the number of times service performance exceeds the upper-limit value or drops below the lower-limit value is less than $S \times n \div 100$ times (rounded up) for 60 seconds, the service performance is determined to have returned to normal.
3	`99` to `100`	An out-of-range value is detected when service performance continues to exceed the upper-limit value or be below the lower-limit value for 60 seconds. When service performance falls within the upper-limit and lower-limit values even once, it is determined to have returned to normal.

Legend:

S: Number of times service performance is measured in 60 seconds

n: `outlierRate` property value specified in ITSLM - Manager's system definition file (`jp1itslm.properties`)

Note that consecutive out-of-range values are checked for those exceeding the upper-limit value separately from those dropping below lower-limit value. This means that an out-of-range value exceeding the upper-limit value followed consecutively by one dropping below the lower-limit value are not detected as consecutive out-of-range values.

The following service performances are not processed as out-of-range value even if they exceed an upper-limit value or drop below a lower-limit value:

- Average response time when average response time and throughput are both `0` (throughput is detected as an out-of-range value)
- Error rate when error rate and throughput are both `0` (throughput is detected as an out-of-range value)

This is because a throughput value of `0` indicates that there is no data. However, for throughput itself, this `0` value indicates the service performance has a processing count of 0. Therefore, the throughput is still detected as an out-of-range value if its value of `0` is above the upper-limit value or below the lower-limit value.

These average response time and error rate are still used as past service performance for baseline calculation because they can be in a normal status even though they were not processed as out-of-range values.

When system performance is monitored

The detection criterion is the number of the most recent measurements that exceed a specified value that generates an event. The number of times exceeded and the number of times measured are specified in **Occurrence**

frequency under **Error Predict. settings** in the **Monitor settings** area of the Settings window. The following table describes the correspondence between the settings and the criterion for detecting an out-of-range value.

Table 3–3: Criterion for detecting an out-of-range value

No.	Occurrence frequency settings	Criterion for detecting an out-of-range value
1	`1` is specified for both times exceeded and times measured	An out-of-range value is detected if performance data for the current time falls beyond the lower or upper limit for predictive error detection.
2	A value other than `1` is specified for either times exceeded or times measured or both	An out-of-range value is detected if the following conditions are both satisfied: • Performance data for the current time falls beyond the lower or upper limit for predictive error detection. • The number of the most recent measurements that fell beyond the lower or upper limit for predictive error detection exceeded the specified value. If the measurement acquisition count is less than the specified measurement count, the performance data has already fallen beyond the lower or upper limit for predictive error detection more times than specified.

The following notes apply to evaluating out-of-range value detection:

- Once a notification is sent, no more notifications are sent until the status returns to normal even if the conditions are satisfied again.
- When monitoring is stopped, the measurement acquisition count and the number of times an excess beyond the upper-limit and lower-limit values occurred are initialized to `0`. When monitoring is restarted, no previous measurement values obtained before monitoring was stopped are used for new detection.
- If no measurement value was obtained at a given time due to an error, that time is ignored and as many available most recent measurement values as needed for the specified detection are used.
- If no past data for baseline calculation is available at the time detection is checked, that time is treated as normal (neither the upper nor the lower limit has been exceeded).

(4) Criteria for determining that performance has returned to normal

This subsection explains for service performance and for system performance the criteria for determining that performance has returned to normal since it exceeded the upper-limit value or dropped below the lower-limit value.

When service performance is monitored

Performance is determined to have returned to normal when service performance did not exceed the upper-limit value or drop below the lower-limit value more than $S \times n \div 100$ times (rounded up) for the past 60 seconds.

S indicates the number of times service performance was measured in 60 seconds. *n* indicates the `outlierRate` property value specified in ITSLM - Manager's system definition file (`jp1itslm.properties`).

For details about editing the system definition file, see *5.6.1 Editing the system definition files*.

For example, if *S* is 60 and *n* is 10, performance is determined to have returned to normal when the number of times service performance exceeded the upper-limit value or dropped below the lower-limit value is less than 6. The upper-limit value and lower-limit value are checked separately. When both return to normal, performance is determined to have returned to normal. Recovery of performance is not detected from transient values that approach the baseline.

When system performance is monitored

The criterion for determining that performance has returned to normal depends on the value specified in **Occurrence frequency** for the monitored service under **Error Predict. settings** in the **Monitor settings** area of the Settings window.

For details about setting **Occurrence frequency** under **Error Predict. settings**, see *3.2.8 Setting up the monitoring items for system performance (working with Performance Management)*.

The following table explains the correspondence between the specifiable values and the criterion for determining that performance has recovered.

Table 3–4: Criterion for determining that performance has returned to normal since it exceeded the upper-limit value or dropped below the lower-limit value

No.	Occurrence frequency values under Error Predict. settings	Criterion for determining recovery
1	`1` is specified for both *M* and *N*	Performance is determined to have returned to normal when the performance data for the current time is not above the upper-limit value or below the lower-limit value.
2	A value other than `1` is specified for either *M* or *N* or for both	Performance is determined to have returned to normal when the number of times the most recent *M* measurement values exceeded the upper-limit value for predictive error detection is less than *N* and the number of times they dropped below the lower-limit value is less than *N*. When the measurement acquisition count is less than *M*, performance is determined to have returned to normal when the number of times all the measurement values obtained so far exceeded the upper-limit value for predictive error detection is less than *N* and the number of times they dropped below the lower-limit value is less than *N*.

Legend:

M: Number of measurements taken as specified for **Occurrence frequency** (**measured**) under **Error Predict. settings**

N: Number of times a measured value is allowed to exceed the limit as specified for **Occurrence frequency** (**Times exceeded**) under **Error Predict. settings**

Recovery is determined when the values of the reported monitoring items are updated. Therefore, determination of recovery takes place in the interval during which information about the corresponding monitoring items is acquired.

You can check the recovery status in the Home or Real-time Monitor window. For details about how to check the Home window, see *4.3.1 Checking the status of the monitored services of all service groups*. For details about how to check the Real-time Monitor window, see *4.3.2 Checking the status of the monitored services in a specific service group*.

(5) Supplementary information

- With respect to accumulation of service performance data for baseline calculation, a day when there was no measurement of service performance over some time period but there was at least one measurement of service performance during that day is counted as a day for which service performance has been accumulated. Therefore, the baseline might not be displayed for certain time periods because there is not enough service performance data available for baseline calculation.
- When out-of-range value detection is started for service performance depends on whether the number of days' worth of data specified in the Settings window has been accumulated. The following explains when out-of-range value detection is started.
  - If the number of days, excluding the current day, for which service performance has been accumulated is equal to or greater than the value specified for **Days till start** under **Error Predict. settings**, out-of-range value detection begins when at least 60 seconds have elapsed since the time ITSLM - UR acquired service performance for the first time after monitoring started.
  - If the number of days, excluding the current day, for which service performance has been accumulated is less than the value specified for **Days till start** under **Error Predict. settings**, out-of-range value detection begins at or after 00:00:00 on the day the number of days, excluding the current day, for which service performance has been accumulated reaches the value specified for **Days till start**.
- When out-of-range value detection is started for system performance depends on whether the number of days' worth of data specified in the Settings window has been accumulated. The following explains when out-of-range value detection is started.
  - If the number of days, excluding the current day, for which system performance has been accumulated is equal to or greater than the value specified for **Days till start** under **Error Predict. settings**, out-of-range value

detection begins at the time PFM - Agent or PFM - RM acquires system performance for the first time since monitoring started.

  - If the number of days, excluding the current day, for which system performance has been accumulated is less than the value specified for **Days till start** under **Error Predict. settings**, out-of-range value detection begins at or after 00:00:00 on the day the number of days, excluding the current day, for which system performance has been accumulated reaches the value specified for **Days till start**.

- In the case of a monitoring item whose system performance collection interval is long, the accuracy of the baseline, the upper-limit value, and the lower-limit value might be low because the amount of data for the past hour is small. To improve accuracy, reduce the collection interval in Performance Management or increase the number of days used for baseline calculation so as to increase the amount of past data available to be used.
- If predictive error detection is performed using a monitoring item whose collection interval is 24 hours or more, the data acquired immediately before the most recent data is not used for baseline calculation. Therefore, set the collection interval for monitoring items used for predictive error detection to less than 24 hours in Performance Management.
- If monitoring is stopped and not restarted until more than 24 hours later, the data obtained in the last minute before the stoppage might not be used for baseline calculation. You can correct this situation by performing monitoring for one hour or more continuously or stop monitoring once and then start it again.

(6) Related topics

- *3.2.7 Setting up the monitoring items for service performance*
- *3.2.8 Setting up the monitoring items for system performance (working with Performance Management)*
- *4.3.1 Checking the status of the monitored services of all service groups*

3.1.3 Using trend monitoring for detection in advance of threshold overages

Trend monitoring monitors each monitoring item. For details about the monitoring items, see *3.1.1 ITSLM's monitoring methods and types of monitored targets*. Note that trend monitoring is not applicable to error rate.

This subsection explains trend monitoring.

(1) About trend monitoring

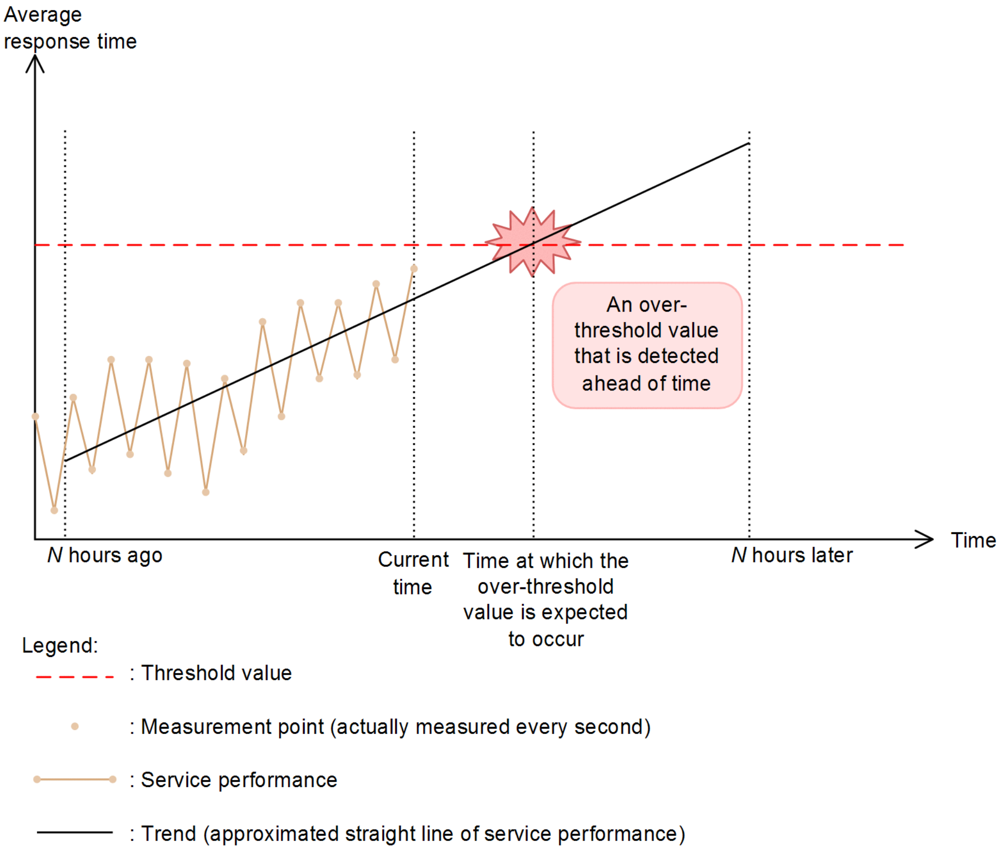
Trend monitoring calculates trends in the performance trends of monitored services and detects in advance possible overages of a service performance threshold.

A *trend* is an approximated straight line obtained from current service performance. An approximated straight line is calculated on the basis of the past *N* hours of service performance. If this approximated straight line exceeds the threshold within *N* hours from the present time, this event is detected as a warning sign of a potential service performance error. The value of *N* is specified in the Settings window.

For details about how to specify numeric values in the Settings window, see *3.2.7 Setting up the monitoring items for service performance*.

The following shows an example in which an overage of a threshold is detected ahead of time by trend monitoring.

Figure 3–15: Example in which an overage of a threshold is detected ahead of time



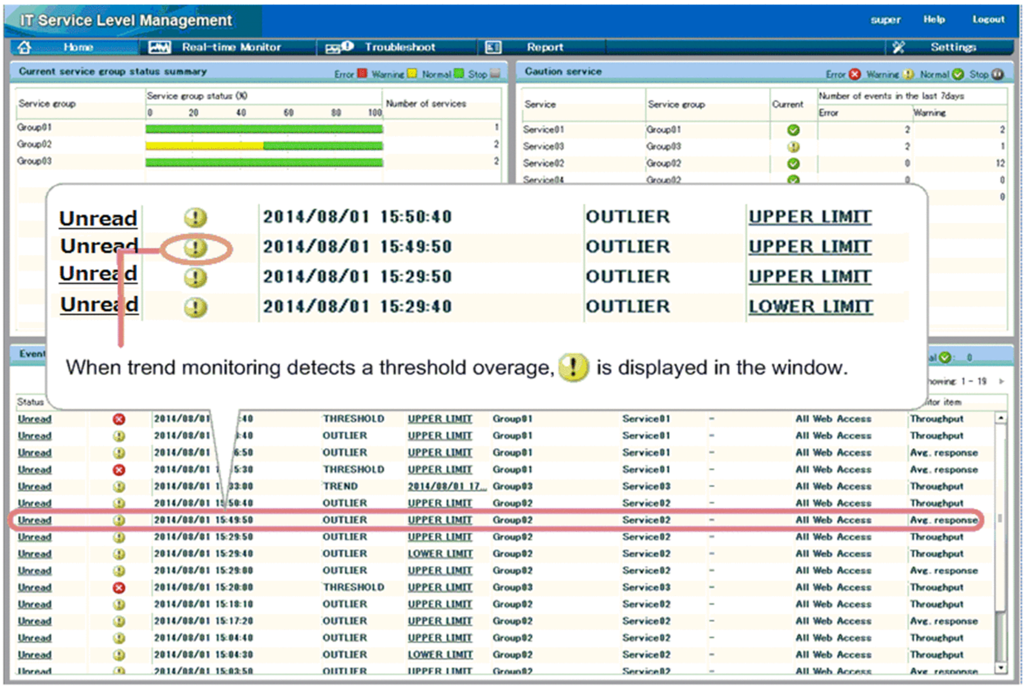
This example monitors average response time. The trend is calculated from the past *N* hours of service performance. A warning sign is detected if the service performance is predicted to exceed the threshold within the next *N* hours.

To obtain a trend for predicting an overage of a threshold within *N* hours, *N* hours' worth of service performance is required. This reduces the error associated with a long period of trend monitoring. To predict an overage of a threshold during the next hour, one hour's worth of service performance is required.

The approximated straight line is updated every 60 seconds and each time this occurs a check is performed to see if an overage of the threshold might occur. If an overage of the threshold is predicted, a warning is displayed in the window.

The following shows an example of a warning displayed in the window.

Figure 3–16: Example of a warning displayed in the window (trend monitoring)



IT Service Level Management

super Help Logout

Home | Real-time Monitor | Troubleshoot | Report | Settings

Current service group status summary

Error 🟥 Warning 🟨 Normal 🟩 Stop ▨

Service group	Service group status (%) 0 20 40 60 80 100	Number of services
Group01		1
Group02		2
Group03		2

Caution service

Error ✕ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
				0

Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT

When trend monitoring detects a threshold overage, ! is displayed in the window.

Event

...al ✓ : 0

...howing 1 - 19 ▸

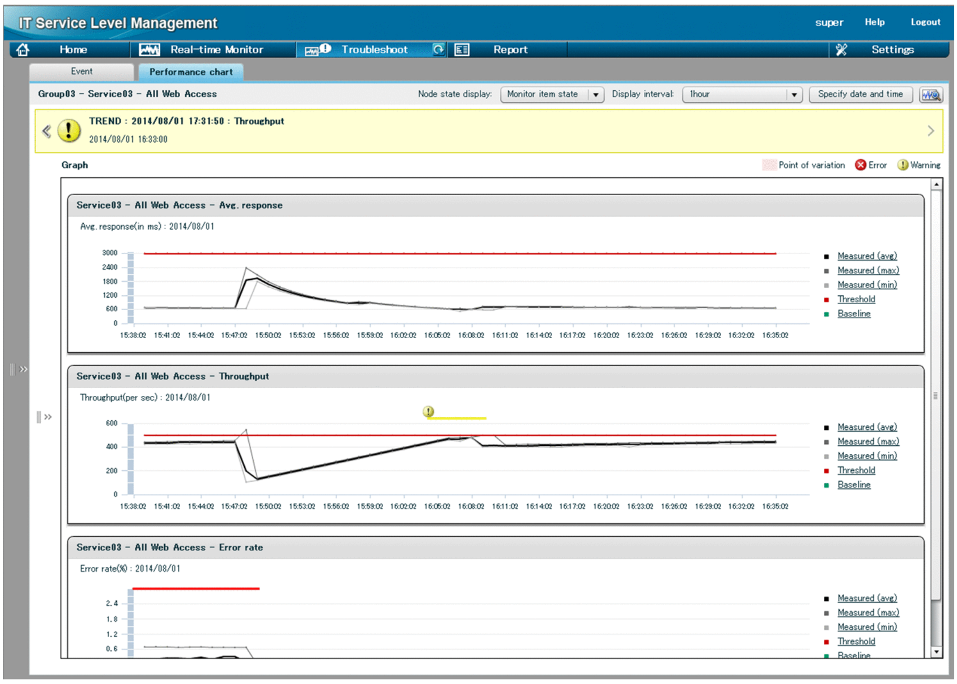
Status									...itor item
Unread	✕	2014/08/01 :40	THRESHOLD	UPPER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!	2014/08/01 :40	OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!	2014/08/01 6:50	OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	✕	2014/08/01 1 5:30	THRESHOLD	UPPER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	!	2014/08/01 1 33:00	TREND	2014/08/01 17...	Group03	Service03	-	All Web Access	Throughput
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response
Unread	✕	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	-	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response

zu030360.vsd／J:¥Hitachi¥2014Jobs¥490911_311¥60_DTP¥VSD¥／／2014/10/29／2:28／

The information displayed in the window includes a warning icon, the detection date and time, the time at which service performance is predicted to exceed the threshold, the name of the service group subject to the warning, and the service name. If the trend keeps exceeding the threshold, a warning is displayed only the first time the trend is detected. You can view the service performance leading up to and following the point of the warning as a graph.

The following shows an example of a graph that is displayed.

Figure 3–17: Example of a graph that is displayed (trend monitoring)



In the graph, a warning icon indicates the time the threshold would be exceeded and a colored belt indicates the time period during which the event resulting in the overage of the threshold is assumed to occur.

To run trend monitoring, you must specify the following items in the Settings window:

- Threshold
- Reference time for calculating trends

Threshold

Specifies the reference threshold that is to be used to determine the status of the monitored service.

Reference time for calculating trends

Specifies *N* hours as the reference time for calculating trends. *N* hours are used as follows:

- A trend is calculated on the basis of the past *N* hours of service performance.
- A warning sign is detected if an overage of a threshold is predicted to occur within *N* hours from the present time.

When linking with Performance Management

If you link ITSLM with Performance Management, you can also run trend monitoring for system performance. In trend monitoring for system performance, there are two types of monitoring items:

- Monitoring item to be reported when it exceeds the threshold
- Monitoring item to be reported when it drops below the threshold

You can determine which type applies to a monitoring item by checking the **Monitor settings** area in the Settings window. If the icon in the **Threshold** column is ⬆, the monitoring item is reported when it exceeds the threshold. If the icon in the **Threshold** column is ⬇, the monitoring item is reported when it drops below the threshold.

(2) Detection criteria

In trend monitoring, a warning is detected if the calculated trend is flat or uptrending and satisfies one of the following conditions:

- The trend is currently already above the threshold

  The time that is displayed in **Details** for the reported warning event is the current time.
- The trend indicates that the threshold will be reached or exceeded within *N* hours

  The time that is displayed in **Details** for the reported warning event is the time the overage of the threshold is predicted to occur.

The value of *N* is specified in the Settings window.

For details about how to specify numeric values in the Settings window, see *3.2.7 Setting up the monitoring items for service performance*.

In the case of a downward trend, no warning is detected even if the current trend exceeds the threshold because such a trend might be indicative of recovery.

To maintain accuracy, a trend is calculated only when a condition is satisfied. The criteria for calculating a trend when service performance is being monitored differs from when system performance is being monitored. The following explains both cases.

When service performance is monitored

A trend is calculated when the following condition is satisfied:

- Total amount of time over the past *N* hours during which service performance was collected (seconds) ≥ *N* × 3,600 × 30 ÷ 100 (seconds)

For example, if the value of *N* is 5, 5 × 3,600 × 30 ÷ 100 = 5,400 (seconds), which is 90 minutes. If at least 90 minutes' worth of service performance has been collected, a trend is calculated and trend monitoring is run.

When system performance is monitored

A trend is calculated when the following criteria are both satisfied:

- Total amount of time over the past *N* hours during which service performance was collected (seconds) ≥ *N* × 3,600 × 30 ÷ 100 (seconds)
- At least two performance data items have been collected during the past *N* hours.

For example, if the value of *N* is 5, 5 × 3,600 × 30 ÷ 100 = 5,400 (seconds), which is 90 minutes. If at least 90 minutes' worth of service performance has been collected and at least two performance data items have been collected, a trend is calculated and trend monitoring is run.

(3) Criteria for determining that performance has returned to normal

This subsection explains the criteria for determining that performance has returned to normal.

Monitoring items for upper-limit threshold value

If any of the following conditions is true, the trend monitoring status returns to normal.

- The trend will no longer exceed the threshold *N* hours from now.
- The trend is downtrending.
- The trend is currently below the threshold and will no longer exceed the threshold in the next *N* hours.

Monitoring items for lower-limit threshold value

If any of the following conditions is true, the trend monitoring status returns to normal.

- The trend will no longer exceed the threshold *N* hours from now.
- The trend is uptrending.
- The trend is currently above the threshold and will no longer be below the threshold in the next *N* hours.

The value of *N* is specified in the Settings window.

For details about how to specify numeric values in the Settings window, see *3.2.7 Setting up the monitoring items for service performance*.

Note that a monitored service is placed in warning status when a warning is reported for it in ITSLM's Home or Real-time Monitor window, and such a monitored service will remain in warning status until it recovers to normal status. A trend monitoring notification for the same monitoring item for the same monitored service is suppressed. Therefore, when an overage of a threshold is detected by trend monitoring, the warning status remains displayed for at least 60 seconds after the notification.

(4) Supplementary information

- If an overage of a threshold is currently already detected by threshold value monitoring, it will not be detected by trend monitoring.
- The following service performance is not used for calculation of a trend:
  - If monitoring was stopped once and restarted within *N* hours, the service performance existing before monitoring was restarted
  - Service performance existing when average response time and throughput were both 0

  The value of *N* is specified in the **Monitor settings** area of the Settings window.

  For details about how to specify numeric values in the Settings window, see *3.2.7 Setting up the monitoring items for service performance*.
- If service performance data that is not used for trend monitoring continues to exist after a warning was detected, such as when a condition where throughput and average response time are both 0 continues after an overage of a threshold was detected by trend monitoring for average response time, it might take time for the monitored service resulting in the warning to return to its normal status because there is no additional data to change the trend.
- If the value of *N* specified in the Monitor settings window is less than the collection interval for that monitoring item, the required number of performance data items (minimum of two) cannot be acquired within the trend monitoring time even if trend monitoring is set to be run. In such a case, trend monitoring is not run because an approximated straight line cannot be created.

(5) Related topics

- *3.2.7 Setting up the monitoring items for service performance*
- *4.3.1 Checking the status of the monitored services of all service groups*

3.1.4 Using threshold value monitoring for detection of threshold overages

Threshold value monitoring monitors each monitoring item. For details about the monitoring items, see *3.1.1 ITSLM's monitoring methods and types of monitored targets*.

This subsection explains threshold value monitoring.

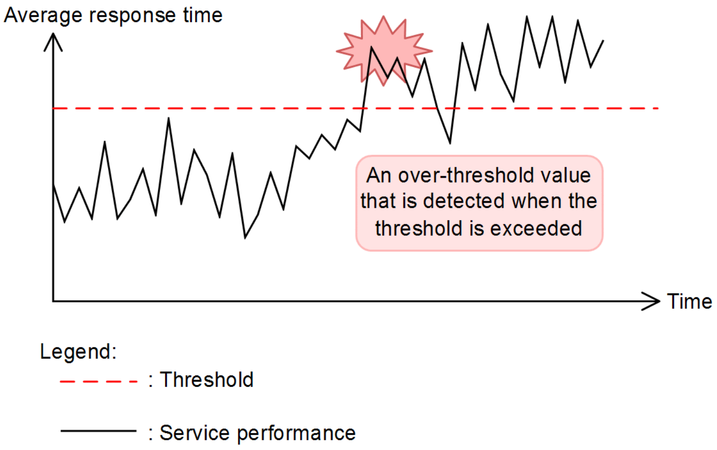
(1) About threshold value monitoring

Threshold value monitoring detects an overage of the threshold set for the performance of a monitored service.

If an SLO has been defined, you can detect an overage of the SLO value by specifying the SLO value as the threshold. If no SLOs have been defined, you can detect an overage of some criterion assumed for service performance by specifying for the threshold a value representing the criterion.

The following shows an example in which an overage of a threshold is detected by threshold value monitoring.

Figure 3–18: Example in which an overage of a threshold is detected

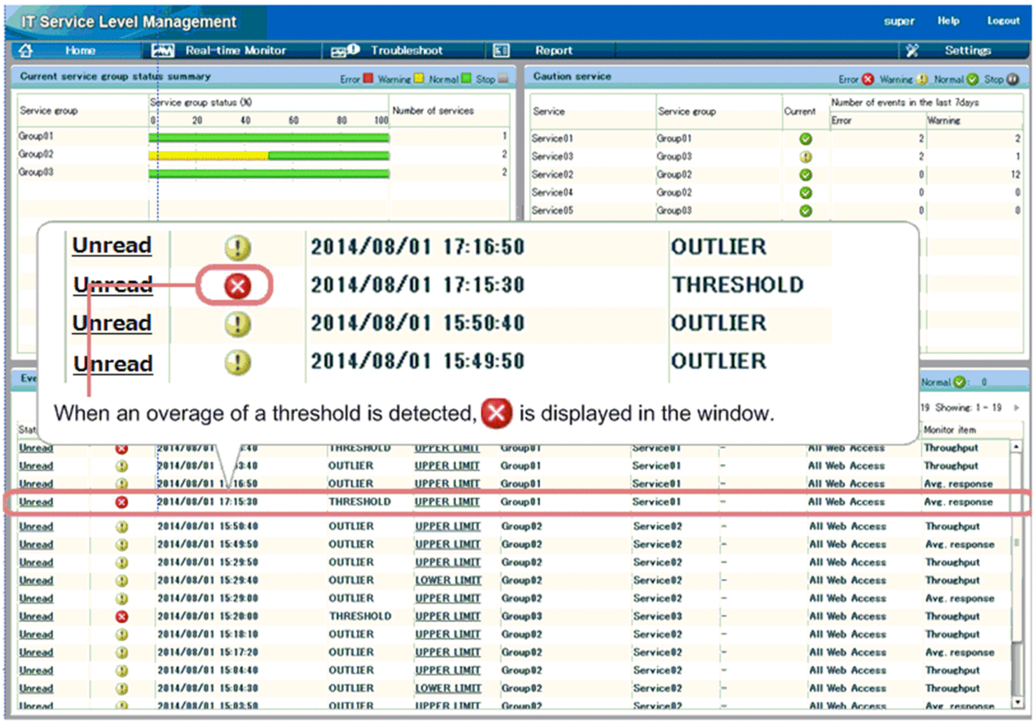


This example monitors average response time. As time passed, the service performance value increased until an overage of the threshold was detected.

When an overage of a threshold is detected, an error is displayed in the window.

The following shows an example in which an error is displayed in the window.

Figure 3–19: Example in which an error is displayed in the window (threshold value monitoring)



IT Service Level Management
super
Help
Logout
Home
Real-time Monitor
Troubleshoot
Report
Settings
Current service group status summary
Error 🟥 Warning 🟨 Normal 🟩 Stop ▨
Caution service
Error Warning Normal Stop

Service group	Service group status (%)	Number of services
Group01		1
Group02		2
Group03		2

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
Service05	Group03	✓	0	0

Unread	!	2014/08/01 17:16:50	OUTLIER
Unread	✕	2014/08/01 17:15:30	THRESHOLD
Unread	!	2014/08/01 15:50:40	OUTLIER
Unread	!	2014/08/01 15:49:50	OUTLIER

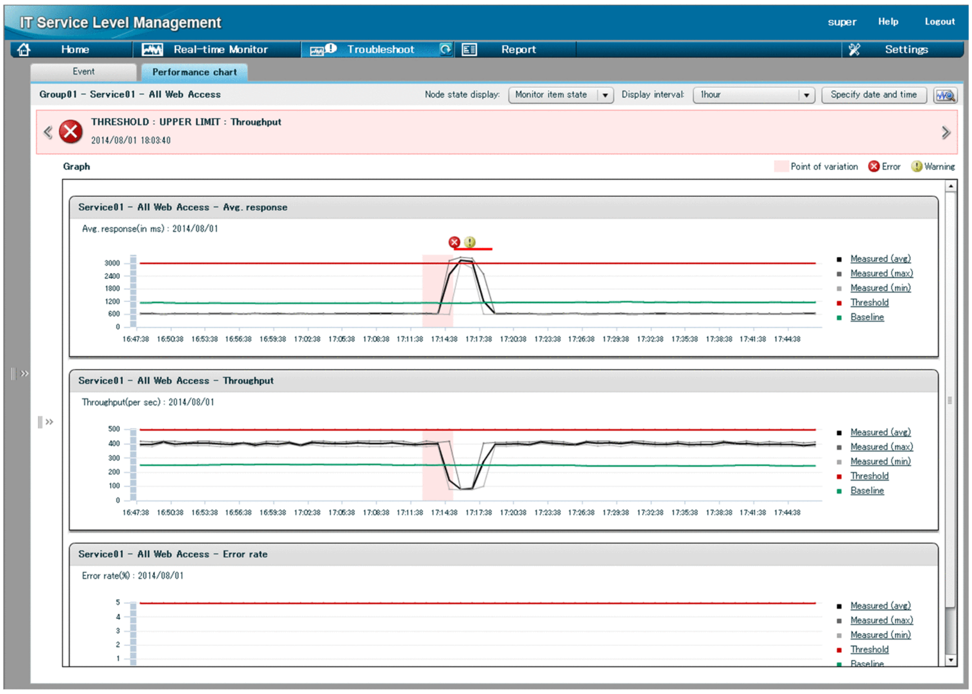
When an overage of a threshold is detected, ✕ is displayed in the window.

Stat									Monitor item
Unread	✕		THRESHOLD	UPPER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!		OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!		OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	✕	2014/08/01 17:15:30	THRESHOLD	UPPER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response
Unread	✕	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	-	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	-	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	-	All Web Access	Avg. response

The information displayed in the window includes an error icon, the detection date and time, the name of the service group subject to the error, and the service name. If service performance keeps exceeding the threshold, an error is displayed only the first time overage of the threshold is detected. You can view the service performance leading up to and following the displayed error in a graph.

The following shows an example of a graph that is displayed.

Figure 3–20: Example of a graph that is displayed (threshold value monitoring)



Group01 - Service01 - All Web Access

Node state display: Monitor item state ▾ Display interval: 1hour ▾ Specify date and time

THRESHOLD : UPPER LIMIT : Throughput
2014/08/01 18:03:40

In the graph, an error icon indicates the time the threshold was exceeded and a colored bar indicates the time period during which the event resulting in the overage of the threshold is assumed to have occurred.

To run threshold value monitoring, you must specify the following item in the Settings window:

Threshold

Specifies the reference threshold that is to be used to determine the status of the monitored service.

When linking with Performance Management

If you link ITSLM with Performance Management, you can also run threshold value monitoring for system performance. In threshold value monitoring for system performance, there are two types of monitoring items:

- Monitoring item to be reported when it exceeds the threshold
- Monitoring item to be reported when it drops below the threshold

You can determine which type applies to a monitoring item by checking the **Monitor settings** area in the Settings window. If the icon in the **Threshold** column is ⤒ , the monitoring item is reported when it exceeds the threshold. If the icon in the **Threshold** column is ⤓ , the monitoring item is reported when it drops below the threshold.

(2) Detection criteria

In threshold value monitoring, an overage of the threshold is detected if the overage persists, so as to avoid detecting a transient overage of the threshold. This subsection explains the criteria for detecting an overage of the threshold when service performance is monitored and when system performance is monitored.

When service performance is monitored

The detection criteria depend on the service performance measurement count per 60 seconds and the `sloThresholdRate` property value specified in ITSLM - Manager's system definition file (`jp1itslm.properties`). The `sloThresholdRate` property value is applied to threshold value monitoring for all monitored services.

For details about editing the system definition file, see *5.6.1 Editing the system definition files*.

The following table describes the relationship between the `sloThresholdRate` property value and the behavior of threshold value monitoring

Table 3–5: Relationship between `sloThresholdRate` property value and the behavior of threshold value monitoring

No.	sloThresholdRate property value (n)	Behavior of threshold value monitoring
1	`1`	An overage of the threshold is detected when service performance exceeds the threshold even once. When service performance no longer exceeds the threshold, it is determined to have returned to normal.
2	`2` to `98`	An overage of the threshold is detected when service performance exceeds the threshold $S \times n \div 100$ times (rounded up) in 60 seconds. When the number of times service performance exceeds the threshold is less than $S \times n \div 100$ times (rounded up) in 60 seconds, service performance is determined to have returned to normal.
3	`99` to `100`	An overage of the threshold is detected when service performance continues to exceed the threshold for 60 seconds. When service performance falls below the threshold even once, it is determined to have returned to normal.

Legend:

S: Number of times service performance is measured in 60 seconds

n: `sloThresholdRate` property value specified in ITSLM - Manager's system definition file (`jp1itslm.properties`)

When system performance is monitored

The detection criterion is the number of the most recent measurements that exceed a specified value that generates an event. The number of times exceeded and the number of times measured are specified in **Occurrence frequency** under **SLO monitor settings** in the **Monitor settings** area of the Settings window. The following table describes the correspondence between the settings and the criterion for detecting an overage beyond the threshold.

Table 3–6: Criterion for detecting an overage of the threshold

No.	Occurrence frequency settings	Criterion for detecting an excess beyond the threshold
1	`1` is specified for both times exceeded and times measured	An overage of the threshold is detected when performance data for the current time exceeds the threshold.
2	A value other than `1` is specified for either times exceeded or times measured or both	An overage of the threshold is detected when the following conditions are both satisfied: • Performance data for the current time exceeds the threshold. • The specified number of measurements exceed the threshold more times than specified. If the measurement acquisition count is less than the specified measurement count, the performance data has already exceeded the threshold more times than specified.

The following notes apply to evaluating detection of overages of the threshold:

- Once a notification is sent, no more notifications are sent until the status returns to normal even if the conditions are satisfied again.
- When monitoring is stopped, the measurement acquisition count and the number of times an overage of the threshold occurred are initialized to `0`. When monitoring is restarted, no previous measurement values obtained before monitoring was stopped are used for new detection.
- If no measurement value was obtained at a given time due to an error, that time is ignored and as many available most recent measurement values as needed for the specified detection are used.

(3) Criteria for determining that performance has returned to normal

This subsection explains for service performance and for system performance the criteria for determining that performance has returned to normal since it exceeded the threshold.

When service performance is monitored

Performance is determined to have returned to normal when service performance did not exceed the threshold more than $S \times n \div 100$ times (rounded up) for the past 60 seconds.

S indicates the number of times service performance was measured in 60 seconds. *n* indicates the `sloThresholdRate` property value specified in ITSLM - Manager's system definition file (`jp1itslm.properties`).

For details about editing the system definition file, see *5.6.1 Editing the system definition files*.

For example, if *S* is 60 and *n* is 10, performance is determined to have returned to normal when the number of times service performance exceeded the threshold is less than 6. Recovery of performance is not detected from transient values that are smaller than the threshold.

When system performance is monitored

The criterion for determining that performance has returned to normal after exceeding the threshold depends on the value specified in **Occurrence frequency** for the monitored service under **SLO monitor settings** in the **Monitor settings** area of the Settings window.

For details about setting **Occurrence frequency** under **SLO monitor settings**, see *3.2.8 Setting up the monitoring items for system performance (working with Performance Management)*.

The following table explains the correspondence between the specifiable values and the criterion for determining that performance has recovered.

Table 3–7: Criterion for determining that performance has returned to normal after it exceeded the threshold

No.	Occurrence frequency values	Criterion for determining recovery
1	`1` is specified for both *M* and *N*	Performance is determined to have returned to normal when the performance data for the current time does not exceed the threshold.
2	A value other than `1` is specified for either *M* or *N* or for both	Performance is determined to have returned to normal when the number of times the most recent *M* measurement values exceeded the threshold is less than *N*. When the measurement acquisition count is less than *M*, performance is determined to have returned to normal if the number of times all the measurement values obtained so far exceeded the threshold is less than *N*.

Legend:

M: Number of measurements taken as specified for **Occurrence frequency** (**measured**) under **SLO monitor settings**

N: Number of times a measured value is allowed to exceed the limit as specified for **Occurrence frequency** (**Times exceeded**) under **SLO monitor settings**

Recovery is determined when the values of the reported monitoring items are updated. Therefore, determination of recovery takes place in the interval during which information about the corresponding monitoring item is acquired.

You can check the recovery status in the Home or Real-time Monitor window. For details about how to check the Home window, see *4.3.1 Checking the status of the monitored services of all service groups*. For details about how to check the Real-time Monitor window, see *4.3.2 Checking the status of the monitored services in a specific service group*.

(4) Supplementary information

- Threshold value monitoring for service performance begins 60 seconds after ITSLM - UR collects the first service performance data after monitoring starts.
- Threshold value monitoring for system performance begins immediately after PFM - Agent or PFM - RM collects the first system performance data after monitoring starts.

(5) Related topics

- *3.2.7 Setting up the monitoring items for service performance*
- *3.2.8 Setting up the monitoring items for system performance (working with Performance Management)*
- *4.3.1 Checking the status of the monitored services of all service groups*

3.1.5 Using availability monitoring for checking the availability of services (working with Performance Management)

Availability monitoring is supported when ITSLM is linked with Performance Management.

This subsection explains availability monitoring.

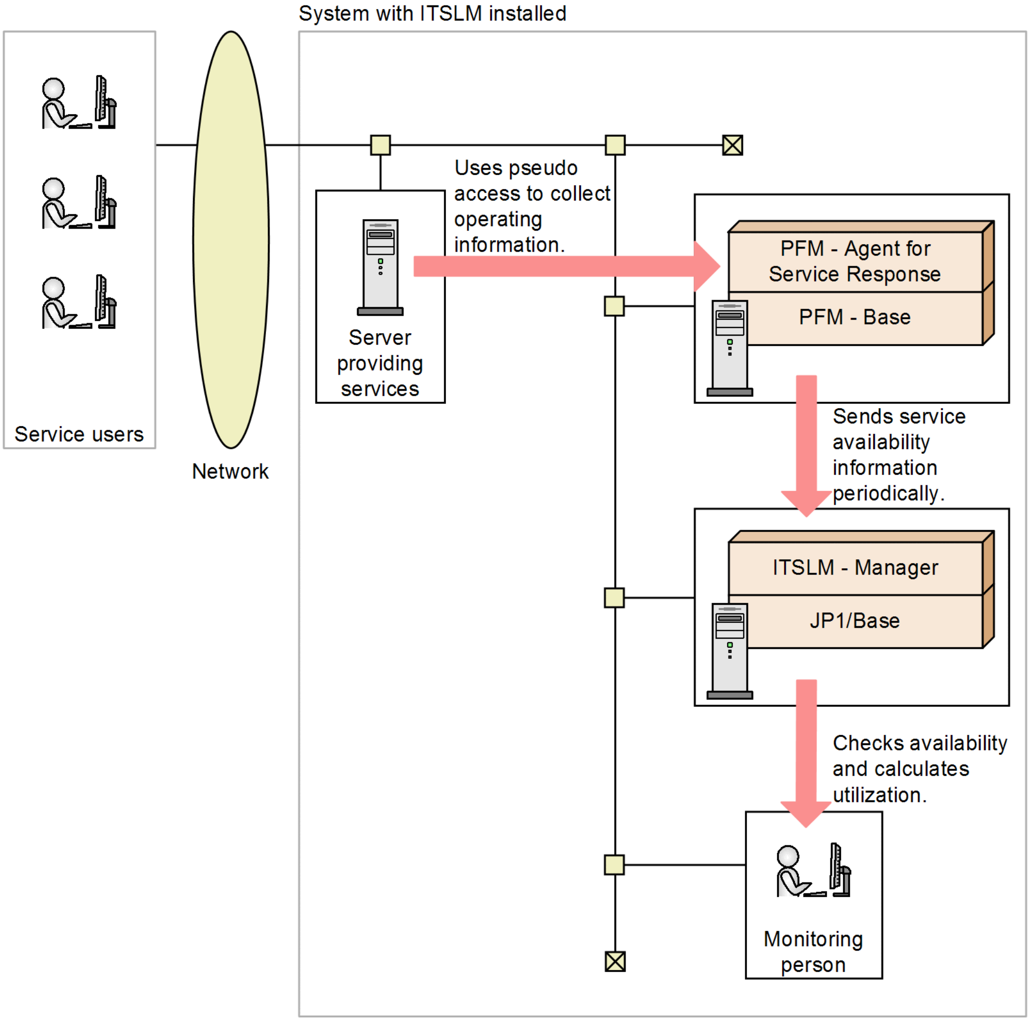
(1) About availability monitoring

Availability monitoring is a method for checking whether monitored services are running smoothly.

PFM - Agent for Service Response is used for monitoring the availability of monitored services. You can monitor the availability of monitored services even when no users are accessing them.

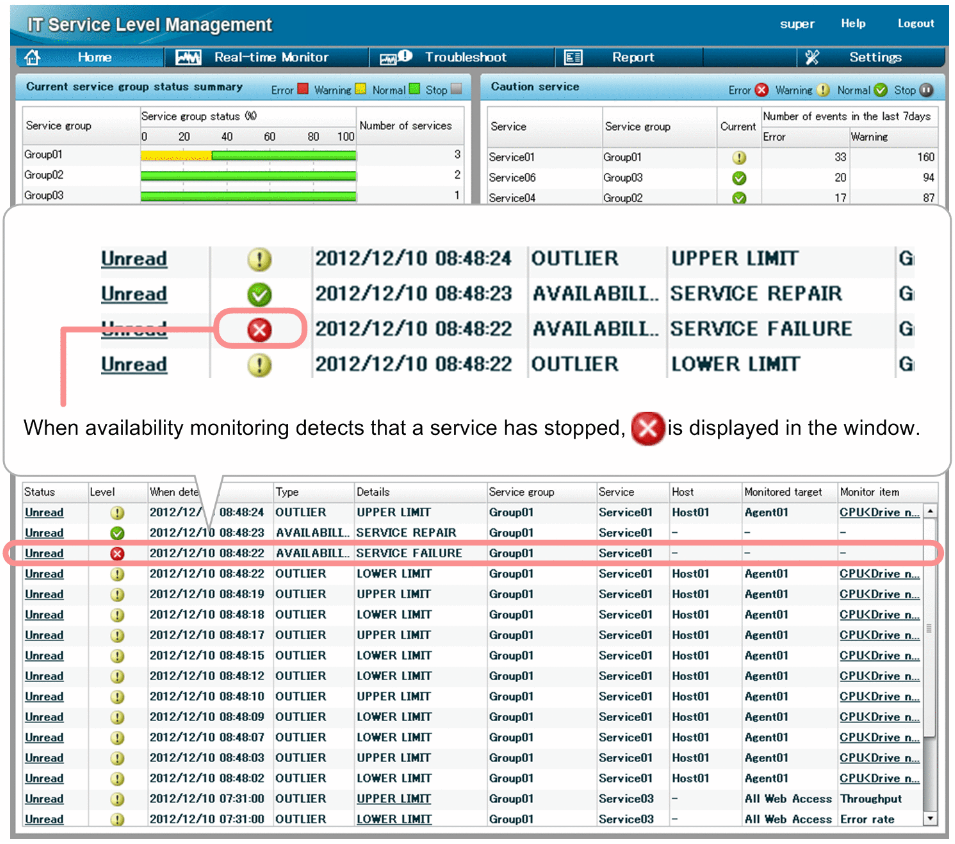
The following figure shows how availability monitoring works.

Figure 3–21: How availability monitoring works


System with ITSLM installed
Service users
Network
Uses pseudo access to collect operating information.
Server providing services
PFM - Agent for Service Response
PFM - Base
Sends service availability information periodically.
ITSLM - Manager
JP1/Base
Checks availability and calculates utilization.
Monitoring person

You can check the current availability of services in the Home window or the Real-time Monitor window. If a monitored service has stopped, an error is displayed in these windows. The following shows an example in which an error is displayed in a window.

Figure 3–22: Example in which an error is displayed in a window (availability monitoring)



Current service group status summary   Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%) 0 20 40 60 80 100	Number of services
Group01		3
Group02		2
Group03		1

Caution service   Error ✗ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	!	33	160
Service06	Group03	✓	20	94
Service04	Group02	✓	17	87

Unread	!	2012/12/10 08:48:24	OUTLIER	UPPER LIMIT	G
Unread	✓	2012/12/10 08:48:23	AVAILABILL..	SERVICE REPAIR	G
Unread	✗	2012/12/10 08:48:22	AVAILABILL..	SERVICE FAILURE	G
Unread	!	2012/12/10 08:48:22	OUTLIER	LOWER LIMIT	G

When availability monitoring detects that a service has stopped, ✗ is displayed in the window.

Status	Level	When dete	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	!	2012/12/ 08:48:24	OUTLIER	UPPER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	✓	2012/12/10 08:48:23	AVAILABILL..	SERVICE REPAIR	Group01	Service01	–	–	–
Unread	✗	2012/12/10 08:48:22	AVAILABILL..	SERVICE FAILURE	Group01	Service01	–	–	–
Unread	!	2012/12/10 08:48:22	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:19	OUTLIER	UPPER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:18	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:17	OUTLIER	UPPER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:15	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:12	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:10	OUTLIER	UPPER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:09	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:07	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:03	OUTLIER	UPPER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 08:48:02	OUTLIER	LOWER LIMIT	Group01	Service01	Host01	Agent01	CPU<Drive n...
Unread	!	2012/12/10 07:31:00	OUTLIER	UPPER LIMIT	Group01	Service03	–	All Web Access	Throughput
Unread	!	2012/12/10 07:31:00	OUTLIER	LOWER LIMIT	Group01	Service03	–	All Web Access	Error rate

(2) Availability items that can be output to reports

For the monitored services whose availability is being monitored, you can output *availability items* to reports. The availability items are metrics used to evaluate availability. Availability monitoring enables you to output the following availability items to reports:

- Service availability
- MTTR (mean time to recovery)
- MTBF (mean time between failures)

The following table provides details about the availability items that can be output to reports by availability monitoring.

Table 3–8: Definition of availability items and formulas

No.	Evaluation metric (SLO)	Definition	Formula
1	Service availability	Percentage of the time during the report interval that the service was running	Service availability (%) = $A \div (A + B) \times 100$ A = Total operational period during the report interval (minutes) B = Total error period during the report interval (minutes)
2	MTTR (mean time to recovery)	Average time required from the occurrence of an error to recovery from the error during the report interval	Mean time to recovery (minutes) = B/C B = Total error period during the report interval (minutes) C = Number of times errors occurred during the report interval
3	MTBF (mean time between failures)	Average time from one error recovery to the occurrence of the next error during the report interval	Mean time between failures (minutes) = A/C A = Total operational period during the report interval (minutes) C = Number of times errors occurred during the report interval

Legend:

Report interval: Total length of time subject to reporting that is obtained from the start time and period entered by the user in the **Report** area of the Report window.

Operational period: Period from the time normal operation of the monitored service was verified to the time a stoppage of the monitored service was detected or monitoring was stopped.

Error period: Period from the time a stoppage of the monitored service was detected to the time normal operation of the monitored service was verified or monitoring was stopped

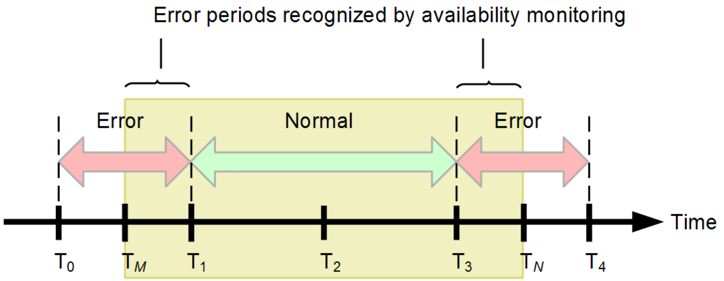
The following explains for three cases how availability items are calculated by availability monitoring.

- Case where the monitored service is stopped at the time reporting begins or at the time reporting ends

  If the time the monitored service stopped due to an error was before the report start time, the report start time is used as the time the monitored service stopped for purpose of calculating the availability items.

  If a stopped monitored service is still stopped at the report end time, the report end time is used as the time the monitored service stopped for purpose of calculating the availability items.

  The following figure shows an example in which the monitored service is already stopped at the report start time and is stopped at the report end time.



  Legend: 🟨 : Report interval

  T_0 to T_4 : Points in time monitoring was performed

  T_M: Report start time

  T_N: Report end time

  The availability items for this example are calculated as follows:

  Service availability = $(T_3 - T_1)/\{(T_3 - T_1) + (T_1 - T_M) + (T_N - T_3)\}$

  = $(T_3 - T_1)/(T_N - T_M)$

  Mean time to recovery = $\{(T_1 - T_M) + (T_N - T_3)\}/2$

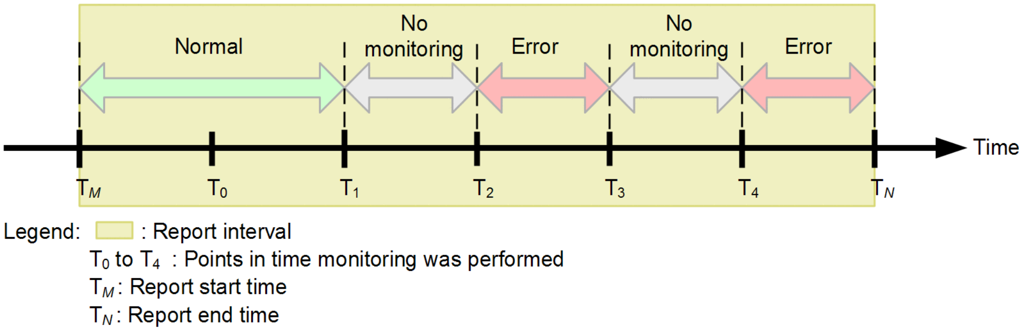
  Mean time between failures = $(T_3 - T_1)/2$

- Case where the report interval contains periods of time during which monitoring is not performed

  If the report creation interval contains within it periods of time during which monitoring is not performed, those periods are not included in the calculation of availability items because availability is not checked during those periods.

  If an error period contains within it a period of time during which monitoring is not being performed, that error period is treated as two error periods separated by the interval when monitoring was not being performed.

  The following figure shows an example in which the report interval contains periods of time during which monitoring is not performed.



The availability items for this example are calculated as follows:

Service availability = $(T_1 - T_M)/\{(T_1 - T_M) + (T_3 - T_2) + (T_N - T_4)\}$

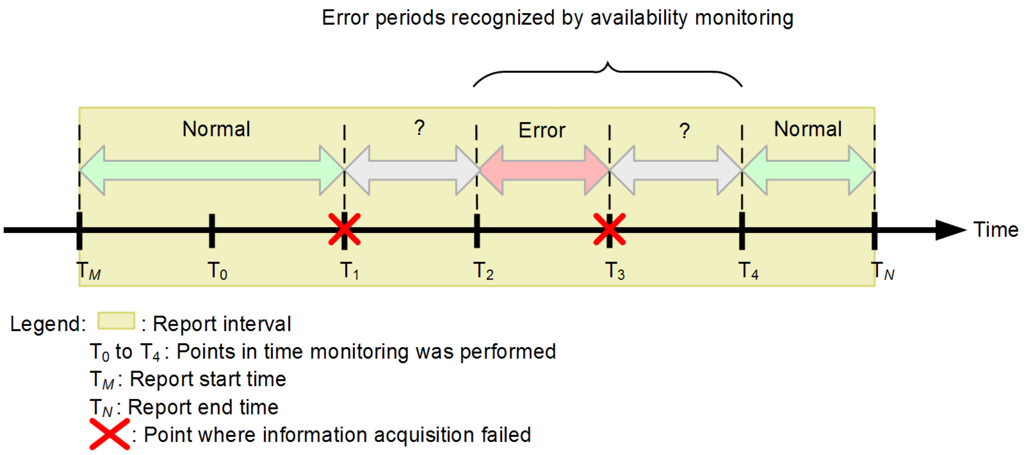
Mean time to recovery = $\{(T_3 - T_2) + (T_N - T_4)\}/2$

Mean time between failures = $(T_1 - T_M)/2$

- Case where the report interval contains periods of time during which information acquisition failed

  If availability information cannot be acquired for a period of time during monitoring because a communication error occurred or because PFM - Agent for Service Response was not running, the availability acquired from PFM - Agent for Service Response immediately before the interval for which there is no availability information is assumed to continue.

  The following figure shows an example in which the report interval contains periods of time during which information acquisition failed:


Error periods recognized by availability monitoring
Normal
?
Error
?
Normal
Time
T_M
T_0
T_1
T_2
T_3
T_4
T_N
Legend: ▭ : Report interval
T_0 to T_4 : Points in time monitoring was performed
T_M: Report start time
T_N: Report end time
✕ : Point where information acquisition failed

The availability items for this example are calculated as follows:

Service availability = $\{(T_2 - T_M) + (T_N - T_4)\}/\{(T_2 - T_M) + (T_N - T_4) + (T_4 - T_2)\}$

Mean time to recovery = $(T_4 - T_2)/1$

Mean time between failures = $\{(T_2 - T_M) + (T_N - T_4)\}/1$

(3) Reporting criteria

When a monitored service that is subject to availability monitoring is stopped, an error is reported. If either of the following criteria is satisfied, the monitored service is treated as being stopped:

- An error was in effect at the time of the first measurement result obtained after monitoring started.
- The previous measurement result was normal and an error had occurred by the time of the measurement result for the current time.

If monitoring is stopped, the measurement results that have been obtained so far are reset. Therefore, if monitoring stops while the monitored service is stopped and an error occurs in the measurement result obtained after monitoring is restated, the error notification indicates that another monitored service has stopped.

(4) Criteria for determining that performance has returned to normal

If both the following criteria are satisfied, the monitored service is determined to have recovered from the stoppage and returned to normal:

- An error had occurred at the time of the previous measurement result.
- The measurement result for the current time is normal.

If monitoring is stopped, the measurement results that have been obtained so far are reset. Therefore, if monitoring stops while the monitored service is stopped, recovery is not reported even if the measurement result obtained after monitoring is restarted is normal.

(5) Supplementary information

- When PFM - Agent for Service Response is used for monitoring, a stoppage of a monitored service is reported whether it was caused by an error or by planned termination, because the difference between these two causes cannot be distinguished.

  Therefore, stop the monitoring before you perform planned termination on a monitored service that is being monitored for availability.
- Availability monitoring starts immediately after availability information is received from PFM - Agent for Service Response. If monitoring of a target service is stopped before availability information is received for the first time after monitoring started, availability monitoring is treated as not having started during that period. In such a case, information about the start and stop of the monitored service is not output to the service availability overview in the report.

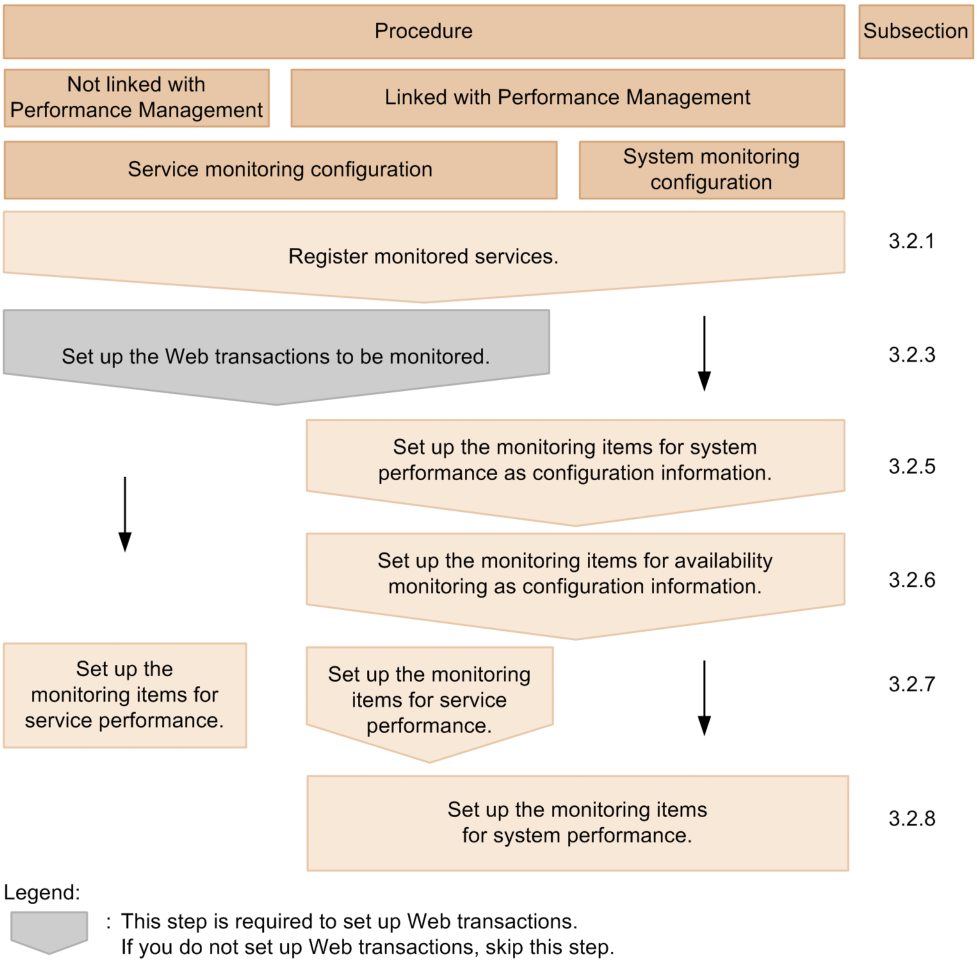
(6) Related topics

- *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)*
- *4.3.1 Checking the status of the monitored services of all service groups*
- *4.3.2 Checking the status of the monitored services in a specific service group*

3.2 How to register monitored services and set up monitoring items

The setup procedure required for monitoring Web transactions differs when monitoring is linked with Performance Management. The following figure provides an overview of the procedure.

Figure 3–23: Procedure for registering monitored services and setting up monitoring items


Procedure
Subsection
Not linked with Performance Management
Linked with Performance Management
Service monitoring configuration
System monitoring configuration
Register monitored services.
3.2.1
Set up the Web transactions to be monitored.
3.2.3
Set up the monitoring items for system performance as configuration information.
3.2.5
Set up the monitoring items for availability monitoring as configuration information.
3.2.6
Set up the monitoring items for service performance.
Set up the monitoring items for service performance.
3.2.7
Set up the monitoring items for system performance.
3.2.8
Legend:
: This step is required to set up Web transactions.
If you do not set up Web transactions, skip this step.

3.2.1 Registering monitored services

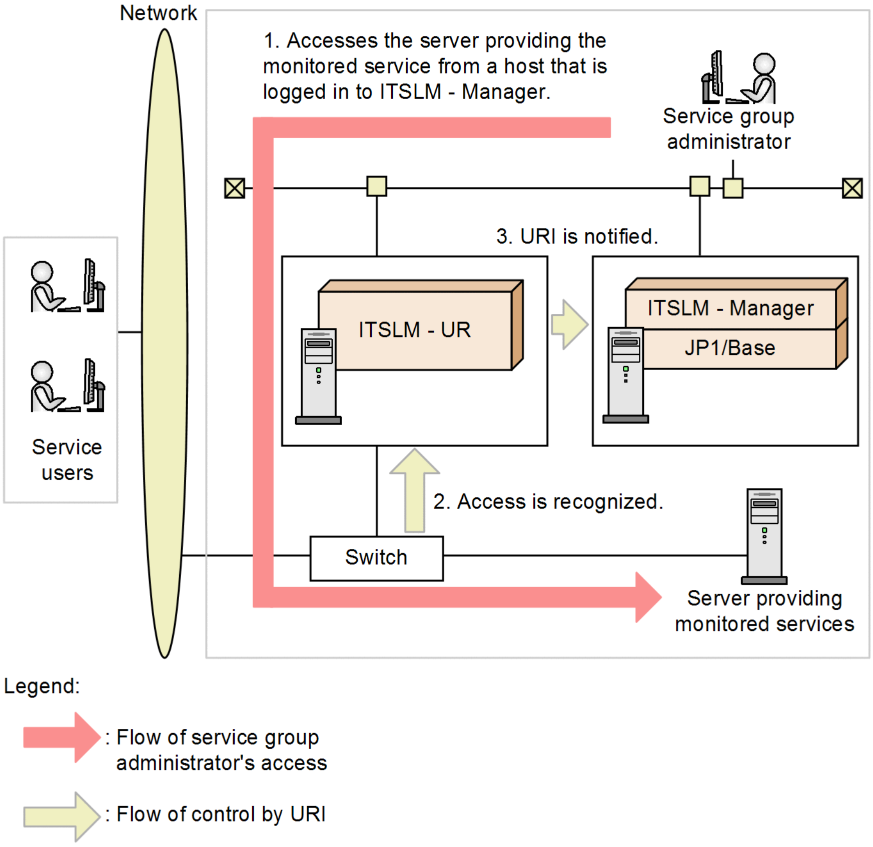
To register a service on which service performance monitoring is performed, register the URI of its Web page in ITSLM - Manager. This URI is detected automatically when you access the monitored service's Web page from a host that is logged in to ITSLM - Manager. The detection results are displayed in the ITSLM - Manager window.

A maximum of 50 monitored services can be registered into ITSLM - Manager, including All Web Access and Web transactions.

Note that you cannot combine services monitored by multiple ITSLM - URs and monitor them as a single service.

The following figure shows the procedure for detecting URIs.

Figure 3–24: URI detection procedure


Network
1. Accesses the server providing the monitored service from a host that is logged in to ITSLM - Manager.
Service group administrator
3. URI is notified.
ITSLM - UR
ITSLM - Manager
JP1/Base
Service users
2. Access is recognized.
Switch
Server providing monitored services
Legend:
: Flow of service group administrator's access
: Flow of control by URI

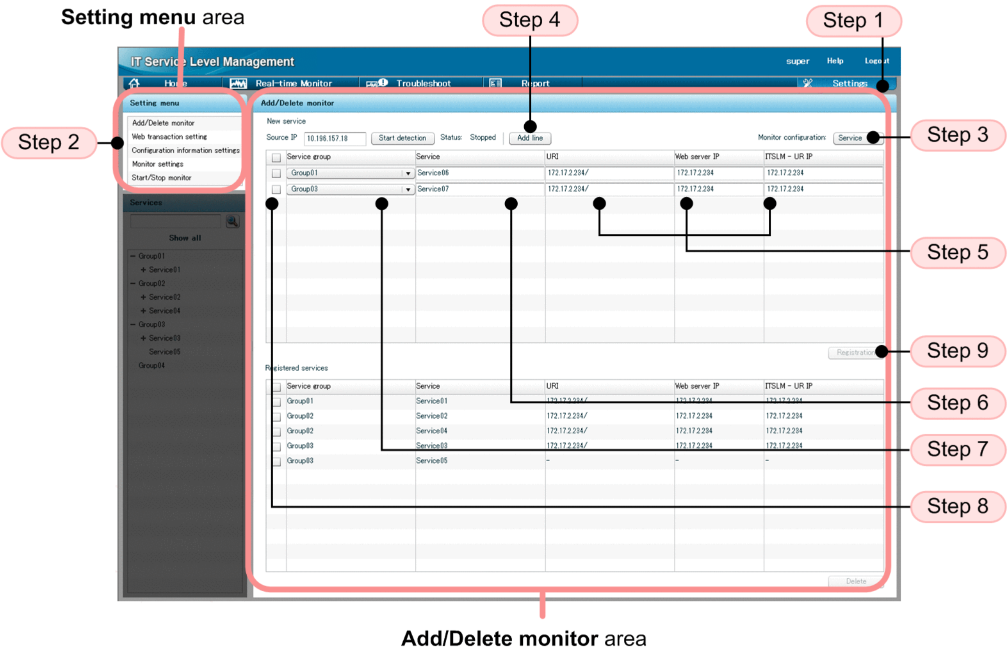
1. Access the Web page that you want to detect as a monitored service from a host that is logged in to ITSLM - Manager.
2. Access to the monitored service is recognized by ITSLM - UR.
3. The detected URI is reported to ITSLM - Manager.

(1) Before you start

- Verify that you have the service group administrator permissions.
- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that you can access the Web page of the monitored service that you want to register from a host that is accessing ITSLM - Manager.

(2) Procedure

The following shows the Settings window used in this procedure.



New service

Source IP: 10.196.157.18

Status: Stopped

Monitor configuration: Service

□	Service group	Service	URI	Web server IP	ITSLM - UR IP
□	Group01	Service06	172.17.2.234/	172.17.2.234	172.17.2.234
□	Group03	Service07	172.17.2.234/	172.17.2.234	172.17.2.234

Registered services

□	Service group	Service	URI	Web server IP	ITSLM - UR IP
□	Group01	Service01	172.17.2.234/	172.17.2.234	172.17.2.234
□	Group02	Service02	172.17.2.234/	172.17.2.234	172.17.2.234
□	Group02	Service04	172.17.2.234/	172.17.2.234	172.17.2.234
□	Group03	Service03	172.17.2.234/	172.17.2.234	172.17.2.234
□	Group03	Service05	-	-	-

To register a monitored service:

1. Click the **Settings** button.

2. In the **Setting menu** area, select **Add/Delete monitor**.

   The **Add/Delete monitor** area is displayed. In the **Add/Delete monitor** area, **Source IP** displays the IP address of the current computer (which is accessing ITSLM via its browser).

   If there are already any registered monitored services, the display in **Registered services** shows for each one its service group name, the name of the monitored service, its URI, its Web server's IP address, and the IP address of ITSLM - UR.

3. Select **Monitor configuration**.

   Select one of the following as the new service's monitoring configuration:

   Service: Monitors both service performance and system performance.

   System: Monitors system performance only.

4. Click the **Add line** button.

   A blank line is added to **New service**.

5. Enter information about the monitored target.

   To add a line for a service whose monitoring configuration is **Service**, enter the URI in **URI**, the IP address of the Web server running the monitored service in **Web server IP**, and the IP address of ITSLM - UR in **ITSLM - UR IP**.

6. Enter a name for the monitored service.

   Click the **Service** text box and enter any desired name.

   If an input rule is violated, an error message is displayed. Although no error message is displayed when platform-dependent characters or control characters are used, do not use these characters because they might cause an erroneous display of log files.

7. Select the service group to which the monitored service belongs.

Clicking the **Service group** pull-down menu displays the names of service groups (JP1 resource group names registered in JP1/Base) that the login user is responsible for monitoring. Select the service group to which the monitored service belongs.

8. Select the monitored service that you want to register.

   If the entered values are correct and **Status** shows **Stopped**, selecting the check box for a monitored service enables the **Registration** button. Note that if no service group was selected in step 7, an error message is displayed.

9. Click the **Registration** button.

   If registration is successful, a dialog box reporting that the monitored service has been registered successfully is displayed.

When you click the **OK** button in the dialog box, the service is added to **Registered services**.

Reference note

You can also detect a URI automatically. The following explains how to detect a URI by using the **Start detection** button. Steps 1 and 2 in the procedure for directly entering a URI are also necessary when you detect a URI automatically. Follow this procedure after you have finished steps 1 and 2.

1. If IP addresses are set to be converted in a system configuration via a device such as a load balancing device or router, change **Source IP** to the converted IP address.

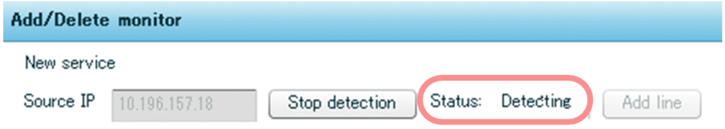
   Enter an IP address in the format *XXX*.*XXX*.*XXX*.*XXX* (*XXX*: `0` to `255`). This change is not needed if your system configuration is not via a device such as a load balancing device or router or is via a device such as a load balancing device or router but is not set to convert IP addresses.

2. Click the **Start detection** button.

   Status changes from **Stopped** to **Detecting** and URI detection is enabled. The **Start detection** button changes to the **Stop detection** button.

   The following figure shows **Status** changed to **Detecting**.

   Figure 3–25: Status changed to Detecting (Add/Delete monitor area)

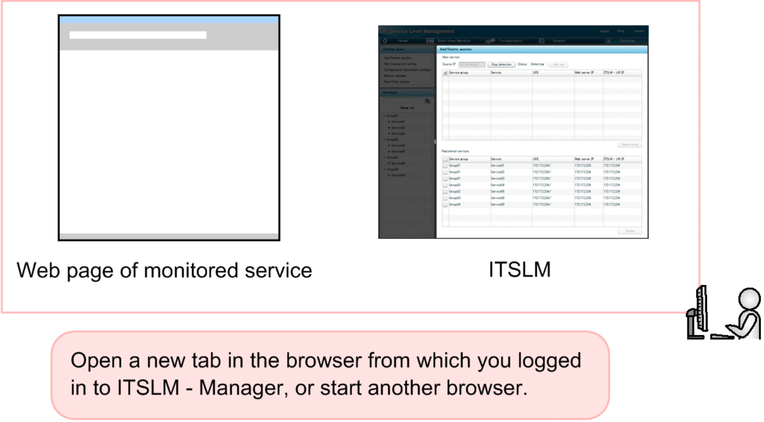


Add/Delete monitor

New service

Source IP 10.196.157.18 Stop detection Status: Detecting Add line

3. Open a new page in the browser logged in to ITSLM - Manager or start another browser, and then access the Web page of the monitored service that you want to register.


Web page of monitored service
ITSLM
Open a new tab in the browser from which you logged in to ITSLM - Manager, or start another browser.

In this case, make sure that you leave the browser that is logged in to ITSLM - Manager as is and open a new page or start another browser.

The monitored service detected by accessing its Web page is added to **New service** and the monitored service name, URI, IP address of the Web server running the monitored service, and the IP address of ITSLM - UR that performed this detection are displayed in **Service**, **URI**, **Web server IP**, and **ITSLM - UR IP**.

During detection, the URI is displayed as the monitored service name in **Service**. If the URI consists of more than 65 characters, only the first 65 characters are displayed and the remainder is discarded.

Each time a different Web page is accessed, a new monitored service is added. A URI that has already been detected is not added.

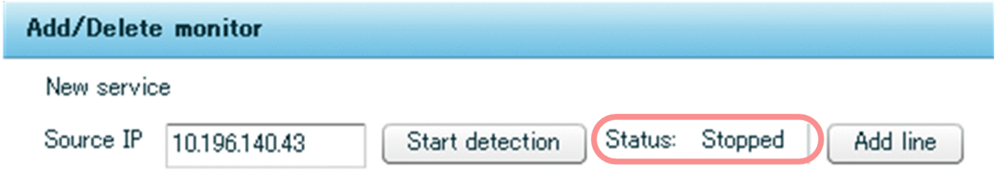
Note that any URIs for which a loopback address was specified, or for which `localhost` was specified as the host name, will not be displayed as monitored services.

4. Once the service you want to register has been detected, click the **Stop detection** button.

   Status changes from **Detecting** to **Stopped** once detection is complete.

   The following figure shows **Status** that has changed to **Stopped**.

Figure 3–26: Status changed to Stopped (Add/Delete monitor area)



Add/Delete monitor

New service

Source IP: 10.196.140.43

5. If you want to edit the URI displayed in **URI**, the IP address of the Web server running the monitored service that is displayed in **Web server IP**, or the IP address of ITSLM - UR that is displayed in **ITSLM - UR IP**, select the corresponding text box and then edit the information.

6. Enter a name for the monitored service.

   Click the **Service** text box and enter any desired name.

   If an input rule is violated, an error message is displayed. Although no error message is displayed when platform-dependent characters or control characters are used, do not use these characters because they might cause an erroneous display of log files.

7. Select the service group to which the monitored service belongs.

   Clicking the **Service group** pull-down menu displays the names of service groups (JP1 resource group names registered in JP1/Base) that the login user is responsible for monitoring. Select the service group to which the monitored service belongs.

8. Select the monitored service that you want to register.

   If the entered values are correct and **Status** shows **Stopped**, selecting the check box for a monitored service enables the **Registration** button. Note that if no service group was selected in step 7, an error message is displayed.

9. Click the **Registration** button.

   If registration is successful, a dialog box reporting that the monitored service has been registered successfully is displayed.

When you click the **OK** button in the dialog box, the service is added to **Registered services**.

(3) Next task

- *3.2.3 Setting up the Web transactions to be monitored* (when monitoring Web transactions)

- *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)* (working with Performance Management)
- *3.2.7 Setting up the monitoring items for service performance* (when Web transactions are not monitored or when not working with Performance Management)

(4) Related topics

- *3.2.2 Deleting monitored services*
- *4.3.1 Checking the status of the monitored services of all service groups*
- *4.3.2 Checking the status of the monitored services in a specific service group*
- *4.4.1 Checking the timing of an event causing an error or warning*
- *5.2 User settings in ITSLM*
- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.4 Add/Delete monitor area*

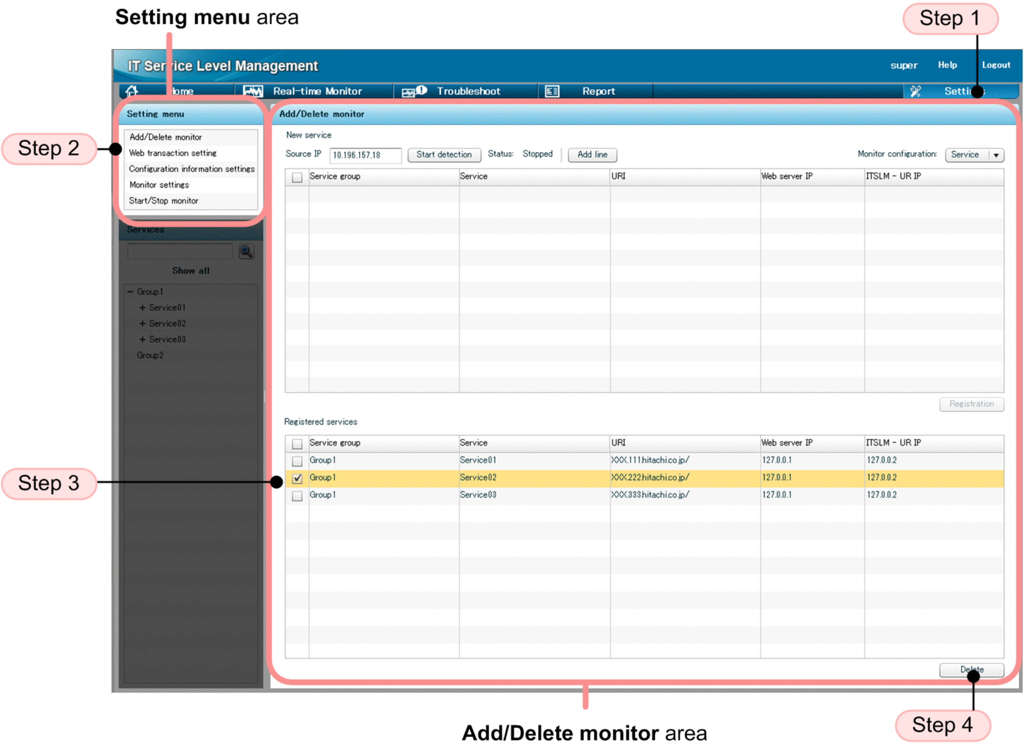
3.2.2 Deleting monitored services

(1) Before you start

- Verify that you have the service group administrator permissions.
- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring of the monitored service to be deleted has stopped.
  For details about how to stop monitoring, *4.2.2 Stopping monitoring*.

(2) Procedure

The following shows the Settings window used in this procedure:



Source IP 10.196.157.18

Status: Stopped

Monitor configuration: Service

□	Service group	Service	URI	Web server IP	ITSLM - UR IP

Registered services

□	Service group	Service	URI	Web server IP	ITSLM - UR IP
□	Group1	Service01	XXX.111.hitachi.co.jp/	127.0.0.1	127.0.0.2
☑	Group1	Service02	XXX.222.hitachi.co.jp/	127.0.0.1	127.0.0.2
□	Group1	Service03	XXX.333.hitachi.co.jp/	127.0.0.1	127.0.0.2

To delete a monitored service:

1. Click the **Settings** button.
2. In the **Setting menu** area, select **Add/Delete monitor**.
   The **Add/Delete monitor** area is displayed. The following items are displayed in **Registered services** for each monitored service: the name of its service group, the name of the monitored service, its URI, the IP address of its Web server, and the IP address of ITSLM - UR.
3. Select the check box for the monitored service that you want to delete from **Registered services**.
   When you select the check box for a monitored service, the **Delete** button becomes enabled.
4. Click the **Delete** button.

The selected monitored service is deleted from **Registered services**.

(3) Related topics

- *3.2.1 Registering monitored services*
- *3.2.7 Setting up the monitoring items for service performance*
- *4.3.1 Checking the status of the monitored services of all service groups*
- *4.3.2 Checking the status of the monitored services in a specific service group*
- *4.4.1 Checking the timing of an event causing an error or warning*
- *5.2 User settings in ITSLM*
- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*

- *10.6.4 Add/Delete monitor area*

3.2.3 Setting up the Web transactions to be monitored

This subsection explains how to set up Web transactions to be monitored. Specify the following three items for a Web transaction:

- Web access conditions (path, query, and cookie conditions)
- Order of Web access conditions
- Session conditions

Web access conditions are used to determine whether the URI and cookie contained in a Web access, which occurs when the user accesses the monitored service, indicate a process that is to be monitored as a Web transaction. Of all the Web accesses to the monitored service, only those that satisfy the Web access conditions are monitored as Web transactions. Session conditions are used to determine whether Web accesses are from the same user.

The service group administrator can set Web access conditions by detecting the URI and cookie from the monitored service or by directly entering the URI and cookie.

If IP addresses are set to be converted in a system configuration via a device such as a load balancing device or router, you must specify the IP address that was converted to the source IP when the URI was detected from the monitored service.

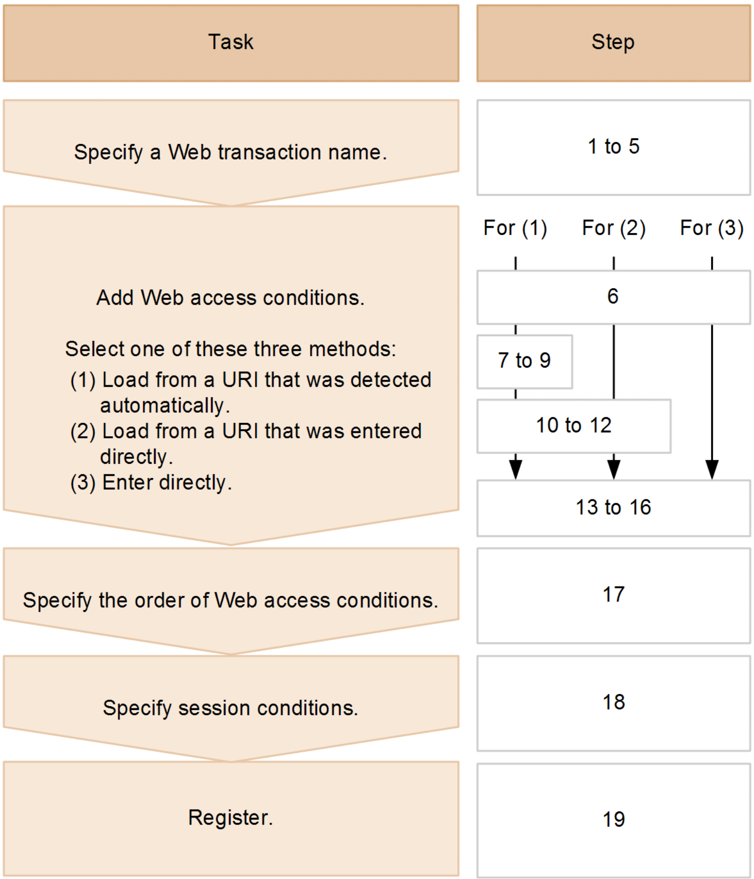
You can register a maximum of 10 Web transactions per monitored service. The maximum number of Web transactions that can be registered for one ITSLM - Manager is 50 including All Web Access and Web transactions.

(1) Before you start

- Verify that you have the service group administrator permissions.
- Verify that the monitored service has been registered.
  For details about how to register monitored services, see *3.2.1 Registering monitored services*.
- Verify that monitoring of the monitored service for which Web transactions are to be set up has been stopped.
  For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

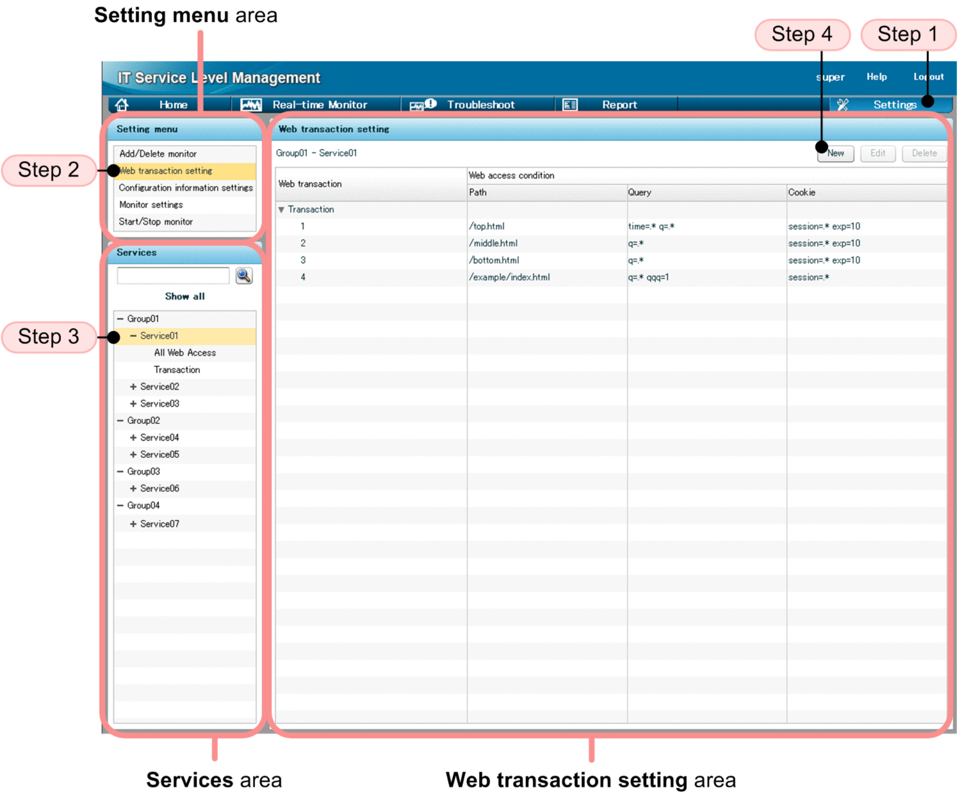
(2) Procedure

The following shows the procedure:


Task
Step
Specify a Web transaction name.
1 to 5
Add Web access conditions.
Select one of these three methods:
(1) Load from a URI that was detected automatically.
(2) Load from a URI that was entered directly.
(3) Enter directly.
For (1)
For (2)
For (3)
6
7 to 9
10 to 12
13 to 16
Specify the order of Web access conditions.
17
Specify session conditions.
18
Register.
19

Shown below are the Settings window, Register Web transaction window, Add Web access condition window, Edit cookie window, and Edit query window that are used in this task.

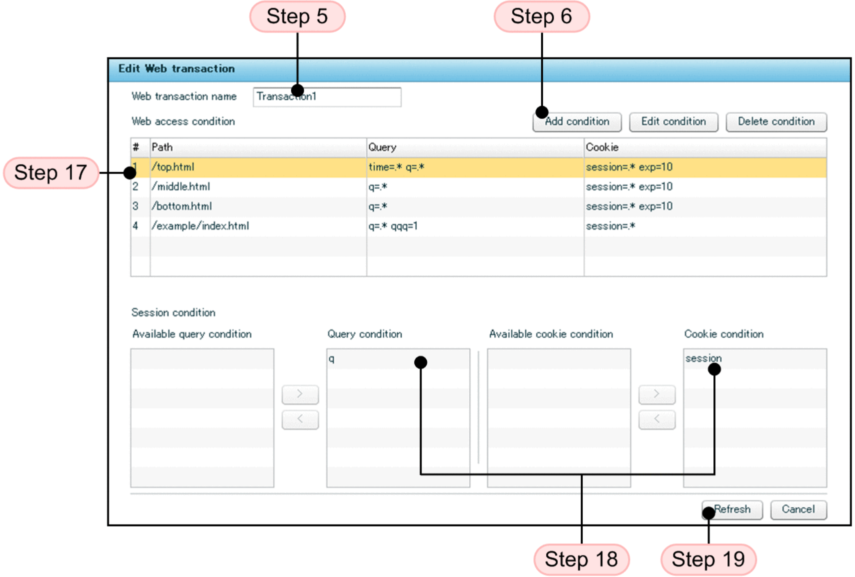
- Settings window



Group01 - Service01

Web transaction	Web access condition		
	Path	Query	Cookie
▼ Transaction			
1	/top.html	time=.* q=.*	session=.* exp=10
2	/middle.html	q=.*	session=.* exp=10
3	/bottom.html	q=.*	session=.* exp=10
4	/example/index.html	q=.* qqq=1	session=.*

- Register Web transaction window (displayed in a new window when the **New** button is clicked (step 4))



Edit Web transaction

Web transaction name: Transaction1

Web access condition

#	Path	Query	Cookie
1	/top.html	time=.* q=.*	session=.* exp=10
2	/middle.html	q=.*	session=.* exp=10
3	/bottom.html	q=.*	session=.* exp=10
4	/example/index.html	q=.* qqq=1	session=.*

Session condition

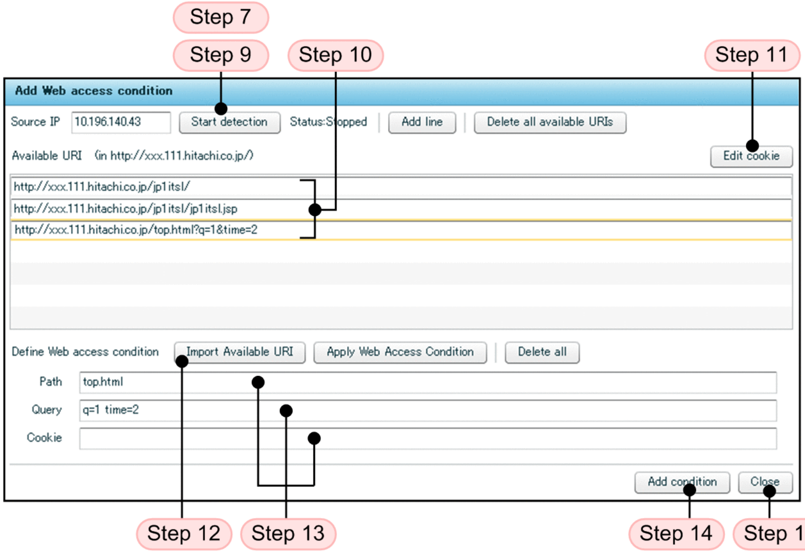
Available query condition:

Query condition: q

Available cookie condition:

Cookie condition: session

- Add Web access condition window (displayed in a new window when the **Add condition** button is clicked (step 6))



Add Web access condition

Source IP: 10.196.140.43

Status:Stopped

Available URI (in http://xxx.111.hitachi.co.jp/)

http://xxx.111.hitachi.co.jp/jp1itsl/
http://xxx.111.hitachi.co.jp/jp1itsl/jp1itsl.jsp
http://xxx.111.hitachi.co.jp/top.html?q=1&time=2

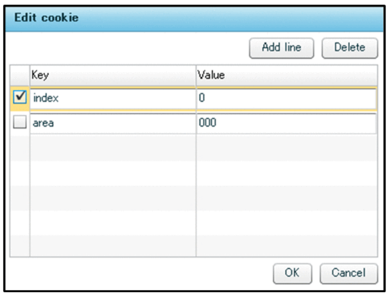
Define Web access condition

Path: top.html

Query: q=1 time=2

Cookie:

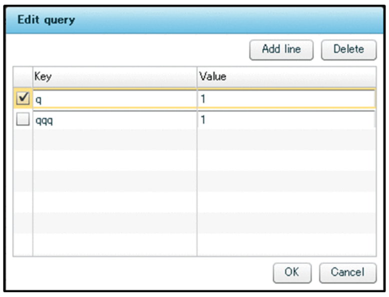
- Edit cookie window (displayed in a new window when the **Edit cookie** button is clicked (step 11) or the **Cookie** text box is clicked (step 13))



Edit cookie

	Key	Value
☑	index	0
□	area	000

- Edit query window (displayed in a new window when the **Query** text box is clicked (step 13))



	Key	Value
☑	q	1
□	qqq	1

To set up the Web transactions to be monitored:

1. Click the **Settings** button.
2. In the **Setting menu** area, select **Web transaction setting**.

   The **Web transaction setting** area is displayed.
3. From the **Services** area, select the monitored service.

   When you select a monitored service, the service group name and monitored service name are displayed in the **Web transaction setting** area. Any Web transaction name that has already been set for the monitored service and the Web access conditions for that Web transaction are displayed under **Web transaction** and **Web access condition** in the **Web transaction setting** area. Immediately after the monitored service has been registered, nothing is displayed under **Web transaction** and **Web access condition**.
4. Click the **New** button.

   The Register Web transaction window is displayed.
5. Enter a name for a Web transaction.

   Enter a name in the **Web transaction name** text box.

   If an input rule is violated, an error message is displayed. Although no error message is displayed when platform-dependent characters or control characters are used, these characters might cause erroneous display of log files.

   Note that the same transaction name cannot be registered more than once for the same monitored service.
6. Click the **Add condition** button.

   The Add Web access condition window is displayed. The **Source IP** text box displays the IP address of the current computer (that is accessing ITSLM via a browser).

   The procedure for adding Web access conditions depends on the addition method:

   - To import Web access conditions from a URI that was detected automatically by accessing the monitored service

     Go to step 7.
   - To import Web access conditions from the URI of a monitored service that you entered directly

     Go to step 10.
   - To directly enter Web access conditions

     Go to step 13.

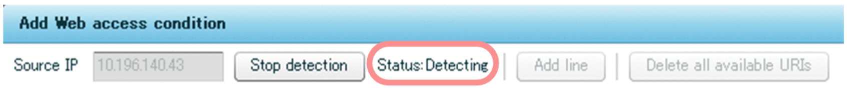
   Specify for the Web access conditions the case-sensitive path, query, and cookie used for actual Web access. ITSLM monitors the Web accesses that match the specified character string.

   Some browsers might convert the case during actual Web access. If the case does not match between the specified Web access conditions and the actual Web access, the Web transaction cannot be monitored.
7. Click the **Start detection** button.

Status changes from **Stopped** to **Detecting** and URI detection is enabled. The **Start detection** button changes to the **Stop detection** button.

The following figure shows **Status** changed to **Detecting**.

Figure 3–27: Status changed to Detecting (Add Web access condition window)



Add Web access condition

Source IP 10.196.140.43

8. Open a new page in the browser logged in to ITSLM - Manager or start another browser, and then access the monitored service's Web page.

   In this case, make sure that you do not change or close the browser logged in to ITSLM - Manager and that you open a new page or start another browser.

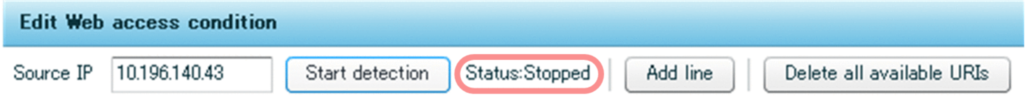
   The URI detected by the access is added to **Available URI**. Each time a different Web page is accessed, a new URI is added. A URI that has already been detected is not added.

9. After the URI has been detected, click the **Stop detection** button.

   Status changes from **Detecting** to **Stopped** and detection is complete.

   The following figure shows **Status** that has changed to **Stopped**.

Figure 3–28: Status changed to Stopped (Add Web access condition window)



Edit Web access condition

Source IP 10.196.140.43

10. To edit a URI displayed under **Available URI**, select a desired URI and then edit it. You can also add a new URI by adding a blank line.

    You can edit any of the URIs displayed under **Available URI** by clicking the URI. You can also add a blank line under **Available URI** and then directly enter a desired URI. To directly enter a URI, click the **Add line** button and then enter the URI on the added line.

11. To check or edit the cookie of a URI displayed under **Available URI**, select the URI, and then click the **Edit cookie** button.

    The Edit cookie window is displayed. In the Edit cookie window, you can check, add, change, or delete the cookie to be imported to the Web access conditions. Edit the cookie, if necessary, and then click the **OK** button.

12. Select a URI from **Available URI** and then click the **Import Available URI** button.

    In **Define Web access condition**, you can enter the path, query, and cookie values of the URI selected from **Available URI** all at once.

13. To directly enter or edit Web access conditions, enter or edit the path condition, query condition, and cookie condition in **Define Web access condition**.

    If you click the **Apply Web Access Condition** button after you have entered or edited the conditions, there is further refinement of the URIs displayed under **Available URI** and only the URIs that perfectly match the conditions are displayed.

    Directly enter the path condition in the text box. Enter query and cookie conditions in the Edit query window and Edit cookie window, respectively, that are opened when you click the corresponding text box.

    You can specify multiple query and cookie conditions, but the maximum number of conditions that you can specify is 20 including both query and cookie conditions. When you specify multiple conditions, they are separated by a space and displayed in a random order.

    Use the path, query, and cookie conditions to refine URIs so that you can obtain only the URIs of those processes that you want to monitor.

14. While the conditions are showing in **Define Web access condition**, click the **Add condition** button in the Add Web access condition window.

    The values entered in **Define Web access condition** in the Add Web access condition window are displayed in **Web access condition** in the Register Web transaction window.

15. Repeat the procedure for adding Web access conditions until all the conditions necessary for the Web transactions to be monitored are displayed in **Web access condition**.

    The same Web access condition cannot be registered more than once. A maximum of five Web access conditions can be specified for one Web transaction.

16. When you have finished adding Web access conditions, click the **Close** button.

    The Add Web access condition window closes and the Register Web transaction window is displayed again.

17. If necessary, change the order of the Web access conditions by dragging Web access conditions in **Web access condition** up and down in the Register Web transaction window.

    ITSLM checks the Web accesses against the Web access conditions displayed in **Web access condition** in this order to determine whether they are for the specified Web transactions.

18. If you want to check whether Web accesses are from the same user, specify session conditions.

    You can specify session conditions by selecting query and cookie conditions displayed in **Available query condition** and **Available cookie condition**, respectively. Select a candidate to be used as a session condition and then click the > button.

    Available query condition and **Available cookie condition** display the keys of query and cookie conditions that match multiple Web access conditions displayed in **Web access condition**.

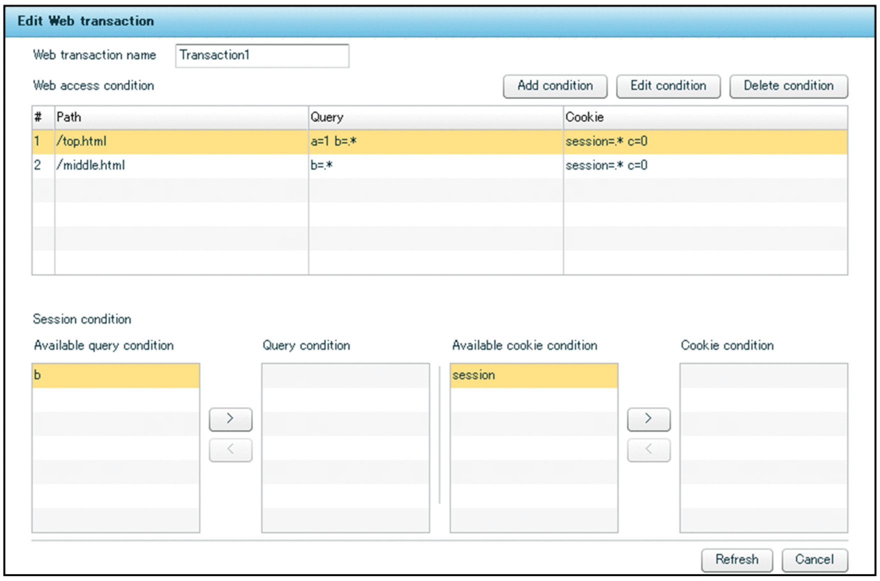
    The following shows an example in which the keys of query and cookie conditions that match multiple Web access conditions are displayed.

    This example assumes that the following Web access conditions are displayed in **Web access condition**:

No.	Path	Query condition	Cookie condition
1	`/top.html`	`a=1 b=.*`	`session=.* c=0`
2	`/middle.html`	`b=.*`	`session=.* d=0`

`b` (the key of `b=.*`) is displayed in **Available query condition** and `session` (the key of `session=.*`) is displayed in **Available cookie condition**. The following figure shows an example in which **Available query condition** and **Available cookie condition** are displayed.

Figure 3–29: Example in which Available query condition and Available cookie condition are displayed



Web transaction name: Transaction1

Web access condition

#	Path	Query	Cookie
1	/top.html	a=1 b=.*	session=.* c=0
2	/middle.html	b=.*	session=.* c=0

Available query condition: b

Available cookie condition: session

To delete query conditions and cookie conditions from **Query condition** and **Cookie condition**, respectively, select a desired query condition or cookie condition in **Query condition** or **Cookie condition**, respectively, and then click the < button to move the query condition or cookie condition back to **Available query condition** or **Available cookie condition**, respectively. The maximum number of conditions you can specify in **Query condition** and **Cookie condition** is 10 including both query and cookie conditions.

19. Click the **Registration** button.

    If any entries have been added in **Web access condition**, the **Registration** button is enabled.

Clicking the **Registration** button closes the Register Web transaction window, and the **Web transaction setting** area is displayed again. The settings in the Register Web transaction window are added as a Web transaction to the **Web transaction setting** area.

(3) Next task

- *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)* (working with Performance Management)
- *3.2.7 Setting up the monitoring items for service performance* (when not working with Performance Management)

(4) Related topics

- *3.1.1 ITSLM's monitoring methods and types of monitored targets*
- *3.2.4 Deleting Web transactions to be monitored*
- *5.2 User settings in ITSLM*
- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.5 Web transaction setting area*
- *10.6.6 Register Web transaction window*
- *10.6.7 Add Web access condition window*

- *10.6.8 Edit Web access condition window*
- *10.6.9 Edit cookie window*
- *10.6.10 Edit query window*
- *10.6.11 Edit Web transaction window*

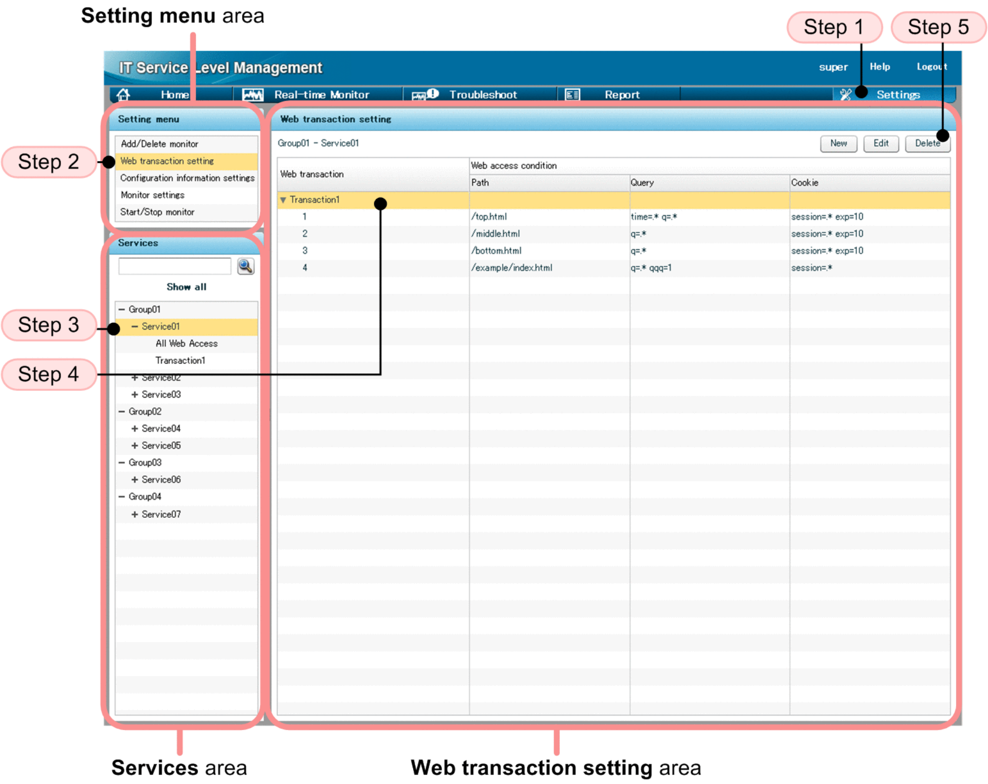
3.2.4 Deleting Web transactions to be monitored

(1) Before you start

- Verify that you have the service group administrator permissions.
- Verify that monitoring of the monitored service for which Web transactions are to be deleted has stopped.
  For details about how to stop monitoring, *4.2.2 Stopping monitoring*.

(2) Procedure

The following shows the Settings window used in this procedure.



Group01 - Service01

Web transaction	Web access condition		
	Path	Query	Cookie
▼ Transaction1			
1	/top.html	time=.* q=.*	session=.* exp=10
2	/middle.html	q=.*	session=.* exp=10
3	/bottom.html	q=.*	session=.* exp=10
4	/example/index.html	q=.* qqq=1	session=.*

To delete Web transactions to be monitored:

1. Click the **Settings** button.

2. In the **Setting menu** area, select **Web transaction setting**.
   The **Web transaction setting** area is displayed.

3. From the **Services** area, select the monitored service.

When you select a monitored service, the service group name and monitored service name are displayed in the **Web transaction setting** area. Also, the name of any Web transaction that has already been set for the monitored service is displayed under **Web transaction** and the Web access condition for the Web transaction is displayed under **Web access condition**. Immediately after the monitored service has been registered, nothing is displayed under **Web transaction** and **Web access condition**.

4. From **Web transaction** or **Web access condition**, select the Web transaction that you want to delete.
   When a Web transaction is selected from **Web transaction** or **Web access condition**, the **Delete** button is enabled.
5. Click the **Delete** button.

The selected Web transaction is deleted from **Web transaction** and **Web access condition**.

(3) Related topics

- *3.2.3 Setting up the Web transactions to be monitored*
- *3.2.7 Setting up the monitoring items for service performance*
- *5.2 User settings in ITSLM*
- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.5 Web transaction setting area*

3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)

Setting up monitoring items for system performance is required when ITSLM is linked with Performance Management.

If you link ITSLM with Performance Management, set up the monitoring items for system performance as configuration information.

Setting up monitoring items for system performance associates information about a business group defined in Performance Management (including information about hosts and monitoring agents) with a monitored service. By performing this setup, you can monitor in ITSLM the system performance of the items that you have associated in this setup.

Monitoring items that have been set up for system performance must be set up again in the following situations:

- Monitored services have been added, changed, or deleted
- Hosts in the business group have been changed
- Monitoring agents have been added or deleted

If you perform monitoring item setup for multi-instance records, verify the values that can be specified as keys beforehand.

(1) Before you start

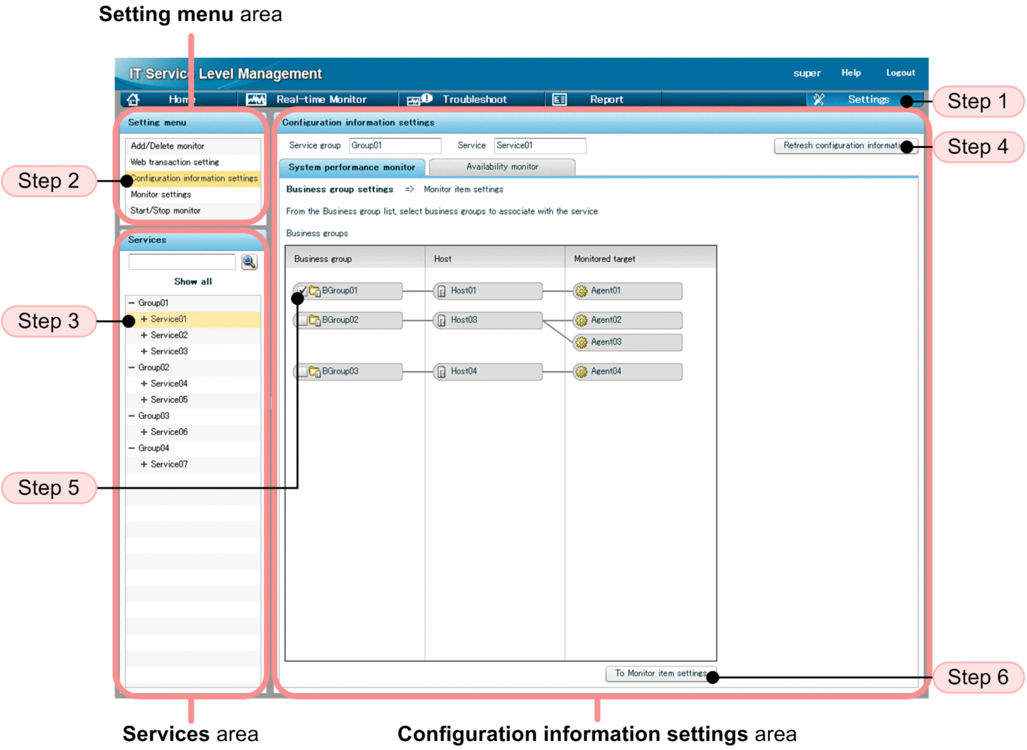
- Verify that you have the service group administrator permissions.

- Verify that the monitored service has been registered.
  For details about how to register monitored services, see *3.2.1 Registering monitored services*.
- If you monitor Web transactions, verify that the Web transactions have been registered.
  For details about how to register Web transactions, see *3.2.3 Setting up the Web transactions to be monitored*.
- Verify that monitoring of the monitored service for which monitoring items are to be set up has stopped.
  For details about how to stop monitoring, *4.2.2 Stopping monitoring*.
- Verify that PFM - Manager is running.
  For details about how to start PFM - Manager, see the description of the PFM - Manager setup procedure in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Procedure

The following shows the **Configuration information settings** area, the Confirmation of refreshing configuration information window, the Add Items to be Monitored window, and the Key field information settings window that are used in this task.

- **Configuration information settings** area (business group settings displayed with the **System performance monitor** tab selected)



Service group: Group01

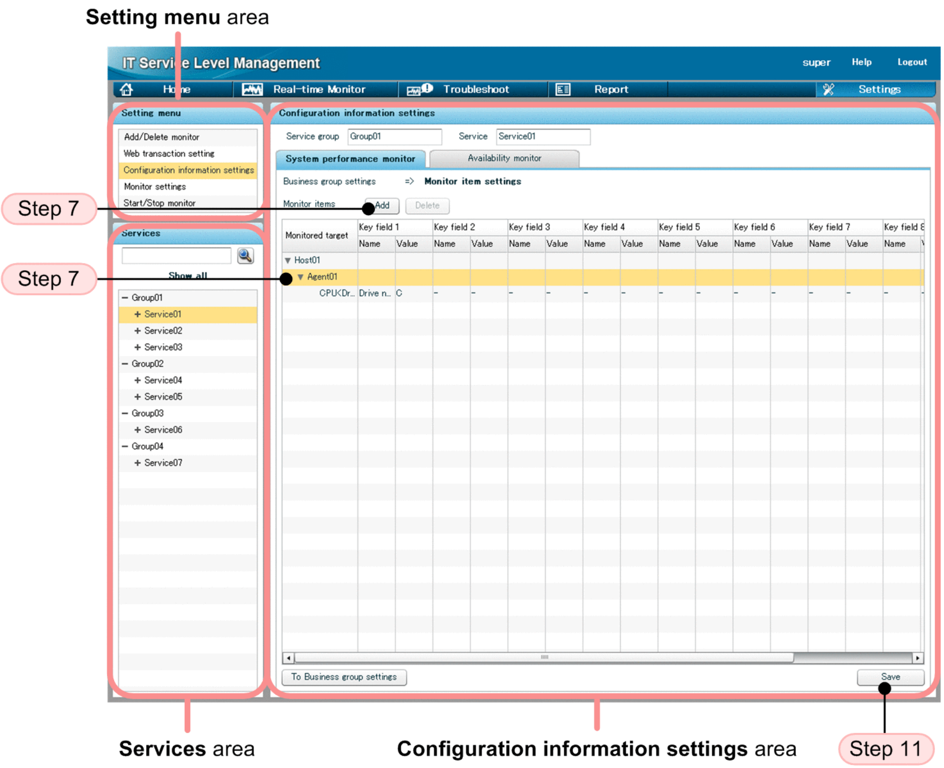
Service: Service01

Business group settings => Monitor item settings

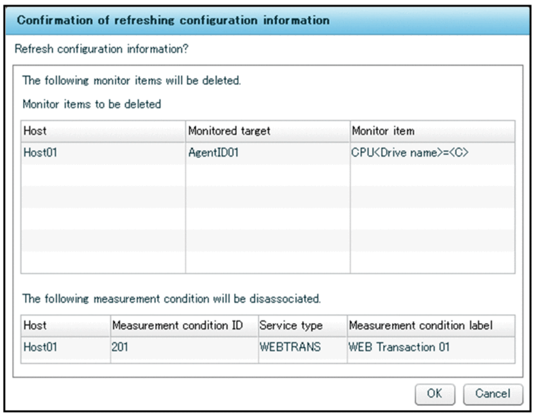
From the Business group list, select business groups to associate with the service

Business group	Host	Monitored target
☑ BGroup01	Host01	Agent01
□ BGroup02	Host03	Agent02 Agent03
□ BGroup03	Host04	Agent04

- **Configuration information settings** area (monitoring item settings displayed with the **System performance monitor** tab selected)



- Confirmation of refreshing configuration information window (displayed in a new window when the **Refresh configuration information** button is clicked (step 4))



Confirmation of refreshing configuration information

Refresh configuration information?

The following monitor items will be deleted.

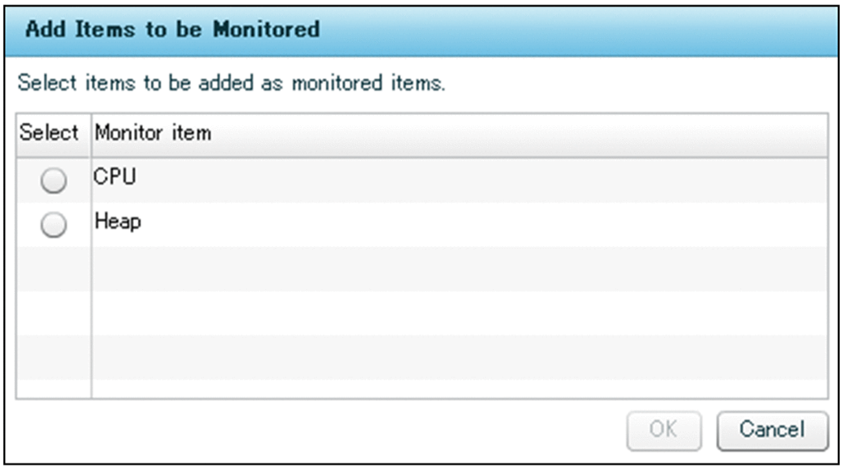
Monitor items to be deleted

Host	Monitored target	Monitor item
Host01	AgentID01	CPU<Drive name>=<C>

The following measurement condition will be disassociated.

Host	Measurement condition ID	Service type	Measurement condition label
Host01	201	WEBTRANS	WEB Transaction 01

- Add Items to be Monitored window (displayed in a new window when the **Add** button is clicked (step 7))

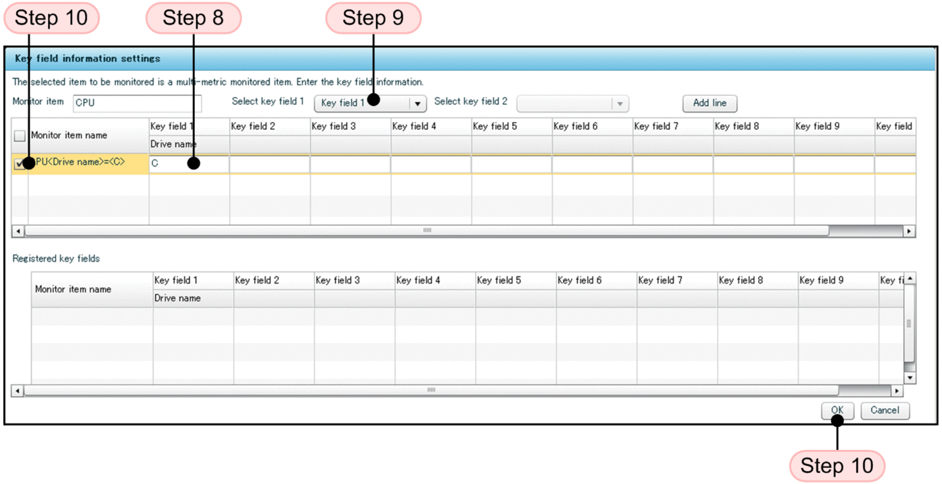


Add Items to be Monitored

Select items to be added as monitored items.

Select	Monitor item
○	CPU
○	Heap

- Key field information settings window (displayed in a new window when the monitoring item consists of multiple instances and the **OK** button is clicked (step 7))



Key field information settings

The selected item to be monitored is a multi-metric monitored item. Enter the key field information.

Monitor item: CPU

Select key field 1: Key field 1

Select key field 2:

☐	Monitor item name	Key field 1	Key field 2	Key field 3	Key field 4	Key field 5	Key field 6	Key field 7	Key field 8	Key field 9	Key field
		Drive name									
☑	PU<Drive name>=<C>	C									

Registered key fields

Monitor item name	Key field 1	Key field 2	Key field 3	Key field 4	Key field 5	Key field 6	Key field 7	Key field 8	Key field 9	Key fi
	Drive name									

To set up the monitoring items for system performance as configuration information:

1. Click the **Settings** button.

2. In the **Setting menu** area, select **Configuration information settings**.

   The **Configuration information settings** area is displayed.

3. From the **Services** area, select a monitored service whose system performance is to be monitored.

   Business groups are displayed for the selected monitored service.

   If a Web transaction was selected, a setup window for the monitored service to which this transaction belongs is displayed.

4. Click the **Refresh configuration information** button.

   Clicking the **Refresh configuration information** button displays the most recent configuration information acquired by Performance Management in the list of business groups.

   If you refresh the configuration information, the Confirmation of refreshing configuration information window is displayed. Check the displayed information and then click the **OK** button.

5. Select the business group to be associated with the monitored service.

   In the list of business groups, select the business group that you want to associate with the monitored service. If a business group has already been associated with the monitored service, the associated group is displayed as being selected.

6. Click the **To Monitor item settings** button.

   A list of monitoring items is displayed.

   The hosts and monitoring agents under the business group selected from the list of business groups are displayed.

   The monitoring agents for which monitoring items have already been set up in Performance Management are displayed here. A monitoring agent for which monitoring items have not been set up is not displayed.

7. Select a monitoring agent and then click the **Add** button.

   The Add Items to be Monitored window is displayed. Select the monitoring items to be added and then click the **OK** button.

   If the added monitoring items are single-instance ones, they are displayed under **Monitored target** in the **Configuration information settings** area. Go to step 11.

   If the added monitoring items are multi-instance ones, the Key field information settings window is displayed.

For the monitoring items in the key field information, those monitoring items selected in the Add Items to be Monitored window are displayed. This information cannot be edited by ITSLM.

> **Tip**
>
> There is a limit to the number of monitoring items that can be monitored concurrently for a single monitoring agent. For details about the number of monitoring items that can be monitored concurrently, see the applicable PFM - Agent or PFM - RM manual.
>
> You can associate a maximum of 100 monitoring items with a single monitored service that is monitored by ITSLM - Manager. If you want to set more than 100 monitoring items, create multiple monitored services and then assign monitoring items to each of them.
>
> Use the value obtained from the following formula as a guideline for the number of monitoring items that can be specified in the entire ITSLM - Manager:
>
> $(\textit{number of All Web Accesses} + \textit{number of Web transactions}) \times 20 + (\textit{number of monitoring items}) \leq 1{,}200$

8. Enter the value to be specified for the key field in the text box.

   Define key field information for the monitoring items.

   For the values to be specified, check the values for monitoring items in Performance Management. For details about checking the values of monitoring items in Performance Management, see the applicable PFM - Agent or PFM - RM manual.

   Note that a monitoring item can be added when its key field value is empty only if the value for the monitoring item in Performance Management is also empty. Therefore, for the key field value, enter the correct value set for the monitoring item in Performance Management.

9. In **Select key field 1**, select a key field and then select the key field information to be displayed as the monitoring item name.

   Entry of **Select key field 2** is optional.

10. Select the check box for the monitoring item to be added, and then click the **OK** button.

    The Key field information settings window closes and the **Configuration information settings** area is displayed. The settings specified for key field information are applied and the added monitoring item is displayed under **Monitored target** in the **Configuration information settings** area.

    If you want to add another monitoring item, click the **Add line** button in the Key field information settings window to add a new monitoring item line. For the added line, repeat steps 8 through 10.

11. Click the **Save** button.

    The settings for system performance monitoring are applied.

    If you want to delete a monitoring item that has already been set up, select it, and then click the **Delete** button.

    If you change business group names, host names, or monitoring agent names in Performance Management, ITSLM displays the applicable monitoring items with the new names.

(3) Next task

- *3.2.6 Setting up the monitoring items for availability monitoring as configuration information (working with Performance Management)*

(4) Related topics

- *10.6.1 Configuration of the Settings window*

- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.12 Configuration information settings area (Business group settings with the System performance monitor tab selected)*
- *10.6.13 Configuration information settings area (Monitoring item settings with the System performance monitor tab selected)*
- *10.6.17 Confirmation of refreshing configuration information window*
- *10.6.15 Add Items to be Monitored window*
- *10.6.16 Key field information settings window*

3.2.6 Setting up the monitoring items for availability monitoring as configuration information (working with Performance Management)

Monitoring item setup for availability monitoring is required when ITSLM is linked with Performance Management.

If you link ITSLM with Performance Management, set up the monitoring items as configuration information.

Monitoring item setup for availability monitoring associates measurement conditions set in Performance Management with monitored services. When you perform this setup, you can check the availability of monitored services in ITSLM.

Configuration information for monitored services that has already been set up must be set up again in the following situations:

- Monitored services have been added, changed, or deleted
- Hosts in the business group have been changed
- Monitoring agents have been added or deleted

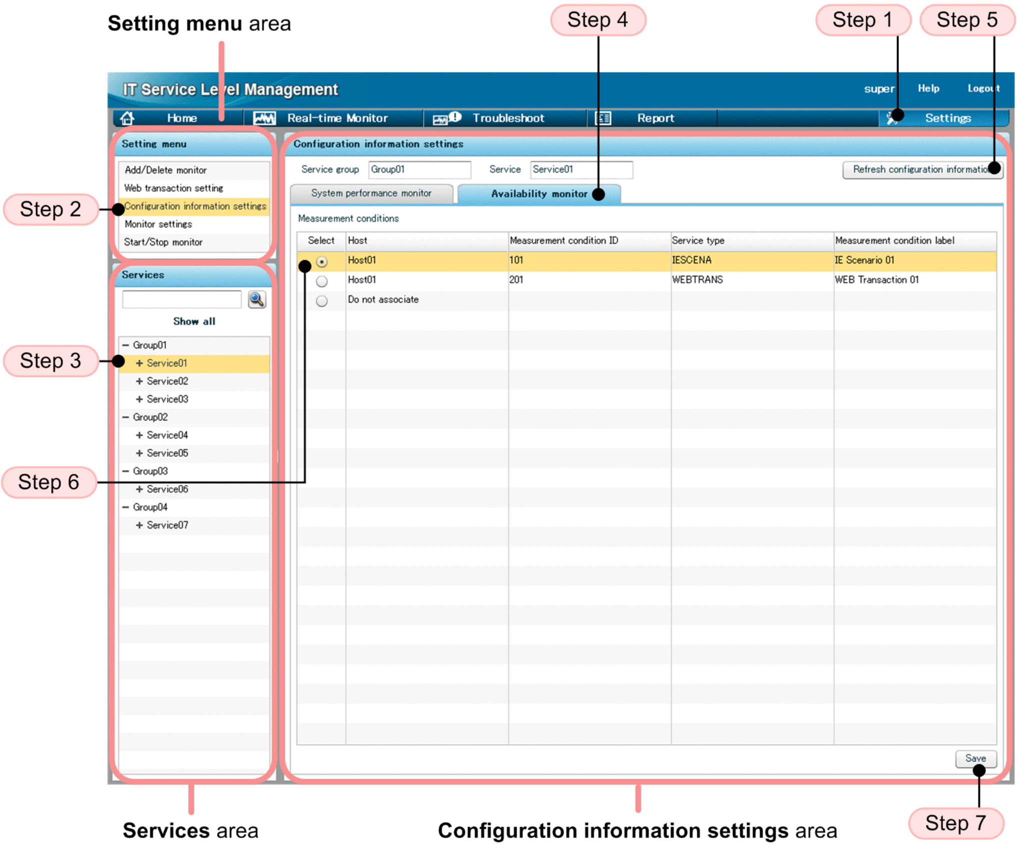
When you set up monitoring items for availability monitoring, you must first use PFM - Agent for Service Response to define IE scenarios or Web transactions. For details about the definitions in PFM - Agent for Service Response, see the applicable PFM - Agent for Service Response manual.

(1) Before you start

- Verify that you have the service group administrator permissions.
- Verify that the monitored service has been registered.
  For details about how to register monitored services, see *3.2.1 Registering monitored services*.
- If you monitor Web transactions, verify that the Web transactions have been registered.
  For details about how to register Web transactions, see *3.2.3 Setting up the Web transactions to be monitored*.
- Verify that monitoring of the monitored service for which monitoring items are to be set up has stopped.
  For details about how to stop monitoring, *4.2.2 Stopping monitoring*.
- Verify that PFM - Manager is running.
  For details about how to start PFM - Manager, see the description of the PFM - Manager setup procedure in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Procedure

The following shows the **Configuration information settings** area (with the **Availability monitor** tab selected) that is used in this task:



Service group: Group01 Service: Service01

Measurement conditions

Select	Host	Measurement condition ID	Service type	Measurement condition label
●	Host01	101	IESCENA	IE Scenario 01
○	Host01	201	WEBTRANS	WEB Transaction 01
○	Do not associate			

To set up monitoring items for availability monitoring as configuration information:

1. Click the **Settings** button.

2. In the **Setting menu** area, select **Configuration information settings**.
   The **Configuration information settings** area is displayed.

3. From the **Services** area, select a monitored service for which availability monitoring is to be set up.
   Business groups are displayed for the selected monitored service.
   If a Web transaction was selected, a setup window for the monitored service to which this transaction belongs is displayed.

4. Click the **Availability monitor** tab.
   A list of measurement conditions is displayed.

5. Click **Refresh configuration information** button.
   Clicking the **Refresh configuration information** button displays the most recent configuration information acquired by Performance Management in the list of measurement conditions.
   If you refresh the configuration information, the Confirmation of refreshing configuration information window is displayed. Check the displayed information and then click the **OK** button.

6. Select the measurement condition to be associated with the monitored service. If you do not wish to associate a measurement condition with the monitored service, select **Do not associate**.

Select the measurement condition to be associated with the monitored service.

7. Click the **Save** button.
   The availability monitoring settings are applied and the monitored service in ITSLM is associated with the measurement condition in PFM - Agent for Service Response.

(3) Next task

- *3.2.7 Setting up the monitoring items for service performance*

(4) Related topics

- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.14 Configuration information settings area (with the Availability monitor tab selected)*

3.2.7 Setting up the monitoring items for service performance

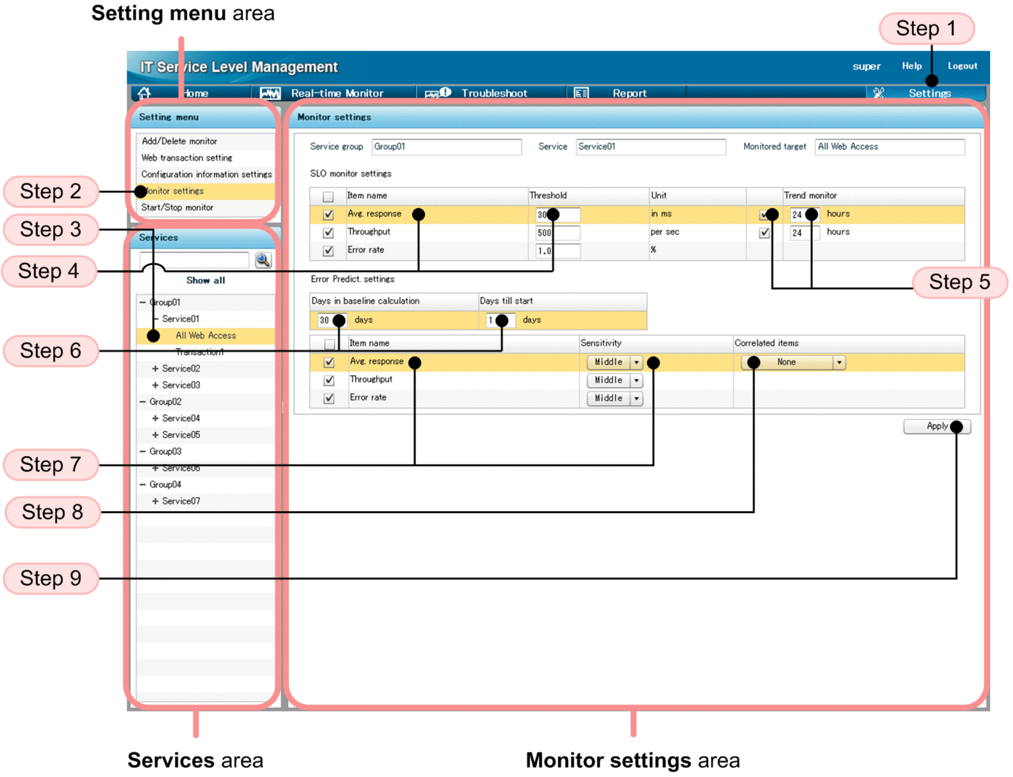
You must set up monitoring items for each monitored service.

(1) Before you start

- Verify that you have the service group administrator permissions.
- Verify that the monitored service has been registered.
  For details about how to register monitored services, see *3.2.1 Registering monitored services*.
- If you monitor Web transactions, verify that the Web transactions have been registered.
  For details about how to register Web transactions, see *3.2.3 Setting up the Web transactions to be monitored*.
- Verify that monitoring of the monitored service for which monitoring items are to be set up has stopped.
  For details about how to stop monitoring, *4.2.2 Stopping monitoring*.

(2) Procedure

The following shows the Settings window used in this task:



Service group: Group01 Service: Service01 Monitored target: All Web Access

SLO monitor settings

□	Item name	Threshold	Unit		Trend monitor
☑	Avg. response	30	in ms	☑	24 hours
☑	Throughput	500	per sec	☑	24 hours
☑	Error rate	1.0	%		

Error Predict. settings

Days in baseline calculation	Days till start
30 days	1 days

□	Item name	Sensitivity	Correlated items
☑	Avg. response	Middle	None
☑	Throughput	Middle	
☑	Error rate	Middle	

To set up monitoring items for service performance:

1. Click the **Settings** button.
2. In the **Setting menu** area, select **Monitor settings**.

   The **Monitor settings** area is displayed.
3. From the **Services** area, select a monitored target of a monitored service.

   When you select a monitored target of a monitored service, the service group name, monitored service name, and monitored target are displayed in the **Monitor settings** area. The current values are displayed under **SLO monitor settings** and **Error Predict. settings**. Immediately after a monitored service has been registered, the default values are set.
4. If you will be running threshold value monitoring or trend monitoring, select the **Item name** check boxes under **SLO monitor settings** for the items that you want to monitor, and then enter values in **Threshold**.

   An error message is displayed if an **Item name** check box is selected but no value is specified for that item, an invalid value is entered in the text box, or nothing is entered.
5. If you will be running trend monitoring, select the **Trend monitor** check boxes for the items that you want to monitor under **SLO monitor settings**, and then enter the reference time for trend calculation.

   The **Trend monitor** check boxes are enabled only when **Item name** check boxes are selected. In the **Trend monitor** text box, enter the time to be subject to trend monitoring.

   An error message is displayed if a check box is selected but no value is specified for that item or an invalid value is entered in the text box. Note that there is no check box for **Error rate**, because trend monitoring is not applicable to error rate.
6. Under **Error Predict. settings**, enter appropriate values in **Days in baseline calculation** and **Days till start**.

   An error message is displayed if an invalid value or nothing is entered in a text box. If you will not be performing out-of-range value detection, leave the default values in **Days in baseline calculation** and **Days till start**.

7. If you will be performing out-of-range value detection, select the **Item name** check boxes for the items that you want to monitor under **Error Predict. settings** and then select their **Sensitivity** settings.

   Select an item that you want to monitor, and then select **High**, **Middle**, or **Low** as its sensitivity. As the sensitivity becomes higher, it becomes easier to detect the item. As the sensitivity becomes lower, it becomes harder to detect the item. Initially, set the sensitivity to **Middle**, and then you can adjust it later as needed after checking the number of items detected.

8. If you perform out-of-range value detection with multiple monitoring items combined, select **Throughput** from the **Correlated items** pull-down menu on the **Avg. response** row under **Error Predict. settings**.

9. Click the **Apply** button.

   If the monitoring items have been set up successfully, a dialog box to that effect is displayed.

When you click the **OK** button in the dialog box, the settings are applied.

(3) Next task

- *3.2.8 Setting up the monitoring items for system performance (working with Performance Management)*
- *4.2.1 Starting monitoring* (when not working with Performance Management)

(4) Related topics

- *3.1.2 Using out-of-range value detection for detection of unusual status in monitored services*
- *3.1.3 Using trend monitoring for detection in advance of threshold overages*
- *3.1.4 Using threshold value monitoring for detection of threshold overages*
- *5.2 User settings in ITSLM*
- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.18 Monitor settings area (monitored target within the monitored service selected in the Services area)*

3.2.8 Setting up the monitoring items for system performance (working with Performance Management)

You must set up monitoring items for each monitored service.

(1) Before you start

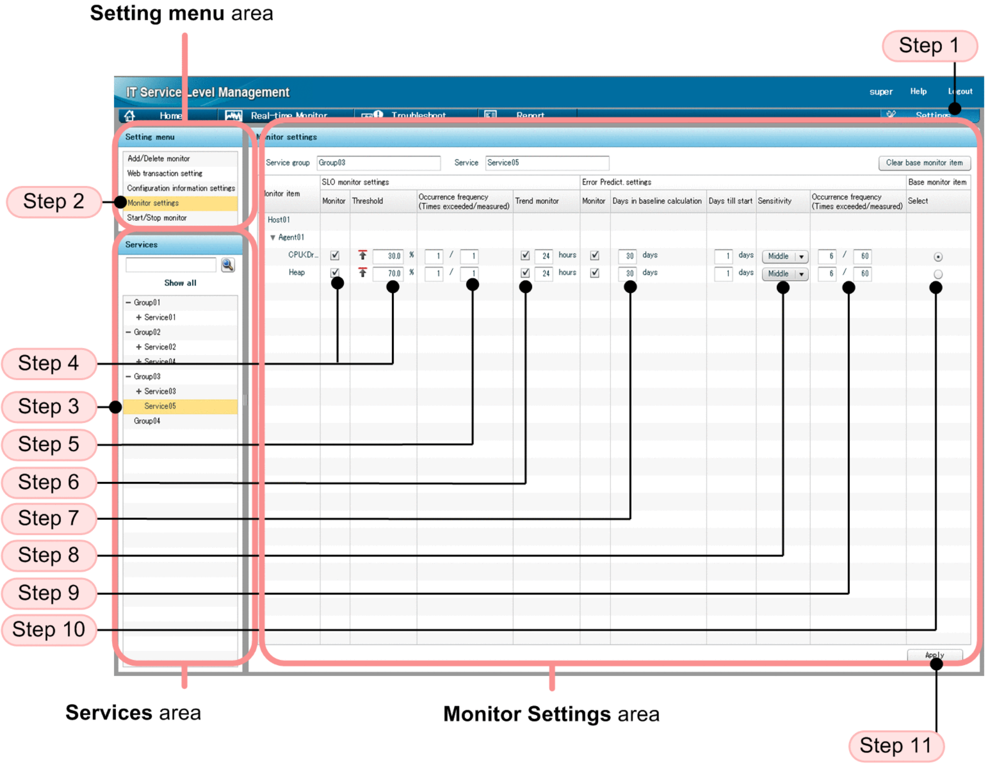
- Verify that you have the service group administrator permissions.
- Verify that the monitored service has been registered.

  For details about how to register monitored services, see *3.2.1 Registering monitored services*.
- Verify that monitoring of the monitored service for which monitoring items are to be set up has stopped.

  For details about how to stop monitoring, *4.2.2 Stopping monitoring*.
- Verify that configuration information for the monitored service has been specified. For details about specifying configuration information for monitored services, see *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)*.

(2) Procedure

The following shows the Settings window used in this procedure:



Service group: Group03 Service: Service05

Monitor item	SLO monitor settings				Error Predict. settings					Base monitor item
	Monitor	Threshold	Occurrence frequency (Times exceeded/measured)	Trend monitor	Monitor	Days in baseline calculation	Days till start	Sensitivity	Occurrence frequency (Times exceeded/measured)	Select
Host01										
▼ Agent01										
CPU<Dr...	☑	30.0 %	1 / 1	☑ 24 hours	☑	30 days	1 days	Middle ▾	6 / 60	●
Heap	☑	70.0 %	1 / 1	☑ 24 hours	☑	30 days	1 days	Middle ▾	6 / 60	○

To set up monitoring items for system performance:

1. Click the **Settings** button.

2. In the **Setting menu** area, select **Monitor settings**.

   The **Monitor settings** area is displayed.

3. From the **Services** area, select a monitored service.

   When you select a monitored service, the service group name, service name, and monitoring items subject to setup are displayed in the **Monitor settings** area. The current values are displayed under **SLO monitor settings** and **Error Predict. settings**. Immediately after a monitored service has been registered, the default values are set.

4. If you will be running threshold value monitoring or trend monitoring, select the **Monitor** check boxes for the items that you want to monitor under **SLO monitor settings**, and then enter values in **Threshold**.

   If ↑ (upper-limit threshold value) is displayed, specify an upper-limit threshold. If ↓ (lower-limit threshold value) is displayed, specify a lower-limit threshold.

   An error message is displayed if a **Monitor** check box is selected but no value is specified for that item or an invalid value is entered in the text box.

5. Under **SLO monitor settings**, specify **Occurrence frequency**.

   Specify a most recent measurement count for the denominator, and specify an excess count for the numerator. An error will be displayed when the specified excess count is exceeded.

6. If you will be running trend monitoring, select the **Trend monitor** check boxes for the items that you want to monitor under **SLO monitor settings**, and then enter the reference time for trend calculation.

The **Trend monitor** check boxes are enabled only when the **Monitor** check boxes are selected. In a **Trend monitor** text box, enter the time to be subject to trend monitoring.

An error message is displayed if a check box is selected but no value is specified for that item or an invalid value is entered in the text box.

7. Under **Error Predict. settings**, enter appropriate values in **Days in baseline calculation** and **Days till start**.

   An error message is displayed if an invalid value or nothing is entered in the text box. If you will not be performing an out-of-range value detection, clear the **Monitor** check box for **Error Predict. settings**.

8. If you will be performing out-of-range value detection, select the **Monitor** check boxes for the items that you want to monitor under **Error Predict. settings**, and then select their **Sensitivity** settings.

   Select an item that you want to monitor, and then select **High**, **Middle**, or **Low** as its sensitivity. As the sensitivity becomes higher, it becomes easier to detect the item. As the sensitivity becomes lower, it becomes harder to detect the item. Initially, set the sensitivity to **Middle**, and then you can adjust it later as needed after checking the number of items detected.

9. Under **Error Predict. settings**, specify **Occurrence frequency**.

   Specify a most recent measurement count for the denominator, and an excess count for the numerator. An error will be displayed when the specified excess count is exceeded.

10. Select **Base monitor item**.

    If the service's monitoring configuration is **System**, the **Base monitor item** radio buttons and the **Clear base monitor item** button are displayed.

    Select the **Base monitor item** radio button corresponding to the monitoring item to be used as the base for determining the dates used for obtaining the baseline for out-of-range value detection.

    If no monitoring item is selected, the service's throughput will be used as the base.

11. Click the **Apply** button.

    If the monitoring items have been set up successfully, a dialog box to that effect is displayed.

When you click the **OK** button in the dialog box, the settings are applied.

(3) Next task

- *4.2.1 Starting monitoring*

(4) Related topics

- *3.1.2 Using out-of-range value detection for detection of unusual status in monitored services*
- *3.1.3 Using trend monitoring for detection in advance of threshold overages*
- *3.1.4 Using threshold value monitoring for detection of threshold overages*
- *5.2 User settings in ITSLM*
- *10.6.1 Configuration of the Settings window*
- *10.1.2(3) Services area*
- *10.6.3 Setting menu area*
- *10.6.19 Monitor settings area (monitored service selected in the Services area)*

3.2.9 Notes about setting up monitoring items

(1) Timing of updating the number of registered monitored targets

If a service group administrator adds or deletes a monitored target while multiple users are logged in to ITSLM - Manager, the change will be applied to the other monitoring persons' windows when the number of registered monitored targets is updated. The number of registered monitored targets is updated, excluding during re-login, when a monitoring person accesses a monitored target that was deleted by the service group administrator or when the window is refreshed automatically. Until the number of registered monitored targets is updated, the status in effect before the service group administrator added or deleted monitored targets is maintained.

The following table describes the timing of updating the registered monitored targets.

Table 3–9: Timing of updating the registered monitored targets

No.	Window accessed by a monitoring person other than the service group administrator	Update timing
1	IT Service Level Management window	• When a monitoring person re-logs in.
2	Home window	• When **Details** for a deleted monitored target is clicked in the **Events in the last 7 days** area. • When **Unread** is clicked in the **Events in the last 7 days** area while **Status** for a deleted monitored target's event is **Unread**. • When the window is refreshed automatically after a monitoring target was deleted.
3	Real-time Monitor window	• When an already deleted monitored target is selected in the **Services** area (if a deleted monitored target was already selected, another service was selected, and then the deleted monitored target is selected again). • When an already deleted monitored target is selected in the **Service performance information** area. • When the value for **Display interval** is changed while a chart for an already deleted monitored target is being displayed on the **Performance chart** tab. • When the **Troubleshoot** button on the **Performance chart** tab is clicked while a chart for an already deleted monitored target is being displayed on the **Performance chart** tab. • When **Details** is clicked while an already deleted monitored target is being displayed on the **Event** tab. • When **Unread** is clicked while **Status** of a deleted monitored target's event is **Unread** on the **Event** tab. • When the window is refreshed automatically after a monitoring target was deleted.
4	Troubleshoot window	• When an already deleted monitored target is selected in the **Services** area (if a deleted monitored target was already selected, another monitored target was selected, and then the deleted monitored target is selected again, or the ⟳ (reload) button is clicked). • When the **Details** button for an already deleted monitored target on the **Event** tab is clicked. • When **Unread** on the **Event** tab is clicked while **Status** of a deleted monitored target's event is **Unread**. • When the ⟳ (reload) button is clicked while an event of a deleted monitored target is being displayed on the **Event** tab. • When the logging range is changed by dragging a chart when the chart displays a deleted monitored target on the **Performance chart** tab. • When the value for **Display interval** is changed while a chart for a deleted monitored target is being displayed on the **Performance chart** tab.

No.	Window accessed by a monitoring person other than the service group administrator	Update timing
5	Report window	• When an attempt is made to display a report for a deleted monitored target.
6	Settings window	• When the **Add/Delete monitor** area is displayed. • When a monitored service is added or deleted in the **Add/Delete monitor** area (if the **Start/Stop monitor** area is already displayed, it is displayed again). • When an already deleted monitored target is selected in the **Services** area with the **Monitor settings** area displayed (if a deleted monitored target was already selected, another monitored target was selected, and then the deleted monitored target is selected again). • When an attempt is made to add monitor settings for a deleted monitored target in the **Monitor settings** area. • When a Web transaction is added or deleted in the **Web transaction setting** area. • When an already deleted monitored target is selected in the **Web transaction setting** area and then the **Edit** or **Delete** button is clicked. • In the **Web transaction setting** area, a Web transaction of a deleted monitored target was selected, and then the **Edit** or **Delete** button was clicked. • When the **Start/Stop monitor** area is displayed (if the **Start/Stop monitor** area was already displayed, the **Start/Stop monitor** area is displayed again). • When an attempt is made to start or stop monitoring of an already deleted monitored service in the **Start/Stop monitor** area.

When any of the above operations is performed, an error message is displayed and the current window is refreshed. The refreshed window is in newly opened status. Any data, such as numeric values, that was entered in the window before the window was refreshed is not retained.

(2) Character strings displayed as monitoring item names (working with Performance Management)

When the language setting of the OS on which ITSLM - Manager is installed is Japanese and **Monitor item name displayed on ITSLM (Japanese)** is specified in Performance Management, the values as specified are displayed for monitoring item names. Check if the language setting of the OS on which ITSLM - Manager is installed is Japanese.

When **Monitor item name displayed on ITSLM (Japanese)** is not specified in Performance Management, the values for **Monitor item name displayed on ITSLM (English)** are displayed. For details about the monitoring items, see the applicable PFM - Agent or PFM - RM manual.

(3) Notes about units used in ITSLM windows (working with Performance Management)

When the language setting of the OS on which ITSLM - Manager is installed is Japanese and **Monitor item name displayed on ITSLM (Japanese)** is specified in Performance Management, the values as specified are displayed as the units for monitoring items for system performance that are displayed in ITSLM. Check if the language setting of the OS on which ITSLM - Manager is installed is Japanese.

When **Monitor item name displayed on ITSLM (Japanese)** is not specified in Performance Management, the values for **Monitor item name displayed on ITSLM (English)** or the units specified in the custom monitoring item definition are displayed. For details about the monitoring items, see the applicable PFM - Agent or PFM - RM manual.

(4) Notes about configuration information that differs between ITSLM and Performance Management (working with Performance Management)

If a business group's reference permissions have been changed or the configuration has been changed, ITSLM - Manager can still use the previous reference permissions to start and stop monitoring until the business group is updated in ITSLM - Manager. The following table explains ITSLM's behavior when monitoring of a business group is started or stopped while changes to the business group's configuration information have not yet been applied by ITSLM - Manager.

Table 3–10: ITSLM's behavior when configuration information does not match between ITSLM and Performance Management

No.	Configuration information whose change has not been applied	Processing	ITSLM's behavior
1	Addition of business group permissions	Start monitoring.	Monitoring is started successfully.
2		Stop monitoring.	Monitoring is stopped successfully.
3	Deletion of business group permissions	Start monitoring.	Monitoring is started successfully.
4		Stop monitoring.	Monitoring is stopped successfully.
5	Addition of a host	Start monitoring.	Monitoring is started successfully for the monitoring items in the configuration information that has already been applied to ITSLM. The monitoring items for an added host that has not been applied are not processed.
6		Stop monitoring.	Monitoring is stopped successfully.
7	Deletion of a host	Start monitoring.	A message indicating that the configuration information does not match is output to a log file and the monitoring start processing on monitoring items for the deleted host fails.
8		Stop monitoring.	A message indicating that the configuration information does not match is output to a log file and monitoring is stopped successfully.
9	Addition of a monitoring agent	Start monitoring.	Monitoring is started successfully for the monitoring items in the configuration information that has already been applied to ITSLM. The monitoring items for an added monitoring agent that has not been applied are not processed.
10		Stop monitoring.	Monitoring is stopped successfully.
11	Deletion of a monitoring agent	Start monitoring.	A message indicating that the configuration information does not match is output to a log file and the monitoring start processing on monitoring items for the deleted monitoring agent fails.
12		Stop monitoring.	A message indicating that the configuration information does not match is output to a log file and monitoring is stopped successfully.

No.	Configuration information whose change has not been applied	Processing	ITSLM's behavior
13	Change to the data model of a monitoring agent	Start monitoring.	A message indicating that the configuration information does not match is output to a log file and the monitoring start processing for the monitoring agent whose data model has changed fails.
14		Stop monitoring.	Monitoring is stopped successfully.

(5) Notes about monitoring items with the same display names (working with Performance Management)

If more than one monitoring item has the same display name in the Performance Management settings, the duplicately-named monitoring items cannot be distinguished in the ITSLM windows. To change the display names of monitoring items, change the definition values for custom monitoring items in PFM - Manager. For details about the monitoring items, see the applicable PFM - Agent or PFM - RM manual.

(6) About monitoring items with multi-instance records (working with Performance Management)

Monitoring items with multi-instance records depend on the monitoring agent. For details about the monitoring items for each monitoring agent, see the applicable PFM - Agent or PFM - RM manual.

(7) Notes about collecting performance data by linking with Performance Management (working with Performance Management)

To be able to reference data related to system performance by connecting to PFM - Web Console, the **Log** property must be set to **Yes** in Performance Management. For details, see *5.4.2 Specifying settings for saving Performance Management's performance data from ITSLM (working with Performance Management)*.

3.3 Examples of setup of the monitoring items

This section explains setup of monitoring items for the following examples discussed in Chapter 1:

- Predictive error detection in the performance of monitored services and the corrective action support methodology
- Predictive error detection in the performance of processes in monitored services and the corrective action support methodology
- Predictive system error detection in the performance of systems running monitored services and the corrective action support methodology
- Periodic evaluation of the status of monitored services

3.3.1 Example of setup for predictive error detection in the performance of monitored services and the corrective action support methodology

This subsection explains an example of predictive error detection in the performance of monitored services and the corrective action support methodology, as discussed in *1.1.2 Monitoring service status*.

This subsection explains by way of example how to perform evaluation and setup based on given conditions to support predictive error detection in the performance of monitored services and the corrective actions to take.

(1) Prerequisites

The following are the conditions for this setup example:

- There is a service level agreement (SLA) regarding the service quality (service level) between the service's outsourcing company (service provider) and an outsourced contractor (data center). The data center is required to maintain the service level based on the SLA.
- The outsourced services are registered as monitored services as shown below, and monitoring of the monitored services has stopped.
  - Service group: `Group01`

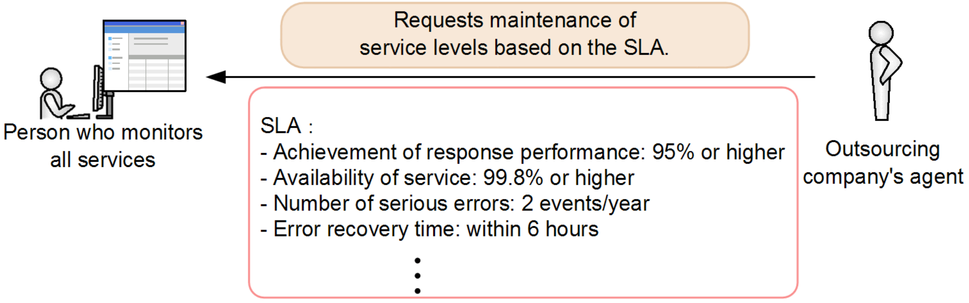
    Services belonging to service group `Group01`: `Service01` to `Service03`
  - Service group: `Group02`

    Services belonging to service group `Group02`: `Service04` and `Service05`
  - Service group: `Group03`

    Service belonging to service group `Group03`: `Service06`
  - Service group: `Group04`

    Service belonging to service group `Group04`: `Service07`
- The following figure shows the relationship among the personnel involved in this task.

Figure 3–30: Relationship among personnel involved in predictive error detection in the performance of monitored services and the corrective action support methodology (setup example)


Requests maintenance of service levels based on the SLA.
Person who monitors all services
Outsourcing company's agent

SLA :
- Achievement of response performance: 95% or higher
- Availability of service: 99.8% or higher
- Number of serious errors: 2 events/year
- Error recovery time: within 6 hours

⋮

- Person who monitors all services

  Determines the SLO for each monitoring item based on the SLA, and then sets up the monitoring items in the Settings window.
- Outsourcing company's agent

  This person is in charge of providing the services outsourced in the agreement. The person who monitors all services is responsible for managing the service level for the outsourced services.

(2) Defining SLOs from the SLA

Tasks required for setting up monitoring items in ITSLM

The person who monitors all services checks the SLA and evaluates the SLOs for thresholds.

Because the SLA contains requirements, including that achievement of response performance be 95% or higher and availability of service be 99.8% or higher, the person who monitors all services defines the SLOs as follows:

- Average response time: 3,000 milliseconds
- Throughput: 800 count/second
- Error rate: 1.0%

The person who monitors all services also decides to perform out-of-range value detection in addition to monitoring based on thresholds as SLOs because warning signs of service performance errors must be detected and handled.

Results of the tasks

Because SLOs have been defined, the person who monitors all services decides to set up monitoring items for each monitored service.

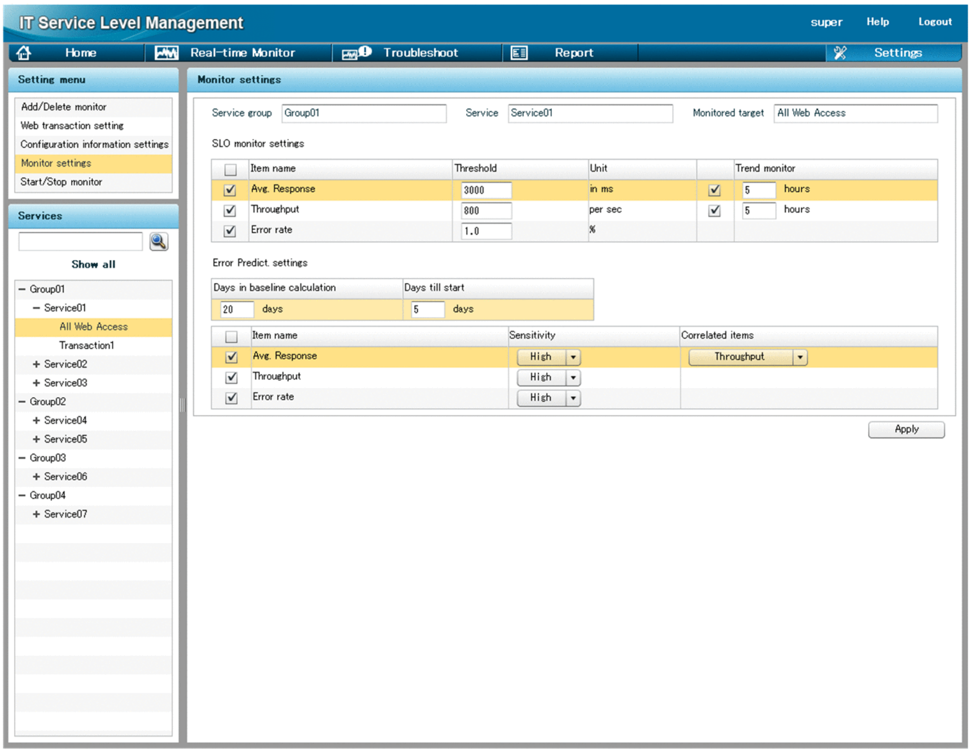
(3) Setting up monitoring items

Tasks in ITSLM

The person who monitors all services decides to log in to ITSLM - Manager to display the Settings window and set up monitoring items for the monitored services based on the defined SLOs.

The following shows a setup example of monitoring items for the monitored services based on the SLOs.

Figure 3–31: Setup example of monitoring items for the monitored services based on the SLOs



Service group Group01 Service Service01 Monitored target All Web Access

SLO monitor settings

□	Item name	Threshold	Unit		Trend monitor
☑	Avg. Response	3000	in ms	☑	5 hours
☑	Throughput	800	per sec	☑	5 hours
☑	Error rate	1.0	%		

Error Predict. settings

Days in baseline calculation	Days till start
20 days	5 days

□	Item name	Sensitivity	Correlated items
☑	Avg. Response	High ▾	Throughput ▾
☑	Throughput	High ▾	
☑	Error rate	High ▾	

This example sets up monitoring items for service `Service01` of service group `Group01`. The following shows the settings for the monitoring items.

SLO monitor settings

Table 3–11: Example settings under SLO monitor settings

Check box	Item name	Threshold	Check box	Trend monitoring
Selected	**Avg. response**	`3000`	Selected	`5`
Selected	**Throughput**	`800`	Selected	`5`
Selected	**Error rate**	`1.0`	--	--

Legend:

--: Cannot be set

Under **SLO monitor settings**, the SLO definition items are specified as thresholds, and then trend monitoring is set up for average response time and throughput so as to promptly detect any error in the performance of a monitored service.

A potential service performance error must be detected at least five hours in advance because other personnel must be contacted to take corrective action in the event of a service performance error. For this reason, trend monitoring is set to 5 hours.

Error Predict. settings

Table 3–12: Example settings under Error Predict. settings

Days in baseline calculation	Days till start	Check box	Item name	Sensitivity	Correlated item
`20`	`5`	Selected	**Avg. response**	**High**	**Throughput**
		Selected	**Throughput**	**High**	--
		Selected	**Error rate**	**High**	--

Legend:

--: Cannot be set

Under **Error Predict. settings**, 20 days' worth of service performance is to be used to calculate the baseline for performing monitoring based on typical service performance. **Days till start** is set to 5 because it was requested that monitoring be started five days later.

Out-of-range value detection is to be performed for all monitoring items. The sensitivity is set to high so that any service performance that veers from the baseline will be detected quickly. Out-of-range value detection with multiple monitoring items combined is also to be performed to improve the precision of out-of-range value detection.

Results of the tasks

Once setup has been completed for service `Service01` of service group `Group01`, the person who monitors all services proceeds to set up monitoring items for the remaining monitored services in the same manner.

After setup has been completed for all monitored services, the person who monitors all services decides to perform monitoring. For an example of execution of monitoring, see *4.6.1 Example of execution for predictive error detection in the performance of monitored services and the corrective action support methodology*.

3.3.2 Example of setup for predictive error detection in the performance of processes in monitored services and the corrective action support methodology

This subsection explains an example of predictive error detection in the performance of processes in a monitored service and the corrective action support methodology, as discussed in *1.1.2 Monitoring service status*.

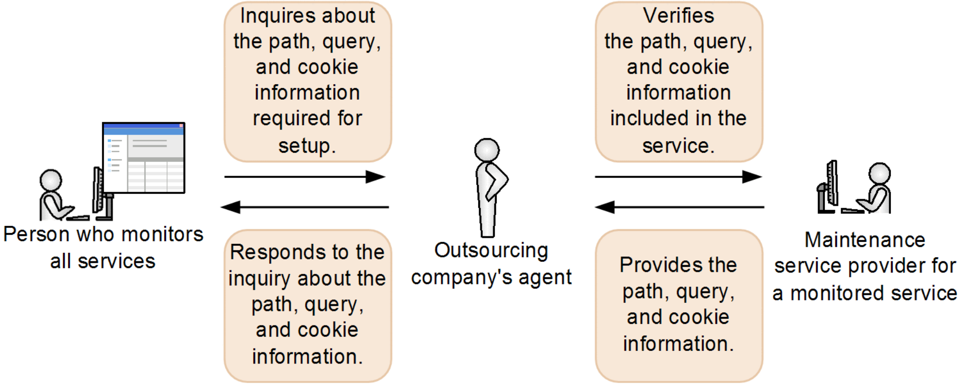
This subsection explains by way of example how to perform evaluation and setup based on given conditions to support predictive error detection in the performance of processes in a monitored service and the corrective actions to take.

(1) Prerequisites

The following are the conditions for this setup example:

- The service group and monitored services have been registered in the same manner as in *3.3.1 Example of setup for predictive error detection in the performance of monitored services and the corrective action support methodology*.
- New processes are scheduled to be added to service `Service01` of server group `Group01` and those processes to be added are not running yet. For the processes that will be added, the average response time, throughput, and error rate values have been determined as system requirements by the service's outsourcing company.
- Monitoring of service `Service01` of server group `Group01` is stopped.
- The following figure shows the relationship among the personnel involved in this task.

Figure 3–32: Relationship among personnel involved in predictive error detection in the performance of processes in a monitored service and the corrective action support methodology (setup example)


Inquires about the path, query, and cookie information required for setup.
Verifies the path, query, and cookie information included in the service.
Person who monitors all services
Outsourcing company's agent
Maintenance service provider for a monitored service
Responds to the inquiry about the path, query, and cookie information.
Provides the path, query, and cookie information.

- Person who monitors all services

  Sets up Web transactions in the Settings window on the basis of the paths, queries, and cookie information obtained from maintenance service engineers for the services via the outsourcing company's agent. This person also evaluates the thresholds for the monitoring items based on the system requirements, and then sets up the monitoring items in the Settings window.

- Outsourcing company's agent

  This person is in charge of providing the services outsourced in the agreement. The person who monitors all services is responsible for managing the service level for the outsourced services. If contacted by the person who monitors all services regarding internal information about a monitored service, such as path, query, and cookie information, this person verifies the information with the maintenance personnel in charge of the monitored service.

- Maintenance service provider for a monitored service

  This is a service engineer who participated in development of the service and who is stationed at the service users' location to provide support. If there are questions about the monitored service from the outsourcing company's agent, this person provides the necessary information.

(2) Defining Web access conditions based on the paths, queries, and cookie information and defining thresholds based on the system requirements

Tasks required for setting up Web transactions in ITSLM

The person who monitors all services obtains the paths, queries, and cookie information for the processes to be monitored from the maintenance service engineers for the services via the outsourcing company's agent. This person also evaluates the thresholds for monitoring items based on the system requirements for the monitored processes. The following table shows the Web access conditions, session conditions, and thresholds for the monitoring items that are defined on the basis of the obtained paths, queries, and cookie information and the system requirements.

- Web access conditions

Web access condition	Path	Query	Cookie

Web access condition 1	`/top.html`	`q=.*`
		`time=.*`
			`session=.*`
			`exp=10`

Web access condition 2	`/middle.html`	`q=.*`	`session=.*`
			`exp=10`

Web access condition 3	`/bottom.html`	`q=.*`	`session=.*`

Web access condition	Path	Query	Cookie
Web access condition 3	/bottom.html	q=.*	exp=10

Web access condition 4	example/index.html	q=.*
		qqq=1
			session=.*

- Session conditions

  Query condition: q

  Cookie condition: session

- Thresholds for monitoring items

  Average response time: 3,000 milliseconds

  Throughput: 800 count/second

  Error rate: 1.0%

The person who monitors all services also decides to perform out-of-range value detection in addition to monitoring based on thresholds because warning signs of service performance errors must be detected and handled.

Results of the tasks

The person who monitors all services decides to name the Web transaction Transaction1 and sets up the defined Web access conditions. This person also decides to set up monitoring items after setting up the Web access conditions for Transaction1.

(3) Setting up the Web transaction

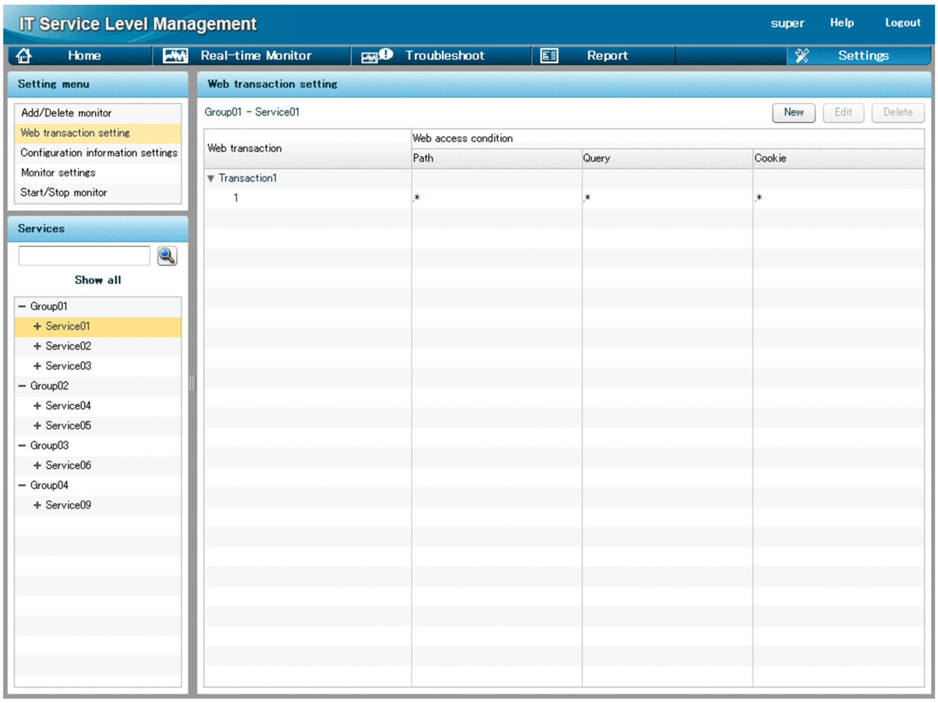
Tasks in ITSLM

The person who monitors all services decides to set up the Web transaction based on the information obtained from the maintenance service engineer for the service. The Web access conditions for the Web transaction are imported from the automatically detected URI. The following procedure is performed for this setup:

1. Log in to ITSLM - Manager, and then display the **Web transaction setting** area in the Settings window.

   The following shows the **Web transaction setting** area in the Settings window.

Figure 3–33: Web transaction setting area in the Settings window (setup example)



Group01 - Service01

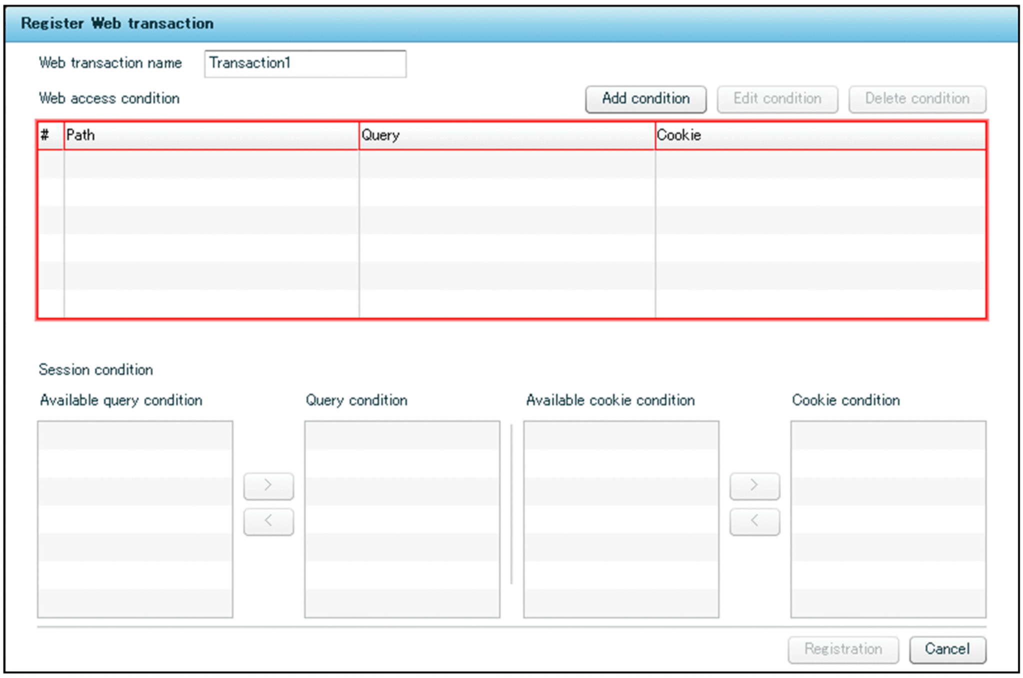
Web transaction	Web access condition		
	Path	Query	Cookie
▼ Transaction1			
1	*	*	*

This example sets up a Web transaction for service `Service01` of service group `Group01`.

2. Select `Service01` of `Group01` in **Services**, then click the **New** button to display the Register Web transaction window to set up each item of the Web transaction.

   The following shows the Register Web transaction window.

Figure 3–34: Register Web transaction window (setup example)



Web transaction name: Transaction1

Web access condition

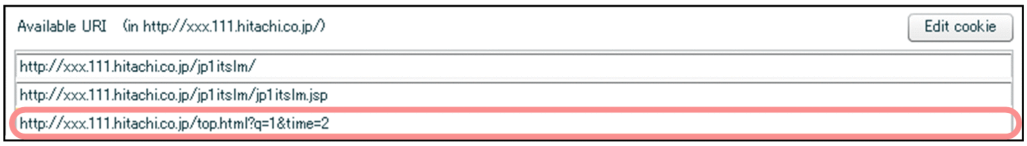
#	Path	Query	Cookie

In this example, `Transaction1` is entered as the Web transaction name.

3. Click the **Add condition** button to display the Add Web access condition window to set up Web access conditions for Web transaction `Transaction1`.

4. Click the **Start detection** button to import Web access conditions from automatically detected URIs. The following shows an example of the detection results.

Figure 3–35: Example of detected URIs



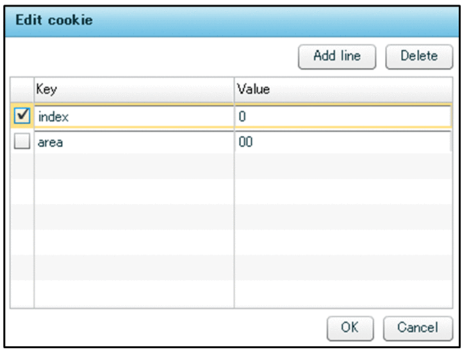
http://xxx.111.hitachi.co.jp/jp1itslm/
http://xxx.111.hitachi.co.jp/jp1itslm/jp1itslm.jsp
http://xxx.111.hitachi.co.jp/top.html?q=1&time=2

In this example, the URI on the third line is edited and Web access conditions are imported. The path is `top.html` and query is `q=1` and `time=2`. The example retains the path as is and changes the query to `q=.*` and `time=.*` to match Web access condition 1.

5. While the URI on the third line is selected, click the **Edit cookie** button to edit the cookie to match Web access condition 1.

   The following shows the Edit cookie window.

Figure 3–36: Edit cookie window (setup example)



	Key	Value
☑	index	0
☐	area	00

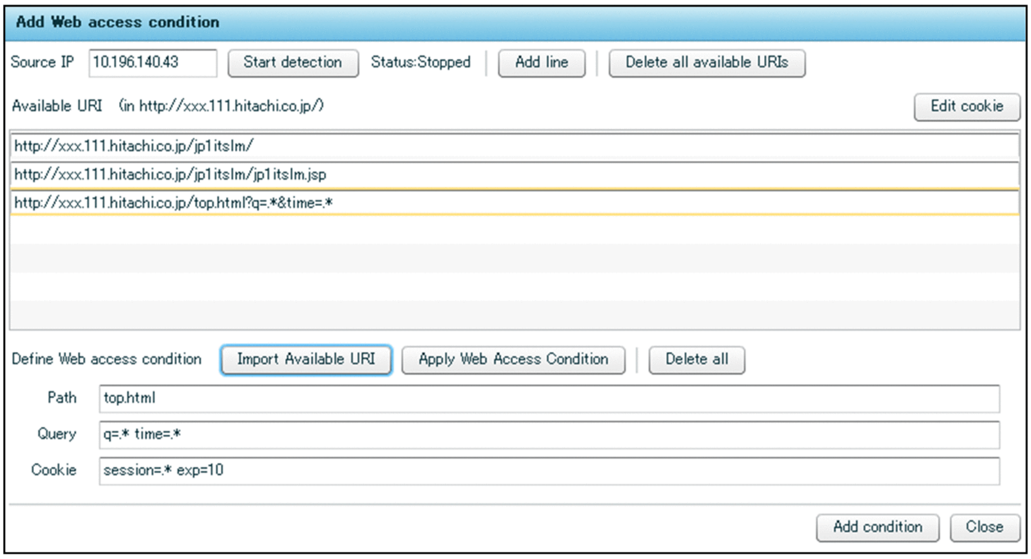
In this figure, a cookie is set to `index=0` and `area=00`. The example edits the text box and changes the cookie to `session=.*` and `exp=10` so that it matches Web access condition 1.

6. Verify that **Available URI** matches Web access condition 1, and then click the **Import Available URI** button while the URI on the third line is selected.

   The same path, query, and cookie information as for the URI on the third line are displayed in **Define Web access condition**.

   The following shows an example of the Add Web access condition window that displays the path, query, and cookie information.

Figure 3–37: Example of Add Web access condition window that displays the path, query, and cookie information



Source IP 10.196.140.43

Status:Stopped

Available URI (in http://xxx.111.hitachi.co.jp/)

http://xxx.111.hitachi.co.jp/jp1itslm/
http://xxx.111.hitachi.co.jp/jp1itslm/jp1itslm.jsp
http://xxx.111.hitachi.co.jp/top.html?q=.*&time=.*

Define Web access condition

Path: top.html

Query: q=.* time=.*

Cookie: session=.* exp=10

By clicking the **Apply Web Access Condition** button in this status, you can verify whether the entered **Define Web access condition** matches the target Web access.

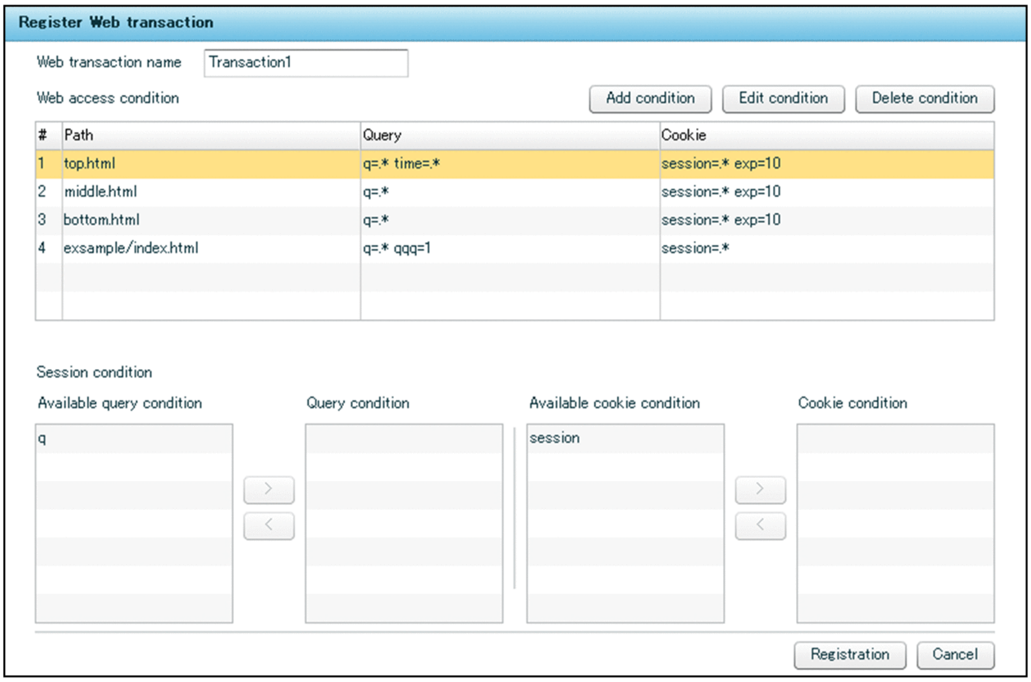
7. Once the Web access condition definition has been entered, click the **Add condition** button.

   Web access condition 1 is added to `Transaction1`.

8. After Web access condition 1 has been added, add the remaining Web access conditions in the same manner. When all four Web access conditions have been added, click the **Close** button to display the Register Web transaction window again.

   The following shows the Register Web transaction window in which the Web access conditions have been added.

Figure 3–38: Register Web transaction window in which Web access conditions have been added (setup example)



Web transaction name: Transaction1

Web access condition

#	Path	Query	Cookie
1	top.html	q=.* time=.*	session=.* exp=10
2	middle.html	q=.*	session=.* exp=10
3	bottom.html	q=.*	session=.* exp=10
4	exsample/index.html	q=.* qqq=1	session=.*

Session condition

Available query condition: q

Query condition:

Available cookie condition: session

Cookie condition:

9. After you have added the Web access conditions, specify session conditions to identify Web access users. From **Available query condition**, select **q** to move to **Query condition**, and then from **Available cookie condition**, select **session** to move to **Cookie condition**.

   After you have finished specifying the session conditions, click the **Registration** button to register `Transaction1`.

Results of the tasks

Once `Transaction1` has been registered, the person who monitors all services decides to set up monitoring items for `Transaction1`.

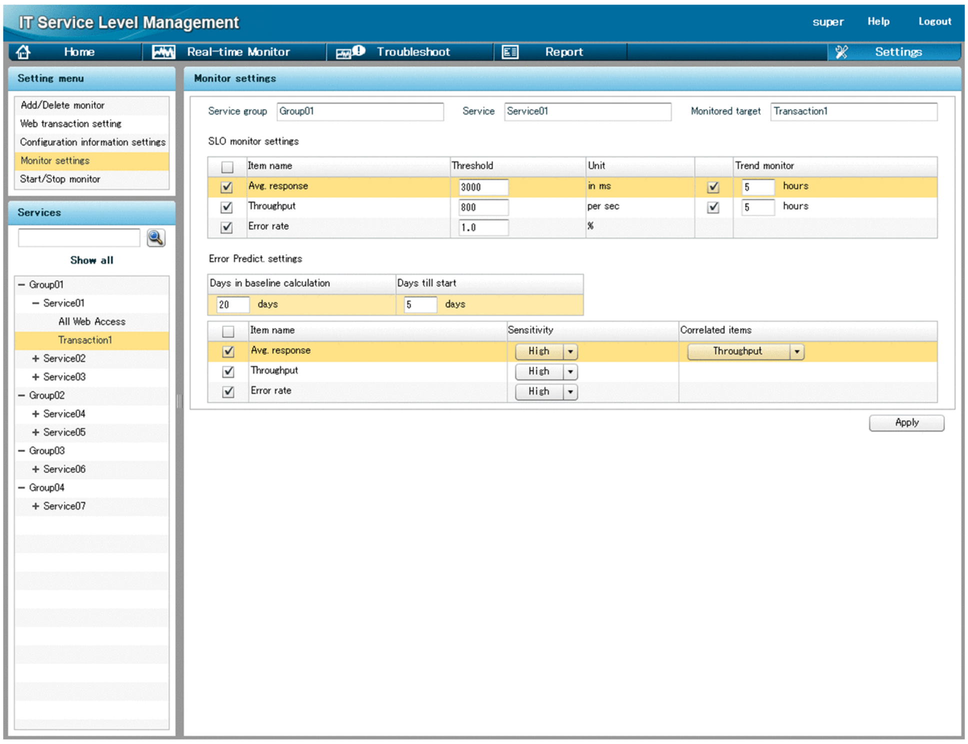
(4) Setting up monitoring items

Tasks in ITSLM

The person who monitors all services decides to display the **Monitor settings** area in the Settings window and set up monitoring items for the Web transaction.

The following shows a setup example of the monitoring items for the Web transaction.

Figure 3–39: Setup example of monitoring items for the Web transaction



Service group: Group01 Service: Service01 Monitored target: Transaction1

SLO monitor settings

□	Item name	Threshold	Unit		Trend monitor
☑	Avg. response	3000	in ms	☑	5 hours
☑	Throughput	800	per sec	☑	5 hours
☑	Error rate	1.0	%		

Error Predict. settings

Days in baseline calculation	Days till start
20 days	5 days

□	Item name	Sensitivity	Correlated items
☑	Avg. response	High	Throughput
☑	Throughput	High	
☑	Error rate	High	

This example sets up monitoring items for `Transaction1` of service `Service01` of server group `Group01`. The following shows the settings for the monitoring items.

SLO monitor settings

Table 3–13: Example settings under SLO monitor settings

Check box	Item name	Threshold	Check box	Trend monitoring
Selected	**Avg. response**	`3000`	Selected	`5`
Selected	**Throughput**	`800`	Selected	`5`
Selected	**Error rate**	`1.0`	--	--

Legend:

--: Cannot be set

Under **SLO monitor settings**, the SLO definition items are specified as thresholds, and then trend monitoring is set up for average response time and throughput so as to promptly detect any error in the performance of the monitored service.

A potential service performance error must be detected at least five hours in advance because other personnel must be contacted to take corrective action in the event of a service performance error. For this reason, trend monitoring is set to 5 hours.

Error Predict. settings

Table 3–14: Example settings under Error Predict. settings

Days in baseline calculation	Days till start	Check box	Item name	Sensitivity	Correlated item
20	5	Selected	**Avg. response**	**High**	**Throughput**
		Selected	**Throughput**	**High**	--
		Selected	**Error rate**	**High**	--

Legend:

--: Cannot be set

Under **Error Predict. settings**, 20 days' worth of service performance is to be used to calculate the baseline for performing monitoring based on typical service performance. **Days till start** is set to 5 because it was requested that monitoring be started five days later.

Out-of-range value detection is to be performed for all monitoring items. The sensitivity is set to high so that any service performance that veers from the baseline will be detected quickly. Out-of-range value detection with multiple monitoring items combined is also to be performed to improve the precision of out-of-range value detection.

Results of the tasks

After setup of Web transaction Transaction1 and of the monitoring items for Service01 has been completed, the person who monitors all services decides to perform monitoring of Service01 and Transaction1. For an example of execution of monitoring, see *4.6.2 Example of execution for predictive error detection in the performance of processes in monitored services and the corrective action support methodology*.

3.3.3 Example of setup for predictive error detection in the performance of systems running monitored services and the corrective action support methodology (working with Performance Management)

This subsection explains an example of predictive error detection in the performance of systems running monitored services, as discussed in *1.2 Linking with Performance Management to monitor service status (working with Performance Management)*.

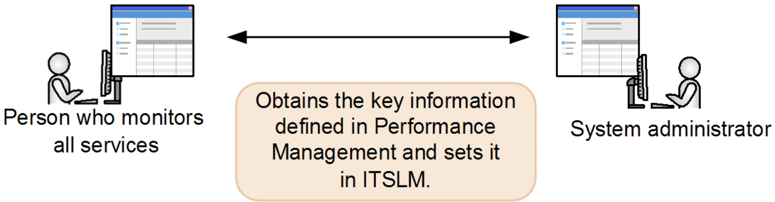
This subsection explains by way of example how to perform evaluation and setup based on given conditions to support predictive error detection in the system performance of hosts and middleware that provide monitored services and the corrective actions to take.

(1) Prerequisites

The following are the conditions for this setup example:

- There is a service level agreement (SLA) regarding the service quality (service level) between the service's outsourcing company (service provider) and an outsourced contractor (data center). The data center is required to maintain the service level based on the SLA. SLOs defined on the basis of the SLA are specified in the same manner as in *3.3.1 Example of setup for predictive error detection in the performance of monitored services and the corrective action support methodology*.
- The service group and monitored services have been registered in the same manner as in *3.3.1 Example of setup for predictive error detection in the performance of monitored services and the corrective action support methodology*. Monitoring of the monitored services has stopped.
- The following figure shows the relationship among the personnel involved in this task.

Figure 3–40: Relationship among personnel involved in predictive error detection in the performance of systems running monitored services and the corrective action support methodology (setup example)


Person who monitors all services
Obtains the key information defined in Performance Management and sets it in ITSLM.
System administrator

  - Person who monitors all services

    Adds the monitoring items for system performance for the services for which SLOs are defined.

    To monitor the monitoring items for system performance in ITSLM, this person verifies the settings in Performance Management with the system administrator.
  - System administrator

    The system administrator defines the monitoring items for system performance in Performance Management. This person provides the information needed for monitoring system performance in ITSLM to the person who monitors all services.

(2) Collecting key field information for monitoring items

This subsection explains an example of multi-instance monitoring items. For single-instance monitoring items, there is no need to define key field information.

Tasks required for setting up monitoring items in ITSLM

The person who monitors all services asks the system administrator to provide the information needed to monitor system performance in ITSLM. The system administrator checks the key field information (multi-instance records) collected by Performance Management and provides the information to the person who monitors all services. For an example of multi-instance records collected by Performance Management, see *3.1.1(7) Monitoring items for system performance*.

Results of the tasks

Because the key field information has been verified, the person who monitors all services decides to set up monitoring items for the system providing each monitored service.

(3) Setting up monitoring items

Tasks in ITSLM

The two types of monitoring item setup tasks are configuration information setup and monitoring setup. These types are explained below.

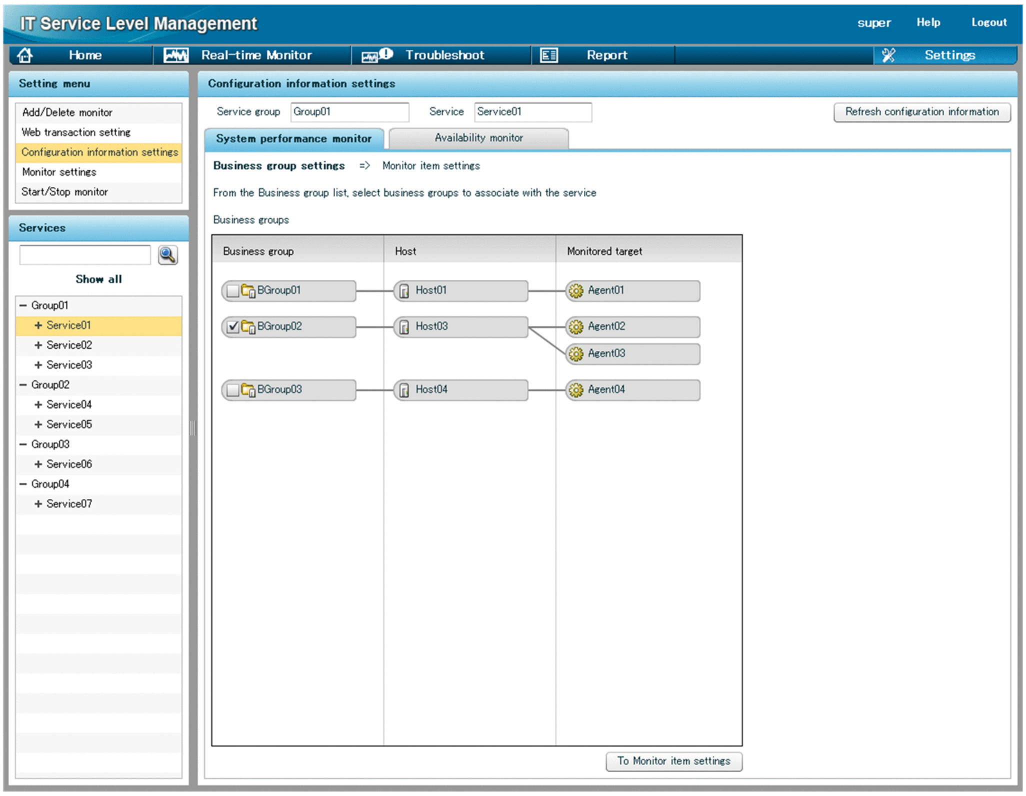
- Configuration information setup

The person who monitors all services decides to log in to ITSLM - Manager, display the Settings window, and then set up the configuration information.

To monitor system performance, you first set up configuration information for the monitored service. Setting up configuration information involves associating the business group with the monitored service and then setting up the monitored target. Monitoring items (such as CPU, HDD, and HEAP) are also set up for the monitored target.

The following shows an example of the setup.

Figure 3–41: Setup example of configuration information (business group setup)



Service group Group01

Service Service01

Business group settings => Monitor item settings

From the Business group list, select business groups to associate with the service

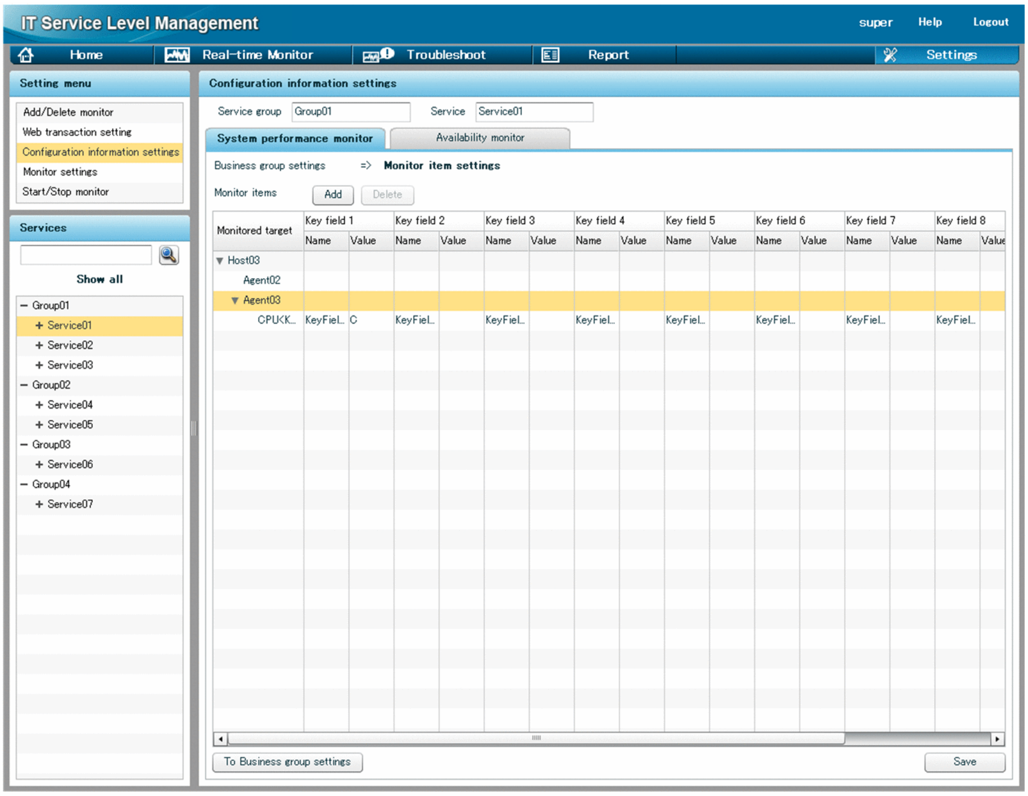
In this figure, the business group to be associated with service `Service01` of service group `Group01` is selected.

Business group `BGroup2` is associated with host `Host03`. Because `Agent02` and `Agent03` are running on host `Host03`, data collected by `Agent02` and `Agent03` will be monitored by ITSLM.

After selecting the business group, click the **To Monitor item settings** button to set up monitoring items for the monitored target.

The following shows an example of the setup.

Figure 3–42: Setup example of configuration information (monitoring item setup)



Service group: Group01 Service: Service01

Monitored target	Key field 1		Key field 2		Key field 3		Key field 4		Key field 5		Key field 6		Key field 7		Key field 8	
	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value
▼ Host03																
Agent02																
▼ Agent03																
CPU(K...	KeyFiel...	C	KeyFiel...		KeyFiel...		KeyFiel...		KeyFiel...		KeyFiel...		KeyFiel...		KeyFiel...	

Monitoring items can be set up for monitored target `Agent03`. Specify in monitoring item setup whether system information measured by Performance Management is to be associated with the monitored service for which the business group has been set.

In this figure, monitoring item **CPU** is set up for `Agent03`. For the value of **Key field 1**, **C** specified in Performance Management is specified.

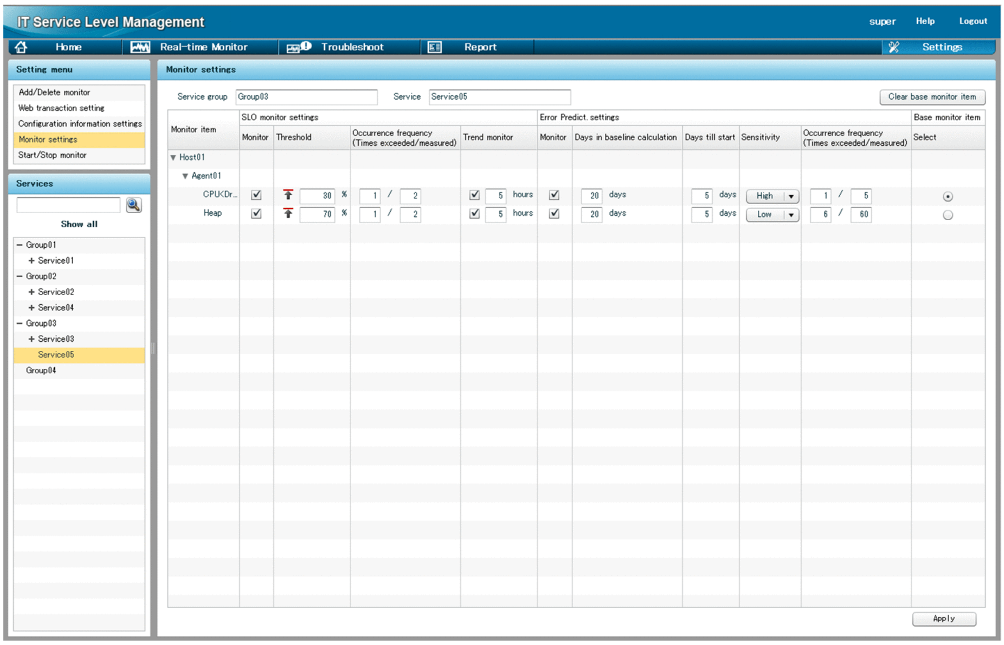
- Monitoring setup

Once the configuration information has been set up, the person who monitors all services decides to specify the details of monitoring.

Based on the SLOs, monitoring items for the system that provides the monitored service are set up.

The following shows an example of the setup.

Figure 3‒43: Setup example of monitoring items for the system that provides the monitored service based on SLOs



Service group: Group03

Service: Service05

Monitor item	SLO monitor settings				Error Predict. settings					Base monitor item
	Monitor	Threshold	Occurrence frequency (Times exceeded/measured)	Trend monitor	Monitor	Days in baseline calculation	Days till start	Sensitivity	Occurrence frequency (Times exceeded/measured)	Select
▼ Host01										
▼ Agent01										
CPU<Dr...	☑	↑ 30 %	1 / 2	☑ 5 hours	☑	20 days	5 days	High ▾	1 / 5	●
Heap	☑	↑ 70 %	1 / 2	☑ 5 hours	☑	20 days	5 days	Low ▾	6 / 60	○

This example sets up a monitoring item for Agent01 that was associated with service Service05 of service group Group03. The following shows the monitoring item settings.

SLO monitor settings

Table 3‒15: Example settings under SLO monitor settings

Monitoring item	Monitoring	Threshold	Occurrence frequency (Times exceeded/measured)	Trend monitoring
CPU	Select	30%	1/2	5

Under **SLO monitor settings**, the SLO definition items are specified as thresholds, and then trend monitoring is set up to promptly detect any error in the performance of the system running the monitored service.

A warning is set to be issued if the probability of exceeding the threshold is 1/2 or higher during the measurement period.

Any potential system performance error must be detected at least five hours in advance because other personnel must be contacted to take corrective action in the event of a system performance error. For this reason, trend monitoring is set to 5 hours.

Error Predict. settings

Table 3‒16: Example settings under Error Predict. settings

Monitoring item	Monitoring	Days in baseline calculation	Days till start	Sensitivity	Occurrence frequency (Times exceeded/measured)
CPU	Select	20 days	5 days	High	1/5

Under **Error Predict. settings**, 20 days' worth of service performance is to be used to calculate the baseline for performing monitoring based on typical system performance. **Days till start** is set to 5 because it was requested that monitoring be started five days later.

A warning is set to be issued if the probability of exceeding the threshold is 1/5 or higher during the measurement period.

Out-of-range value detection is to be performed for all monitoring items. The sensitivity is set to high so that any service performance the veers from the baseline will be detected quickly.

Results of the tasks

Once setup has been completed for service Service05 of service group Group03, the person who monitors all services proceeds to set up monitoring items for the remaining monitored services in the same manner.

After setup has been completed for all monitored services, the person who monitors all services decides to perform monitoring. For an example of execution of monitoring, see *4.6.3 Example of execution for predictive error detection in the performance of systems running monitored services and the corrective action support methodology (working with Performance Management)*.

3.3.4 Example of setup for periodic evaluation of the status of monitored services

This subsection explains an example of periodic evaluation of the status of monitored services, as discussed in *1.1.3 Supporting creation of reports required for periodic reporting*.

With respect to using ITSLM for periodic evaluation of the status of monitored services, this subsection explains by way of example how to perform evaluation and setup based on given conditions.

(1) Prerequisites

The following are the conditions for this setup example:

- There is no agreement regarding service quality (service level) between the service's outsourcing company (service provider) and the outsourced contractor (data center). The data center is required to provide only its minimum level of monitoring.
- The outsourcing company's agent agrees to consider suggestions for system enhancements derived from the monthly service levels. The person who monitors all services at the data center is to report periodically to the outsourcing company's agent.
- The outsourced services are registered as monitored services as follows:
    - Service group: Group01

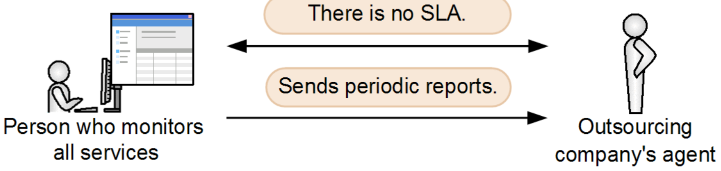
      Services belonging to service group Group01: Service01 to Service03
    - Service group: Group02

      Services belonging to service group Group02: Service04 and Service05
    - Service group: Group03

      Service belonging to service group Group03: Service06
    - Service group: Group04

      Service belonging to service group Group04: Service07
- The following figure shows the relationship among the personnel involved in this task.

Figure 3–44: Relationship among personnel involved in periodic evaluation of the status of monitored services (setup example)



- Person who monitors all services

Evaluates a threshold for each monitoring item because there is no SLA, and then sets up the monitoring items in the Settings window. This person also needs to report the monitoring results periodically to the outsourcing company's agent.

- Outsourcing company's agent

  This person is in charge of providing the outsourced services. This person receives periodic reports from the person who monitors all services at the outsourced contractor. If periodic reports suggest system enhancements, this person evaluates the suggestions and authorizes them, as appropriate.

  This person does not require that the person who monitors all services be responsible for management of the service level.

(2) Defining thresholds

Tasks required for setting up monitoring items in ITSLM

Based on the information provided by the outsourcing company's agent, such as the number of service users and the service description, the person who monitors all services defines thresholds as follows:

- Average response time: 3,000 milliseconds
- Throughput: 800 count/second
- Error rate: 1.0%

Results of the tasks

Once thresholds have been defined, the person who monitors all services proceeds to set up monitoring items for each monitored service.

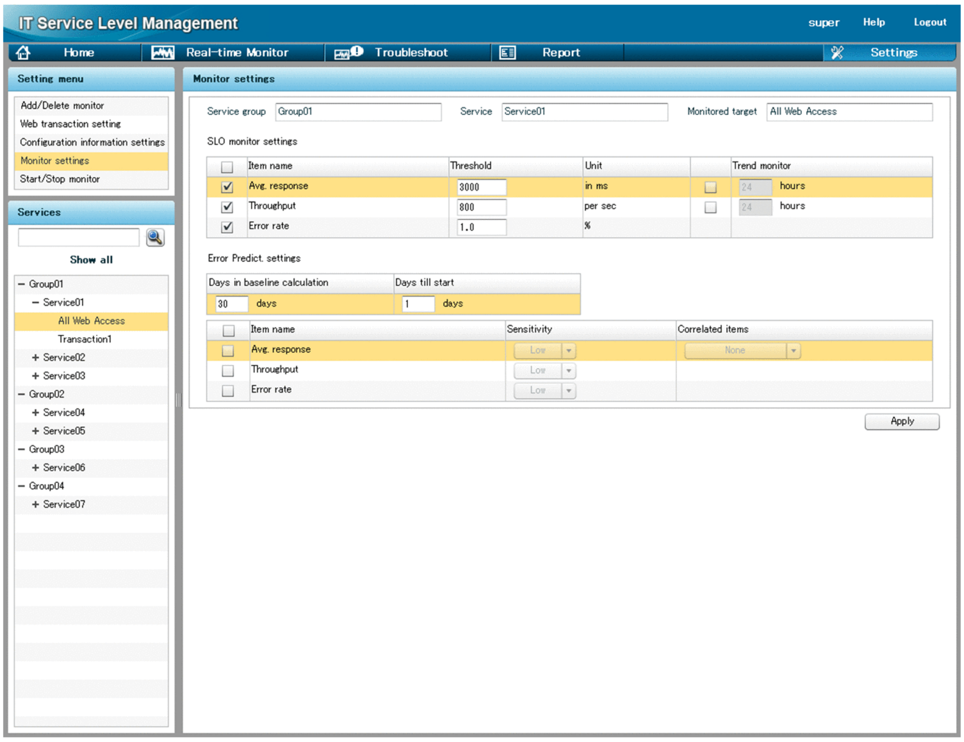
(3) Setting up monitoring items

Tasks in ITSLM

The person who monitors all services decides to log in to ITSLM - Manager to display the Settings window and set up monitoring items for the monitored services based on the defined thresholds.

The following shows a setup example of monitoring items for the monitored services based on the thresholds.

Figure 3–45: Setup example of monitoring items for the monitored services based on thresholds



Service group: Group01 Service: Service01 Monitored target: All Web Access

SLO monitor settings

□	Item name	Threshold	Unit	□	Trend monitor
☑	Avg. response	3000	in ms	□	24 hours
☑	Throughput	800	per sec	□	24 hours
☑	Error rate	1.0	%		

Error Predict. settings

Days in baseline calculation	Days till start
30 days	1 days

□	Item name	Sensitivity	Correlated items
□	Avg. response	Low	None
□	Throughput	Low	
□	Error rate	Low	

This example sets up monitoring items for `All Web Access` of service `Service01` of service group `Group01`. The following shows the monitoring item settings.

SLO monitor settings

Table 3–17: Example settings under SLO monitor settings

Check box	Item name	Threshold	Check box	Trend monitoring
Selected	**Avg. response**	`3000`	Not selected	--
Selected	**Throughput**	`800`	Not selected	--
Selected	**Error rate**	`1.0`	--	--

Legend:

--: Cannot be set

Under **SLO monitor settings**, the settings defined as thresholds are specified.

Because there is no agreement for service level management, neither trend monitoring nor out-of-range value detection is set up. However, **Days in baseline calculation** and **Days till start** are set to the defaults because these items must be specified.

Results of the tasks

Once setup of service `Service01` of service group `Group01` has been completed, the person who monitors all services decides to set up monitoring items for the remaining monitored services in the same manner.

After setup is completed for all monitored services, monitoring is executed. For an example of execution of monitoring, see *4.6.4 Example of execution for periodic evaluation of the status of monitored services*.

4 Performing Monitoring

This chapter provides an overview of using ITSLM for monitoring and explains execution of monitoring. Execution of monitoring includes starting and stopping monitoring, monitoring the status of monitored services, the investigative support methodology for determining the cause when errors or warnings in the monitored services are displayed, and creation of reports used for periodic reporting.

4.1 Overview of monitoring tasks using ITSLM

ITSLM supports stable operation of monitored services by enabling the monitoring persons to monitor the status of the services.

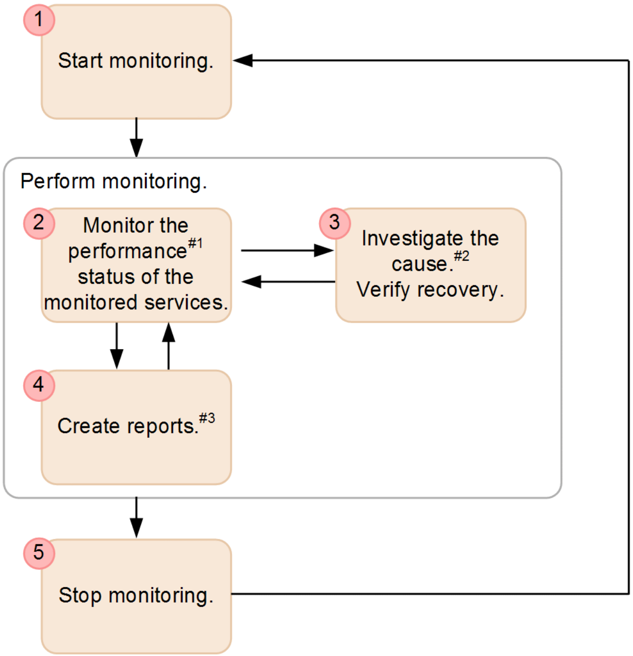
In a system with predefined SLOs, which are the evaluation metrics for the statuses of the monitored services, monitoring is performed so as to comply with the SLOs and to maintain the service level. ITSLM reports warnings based on the monitoring results before overages of thresholds occur. By taking an appropriate corrective action at the warning stage, you can comply with the SLOs and prevent errors from occurring in the performance of monitored services. You can also record and report compliance with SLOs by creating monthly reports of the monitoring results.

This section explains the procedure from start to stop of monitoring when ITSLM is used and the windows in ITSLM that are used for monitoring.

4.1.1 General monitoring procedure

The figure below shows the general procedure for using ITSLM to monitor the status of monitored services. This procedure assumes that the monitored services have been registered into ITSLM and that all the setup required for monitoring has been completed according to the procedures described in Chapter 3.

Figure 4–1: General procedure for monitoring the status of monitored services


1
Start monitoring.
Perform monitoring.
2
Monitor the performance#1 status of the monitored services.
3
Investigate the cause.#2 Verify recovery.
4
Create reports.#3
5
Stop monitoring.

#1: By linking ITSLM with Performance Management, you can also monitor the performance of the systems that are providing monitored services.

#2: You can check the timing of an event in question and investigate changes in the past data. You can use the obtained results to determine the cause.

#3: You can display the performance data needed for report creation in a window and output it to a file.

1. Start monitoring.

   For details about how to start monitoring, see *4.2.1 Starting monitoring*.

2. Monitor the performance status of the monitored services.

You can check the status of monitored services in a window. You can verify that the SLOs are being achieved, and also check for any unusual service performance values.

If you link ITSLM with Performance Management, you can also check the status of the systems that are providing the monitored services, such as hosts and middleware.

The login user can obtain the detailed status of a monitored service of interest based on the overall status of the service's service group that the user is in charge of monitoring or just check the detailed status of the specific monitored service (such as a newly added service or a service that has had problems in the past).

For details about how to monitor the status of monitored services, see *4.3 Monitoring the status of monitored services*.

3. Investigate the cause and verify recovery.

   If a problem is detected while a monitored service is being monitored or investigation is needed to respond to an inquiry from a user of a monitored service, you can check the timing of the problem and past data. Based on the obtained results, you can determine the cause of the problem and take an appropriate corrective action. After the problem has been resolved, verify that the monitored service's status has returned to normal.

   For details about how to check the information that supports root cause investigation, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.

4. Create reports.

   When you need to create reports based on monitoring results, you can display performance data in the monitoring result window and output it to a file. This enables you to keep a record of compliance with the SLOs and optimize the report creation tasks.

   For details about how to check and output the data needed for report creation, see *4.5 Creating reports*.

5. Stop monitoring.

   If you need to change monitoring item settings or ITSLM log output operations, you must first stop monitoring.

   For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

   To resume monitoring the monitored services, go back to step 1.

4.2 Starting and stopping monitoring

To start monitoring, start the registered monitored services. To stop monitoring, stop the monitored services that are being monitored.

4.2.1 Starting monitoring

To start monitoring the target services, the service group administrator must log in to ITSLM and then specify the settings needed to start monitoring. When monitoring of the target services starts, monitoring also starts of the Web transactions set up for the corresponding monitored services.

(1) Before you start

- Verify that you have the service group administrator permissions.
- Log in to ITSLM - Manager.

  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring items have been set up.

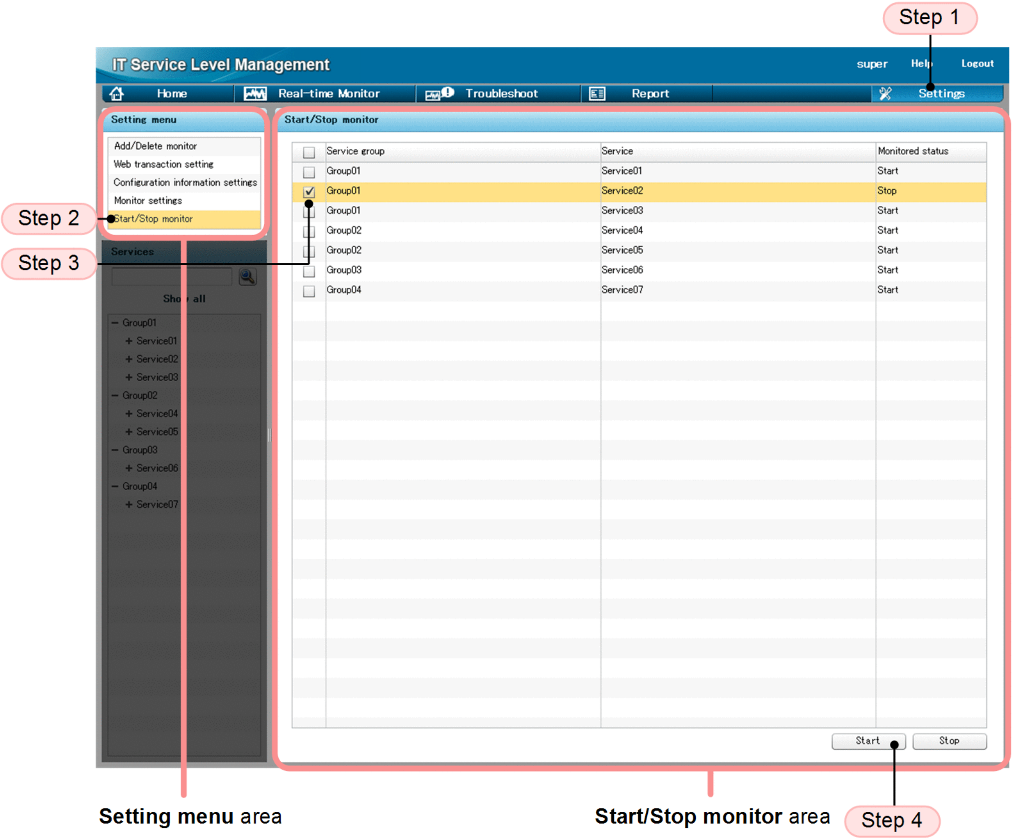
  For details about how to set up monitoring items, see *3.2.7 Setting up the monitoring items for service performance*.
- If you link ITSLM with Performance Management, verify that PFM - Manager is running.

  For details about how to start PFM - Manager, see the description of the PFM - Manager setup procedure in *Job Management Partner 1/Performance Management User's Guide*.
- If you link ITSLM with Performance Management, verify that the monitoring agents are running.

  For details about how to start monitoring agents, see the *Job Management Partner 1/Performance Management User's Guide*.

(2) Procedure

The following shows the Settings window that is used in this task:



□	Service group	Service	Monitored status
□	Group01	Service01	Start
☑	Group01	Service02	Stop
□	Group01	Service03	Start
□	Group02	Service04	Start
□	Group02	Service05	Start
□	Group03	Service06	Start
□	Group04	Service07	Start

To start monitoring:

1. Click the **Settings** button.
2. In the **Setting menu** area, select **Start/Stop monitor**.
   All monitored services whose monitoring is the login user's responsibility are listed in the **Start/Stop monitor** area.
3. In the displayed list of monitored services, select the check box for the monitored service whose monitoring is to be started.
4. Click the **Start** button.
   Monitoring of the selected monitored service begins.

If the start processing is successful, **Monitored Status** changes to **Start**.

Monitoring process if an error occurs when monitoring begins while working with Performance Management

When you start monitoring by clicking the **Start** button, the ⚠ (warning) icon might be displayed in the **Monitored Status** column in the **Start/Stop monitor** area and a message might be displayed. In such a case, an error might have occurred in either ITSLM - UR or PFM - Manager. If monitoring started successfully in ITSLM - UR or PFM - Manager, **Start** is displayed in the **Monitored Status** column. The following table describes the monitoring status and process in the event of an error:

Table 4–1: Monitoring status and process in the event of an error when monitoring starts

No.	Monitoring status	Monitoring process
1	**Start**	Monitoring has started on ITSLM - UR and PFM - Manager.
2	**Start** ⚠	One of the following statuses: • An error has occurred in ITSLM - UR.

No.	Monitoring status	Monitoring process
2	**Start** ⚠	ITSLM failed to start monitoring of All Web Access and the Web transactions that are the targets of ITSLM - UR processing. ITSLM has successfully started monitoring of the availability monitor and the system performance that is the target of PFM - Manager processing. • An error has occurred in PFM - Manager. ITSLM has failed to start monitoring of the availability monitor and the system performance that is the target of PFM - Manager processing. ITSLM successfully started monitoring of All Web Access and the Web transaction that are the targets of ITSLM - UR processing.
3	**Stop**	Monitoring stopped on ITSLM - UR and PFM - Manager.

To determine the monitoring status of each monitoring agent for a monitored service for which the ⚠ (warning) icon is displayed, check the Real-time Monitor window or message logs.

(3) Supplementary information

- When ITSLM - Manager services are started, the following processing is performed based on the `managerStartMode` property value in ITSLM - Manager's system definition file (`jp1itslm.properties`):
  - When `normal` is specified for the `managerStartMode` property

    Stop processing is performed on all monitored services.
  - When `restart` is specified for the `managerStartMode` property

    Start processing is performed on a monitored service whose status is **Start** or **Start** ⚠ .

    Stop processing is performed on a monitored service whose status is **Stop**.

(4) Related topics

- *4.2.2 Stopping monitoring*
- *10.6.1 Configuration of the Settings window*
- *10.6.2 Services area*
- *10.6.3 Setting menu area*
- *10.6.20 Start/Stop monitor area*

4.2.2 Stopping monitoring

To change the settings of the monitoring items for a monitored service after you have already started monitoring the service, you must first stop monitoring the service. To change ITSLM operations or add or delete monitored services, you must stop monitoring of all the monitored services. When monitoring of a monitored service is stopped, monitoring of the Web transactions set for that monitored service is also stopped.

(1) Before you start

- Log in to ITSLM - Manager.

  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- If you link ITSLM with Performance Management, verify that PFM - Manager is running.

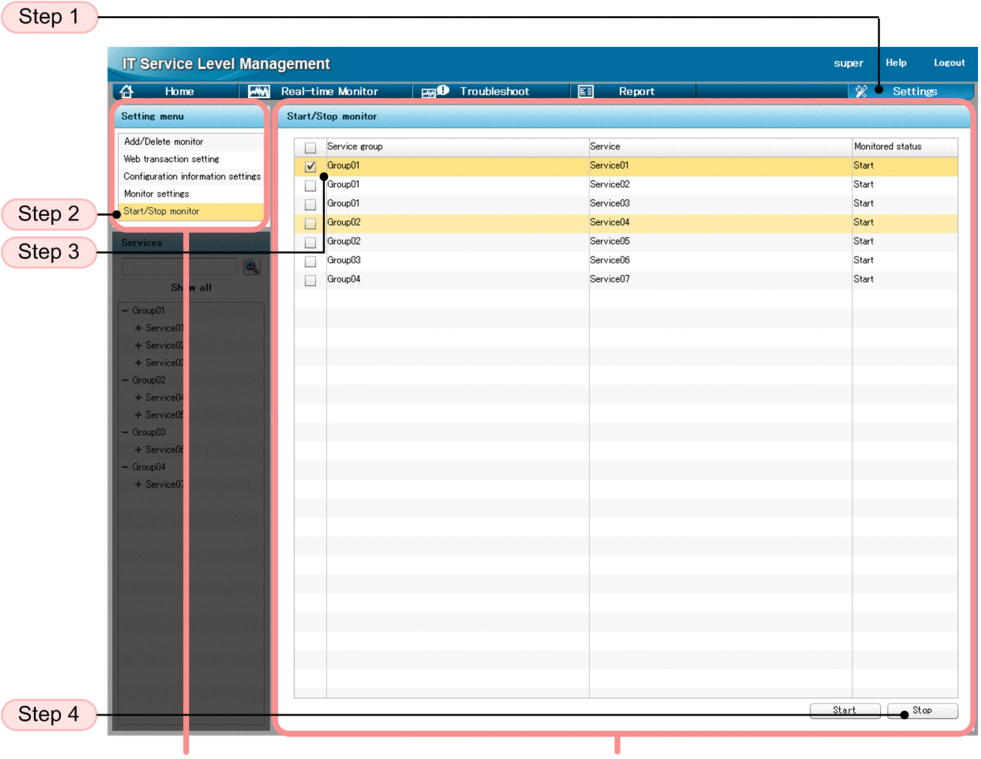
For details about how to start PFM - Manager, see the description of the PFM - Manager setup procedure in *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

- If you link ITSLM with Performance Management, verify that the monitoring agents are running.

  For details about how to start monitoring agents, see the *Job Management Partner 1/Performance Management User's Guide*.

(2) Procedure

The following shows the Settings window that is used in this task:



☐	Service group	Service	Monitored status
☑	Group01	Service01	Start
☐	Group01	Service02	Start
☐	Group01	Service03	Start
☐	Group02	Service04	Start
☐	Group02	Service05	Start
☐	Group03	Service06	Start
☐	Group04	Service07	Start

Setting menu area   **Start/Stop monitor** area

To stop monitoring:

1. Click the **Settings** button.

2. In the **Setting menu** area, select **Start/Stop monitor**.

   All monitored services whose monitoring is the login user's responsibility are listed in the **Start/Stop monitor** area.

3. In the displayed list of monitored services, select the check box for the monitored service whose monitoring is to be stopped.

4. Click the **Stop** button.

   Monitoring of the selected monitored service stops.

If stop processing is successful, **Monitored Status** changes to **Stop**.

Monitoring process if an error occurs when monitoring stops while working with Performance Management

When you stop monitoring by clicking the **Stop** button, the ⚠ (warning) icon might be displayed in the **Monitored Status** column in the **Start/Stop monitor** area and a message might be displayed. In such a case, an error might have occurred in either ITSLM - UR or PFM - Manager. Even if monitoring stopped successfully in ITSLM - UR or PFM - Manager, **Start** is displayed in the **Monitored Status** column. The following table describes the monitoring status and process in the event of an error.

Table 4–2: Monitoring status and process in the event of an error when monitoring stops

No.	Monitoring status	Monitoring process
1	**Stop**	Monitoring has stopped on ITSLM - UR and PFM - Manager.
2	**Start** ⚠	One of the following statuses: • An error has occurred in ITSLM - UR. ITSLM failed to stop monitoring of All Web Access and the Web transactions that are the targets of ITSLM - UR processing. ITSLM has successfully stopped monitoring of the availability monitor and the system performance that is the target of PFM - Manager processing. • An error has occurred in PFM - Manager. ITSLM failed to stop monitoring of the availability monitor and the system performance that is the target of PFM - Manager processing. ITSLM successfully stopped monitoring of All Web Access and the Web transactions that are the targets of ITSLM - UR processing.
3	**Start**	Monitoring has started on ITSLM - UR and PFM - Manager.

To determine the monitoring status of each monitoring agent for a monitored service for which the ⚠ (warning) icon is displayed, check the Real-time Monitor window or message logs.

Forcibly stopping monitoring

If a problem such as an error in a monitoring agent occurs and ITSLM cannot handle the problem, you can forcibly stop monitoring of the monitored services. The methods for forcibly stopping monitoring are as follows:

- Select one monitored service and stop monitoring of that service.
- Click the **OK** button in the forced stop dialog box that is displayed when stopping of monitoring fails.

Forced stop enables you to set the monitoring status to stop even for a service whose stop processing has already failed.

To stop monitoring normally, eliminate the cause of the stop error that occurred in the monitored service on which forced stop was executed. Then start and stop monitoring again to synchronize the monitoring status of the monitoring items between ITSLM and Performance Management.

(3) Related topics

- *3.2.7 Setting up the monitoring items for service performance*
- *4.2.1 Starting monitoring*
- *5.6.1 Editing the system definition files*
- *10.6.1 Configuration of the Settings window*
- *10.6.2 Services area*
- *10.6.3 Setting menu area*
- *10.6.20 Start/Stop monitor area*

4.2.3 Notes about starting and stopping monitoring

If monitoring agents are terminated individually while target services are being monitored, transmission of system performance data from the monitoring agents to ITSLM stops. If this happens, the system performance data existing immediately before monitoring was stopped remains displayed in ITSLM but no new system performance data is displayed. You must restart the monitoring agents to display the system performance data in ITSLM.

If monitoring is stopped forcibly, inconsistency occurs in the monitoring status between ITSLM and Performance Management and data obtained after monitoring stopped might be sent from Performance Management.

In such a case, a message indicating that the transmitted data is to be discarded is output repeatedly in ITSLM. Therefore, if you stopped monitoring forcibly, you must cancel the ITSLM monitoring setting in Performance Management.

4.3 Monitoring the status of monitored services

ITSLM enables you to check the results of monitoring the status of monitored services for all service groups together. You can also select monitored services in a specific service group and check the details about them.

Monitoring of the status of monitored services enables you to detect in advance on the basis of the ! (warning) icon displayed in the window the potential for failures to satisfy SLOs as well as the potential for occurrence of service performance errors. When a failure to meet an SLO has actually occurred, the ✖ (error) icon is displayed in the window to let you know that immediate corrective action is needed.

4.3.1 Checking the status of the monitored services of all service groups

You can obtain the status of the monitored services of all service groups, identify the monitored services that require special attention, and check on errors and warnings in the monitored services.

Use the Home window to perform this checking. You can check the following in the Home window:

- Status of the monitored services in each service group
  You can check a bar graph indicating the percentage of the monitored services that are in error, warning, normal, and monitoring stopped status (among the total number of monitored services that belong to a service).
- Monitored services that require special attention in monitoring
  You can check the monitored services that require special attention in monitoring based on the status of the monitored services over the past seven days, such as monitored services that produce frequent warnings.
- Events that occurred in all monitored services
  You can check a list of events, such as errors and warnings, that occurred in all monitored services over the past seven days.

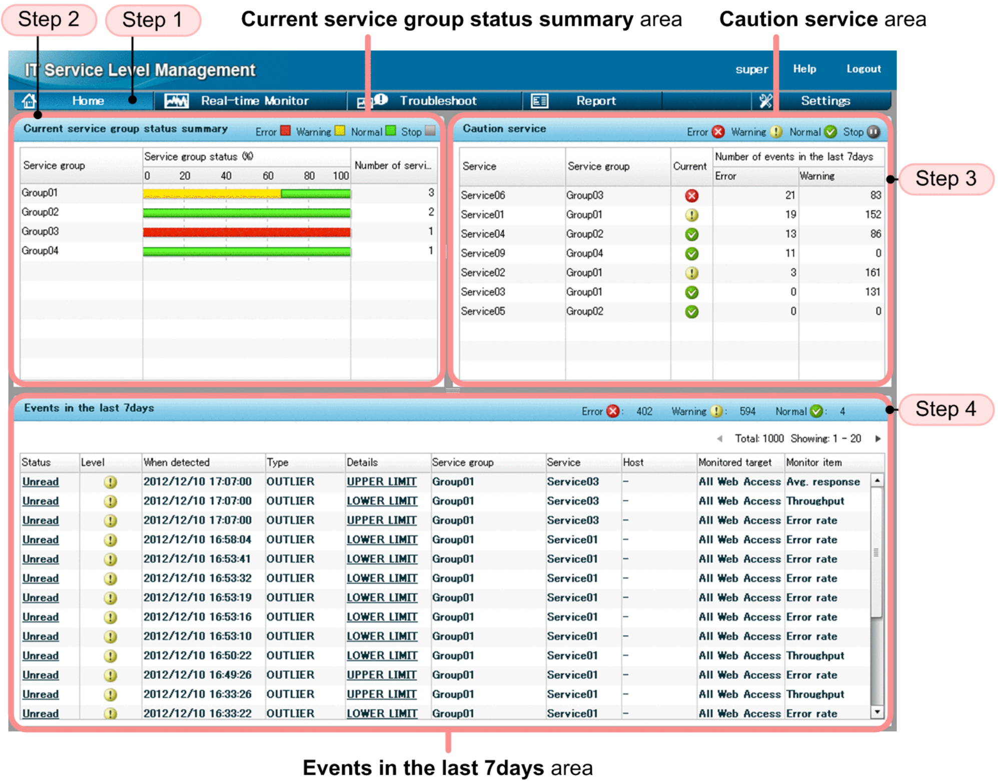
The information displayed in the Home window is refreshed every three seconds.

(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.

(2) Procedure

The following shows the Home window that is used in this task:



Current service group status summary   Error 🟥 Warning 🟨 Normal 🟩 Stop ▨

Service group	Service group status (%) 0 20 40 60 80 100	Number of servi...
Group01		3
Group02		2
Group03		1
Group04		1

Caution service   Error ✗ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service06	Group03	✗	21	83
Service01	Group01	!	19	152
Service04	Group02	✓	13	86
Service09	Group04	✓	11	0
Service02	Group01	!	3	161
Service03	Group01	✓	0	131
Service05	Group02	✓	0	0

Events in the last 7days   Error ✗: 402   Warning !: 594   Normal ✓: 4

◀ Total: 1000 Showing: 1 - 20 ▶

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	!	2012/12/10 17:07:00	OUTLIER	UPPER LIMIT	Group01	Service03	–	All Web Access	Avg. response
Unread	!	2012/12/10 17:07:00	OUTLIER	LOWER LIMIT	Group01	Service03	–	All Web Access	Throughput
Unread	!	2012/12/10 17:07:00	OUTLIER	UPPER LIMIT	Group01	Service03	–	All Web Access	Error rate
Unread	!	2012/12/10 16:58:04	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:53:41	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:53:32	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:53:19	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:53:16	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:53:10	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:50:22	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2012/12/10 16:49:26	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Error rate
Unread	!	2012/12/10 16:33:26	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2012/12/10 16:33:22	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Error rate

To check the status of all service groups' monitored services:

1. If the Home window is not displayed, click the **Home** button.

   The **Current service group status summary**, **Caution service**, and **Events in the last 7 days** areas are displayed. You can determine from the information provided in each area the status of all monitored services being monitored or the status of specific monitored services.

   Note that the steps beginning in 2 below are examples of checking procedures.

2. Check the **Current service group status summary** area and determine the status of all monitored services in the entire service group subject to monitoring.

3. Check the **Caution service** area to identify the monitored services that require special attention.

4. Check the **Events in the last 7 days** area to obtain the error and warning statuses of the monitored services identified in step 3.

   For each event that you have checked, click the **Status** column to change its status from **Unread** to **Read**.

Once all monitored services show normal status, the check is complete.

If errors and warnings are displayed in these areas or some alarm status is displayed, investigate the cause. If you click the **Details** column in the **Events in the last 7 days** area, the Troubleshoot window is displayed. You can determine in the Troubleshoot window the time the event causing the status of concern occurred. For details about how to check the timing of events causing errors and warnings, see *4.4.1 Checking the timing of an event causing an error or warning*.

(3) Related topics

- *4.3.2 Checking the status of the monitored services in a specific service group*
- *4.4.1 Checking the timing of an event causing an error or warning*
- *10.2.1 Configuration of the Home window*

- *10.2.2 Current service group status summary area*
- *10.2.3 Caution service area*
- *10.2.4 Events in the last 7 days area*

4.3.2 Checking the status of the monitored services in a specific service group

If you know the monitored services that require special attention, such as new services whose monitoring has just started and existing monitored services that have had problems in the past, use the Real-time Monitor window to determine their status. You can check the following in the Real-time Monitor window:

- Status of specific service groups or monitored services
  You can check the status of specific service groups or monitored services.
- Events that occurred in specific service groups or monitored services
  You can check a list of events, including errors and warnings, that have occurred in specific service groups or monitored services.
- Performance charts for monitored targets of specific monitored services
  You can view line graphs of the current performance of specific monitored services.

The information displayed in the Real-time Monitor window is refreshed every three seconds.

(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.

(2) Procedure

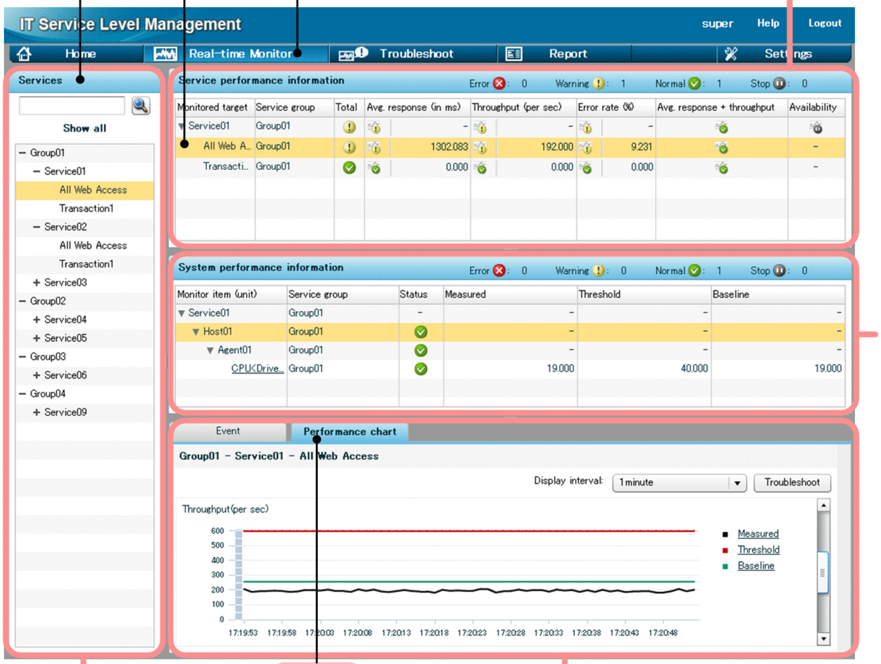
The following shows the Real-time Monitor window that is used in this task:

Step 2

Step 3

Step 1

Service performance information area



- Group01
  - Service01
    - All Web Access
    - Transaction1
  - Service02
    - All Web Access
    - Transaction1
  - + Service03
- Group02
  - + Service04
  - + Service05
- Group03
  - + Service06
- Group04
  - + Service09

Service performance information Error ✕: 0 Warning !: 1 Normal ✓: 1 Stop ⏸: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service01	Group01	!	! -	! -	! -	✓	⏸
All Web A...	Group01	!	! 1302.083	! 192.000	! 9.231	✓	-
Transacti...	Group01	✓	✓ 0.000	✓ 0.000	✓ 0.000	✓	-

System performance information Error ✕: 0 Warning !: 0 Normal ✓: 1 Stop ⏸: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service01	Group01	-	-	-	-
▼ Host01	Group01	✓	-	-	-
▼ Agent01	Group01	✓	-	-	-
CPU(Drive...	Group01	✓	19.000	40.000	19.000

Group01 - Service01 - All Web Access

System performance information area#

Services area

Step 4

Event and **Performance chart** tabs area

#: The **System performance information** area is displayed when ITSLM is linked with Performance Management.

To check the status of monitored services in a specific service group:

1. Click the **Real-time Monitor** button.

   The **Services**, **Service performance information**, and **System performance information**# areas and the **Event** and **Performance chart** tabs area are displayed. In the **Event** and **Performance chart** tabs area, the **Event** tab is selected.

2. In the **Services** area, select a service group, a monitored service, or a monitored target of a monitored service.

   Performance information for the selected service group, monitored service, or monitored target of a monitored service is displayed in the **Service performance information** and **System performance information**# areas and the **Event** and **Performance chart** tabs area. Check the displayed information.

   If you selected a monitored target of a monitored service, go to step 4.

3. In the **Service performance information** area, select a monitored service or a monitored target of a monitored service.

4. In the **Event** and **Performance chart** tabs area, click the **Performance chart** tab to view a graph of the current status of the monitored target of the monitored service.

   A performance chart is displayed indicating the current status of the selected monitored target of the monitored service.

If the display is all normal in the **Service performance information** and **System performance information**# areas, the check is complete.

If errors, warnings, or alarm statuses are displayed in the **Service performance information** or **System performance information**# area or the **Event** and **Performance chart** tabs area, investigate the cause. In the **Event** and **Performance chart** tabs area, selecting the **Performance chart** tab and then clicking the **Troubleshoot** button in the **Event** and **Performance chart** tabs area displays the Troubleshoot window. In the Troubleshoot window, you can check the timing of the event causing the error, warning, or alarm status that is of interest. For details about how to check the timing of events causing errors and warnings, see *4.4.1 Checking the timing of an event causing an error or warning*.

#

The **System performance information** area is displayed when ITSLM is linked with Performance Management. Selecting a monitoring item displayed in the **System performance information** area does not display performance information in the **Event** and **Performance chart** tabs area.

(3) Related topics

- *4.3.1 Checking the status of the monitored services of all service groups*
- *4.4.1 Checking the timing of an event causing an error or warning*
- *10.3.1 Configuration of the Real-time Monitor window*
- *10.1.2(3) Services area*
- *10.3.3 Service performance information area*
- *10.3.4 System performance information area*
- *10.3.5 Event and Performance chart tabs area (Event tab selected)*
- *10.3.6 Event and Performance chart tabs area (Performance chart tab selected)*

4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service

When an event, such as an overage of a threshold or a trend leading to an overage of a threshold, is detected in a monitored service, you can use ITSLM to investigate the cause.

This section discusses what you can do when you use ITSLM for root cause investigation and explains the procedures.

ITSLM enables you to do the following to determine the cause of an error or warning:

- Check the timing of the event that caused the error or warning
- Check past service performance

After you have handled the error or warning, you can check whether the monitored service's status has returned to normal.

If you link ITSLM with Performance Management, you can check not only the performance of the monitored services, but you can also check the systems that are providing the monitored services, such as hosts and middleware, for the causes of errors and warnings.

4.4.1 Checking the timing of an event causing an error or warning

When an error or warning is displayed for a monitored service, you can check a performance chart for the monitored service's monitored target to determine the timing of the event that caused the error or warning.

Use the Home window, Real-time Monitor window, and Troubleshoot window for this checking.

If you want to check the overall status of the service group, you identify the target monitored service, and then use the Home window to investigate the cause of the event. If you are focusing in on a specific monitored service and want to investigate the cause of an event that occurred in that monitored service, use the Real-time Monitor window.

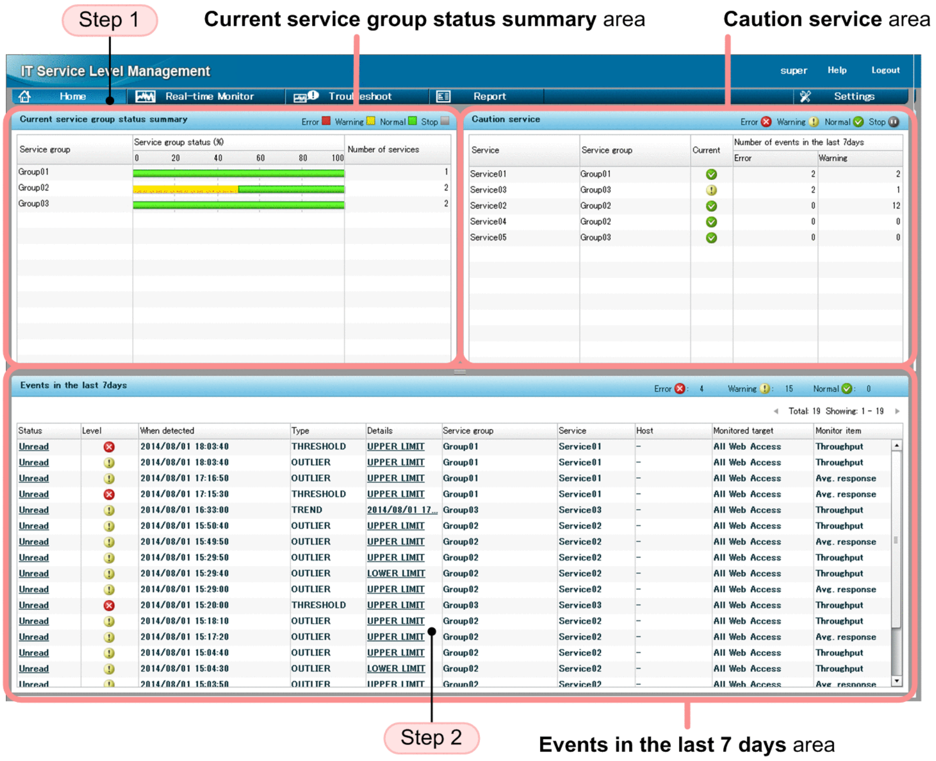
(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.

(2) Procedure

The following shows the Home window and the Troubleshoot window:

- Home window



Step 1

Current service group status summary area

Caution service area

Current service group status summary   Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%)	Number of services
Group01	🟩	1
Group02	🟨🟩	2
Group03	🟩	2

Caution service   Error ✕ Warning ! Normal ✓ Stop ‖

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
Service05	Group03	✓	0	0

Events in the last 7days   Error ✕: 4   Warning !: 15   Normal ✓: 0

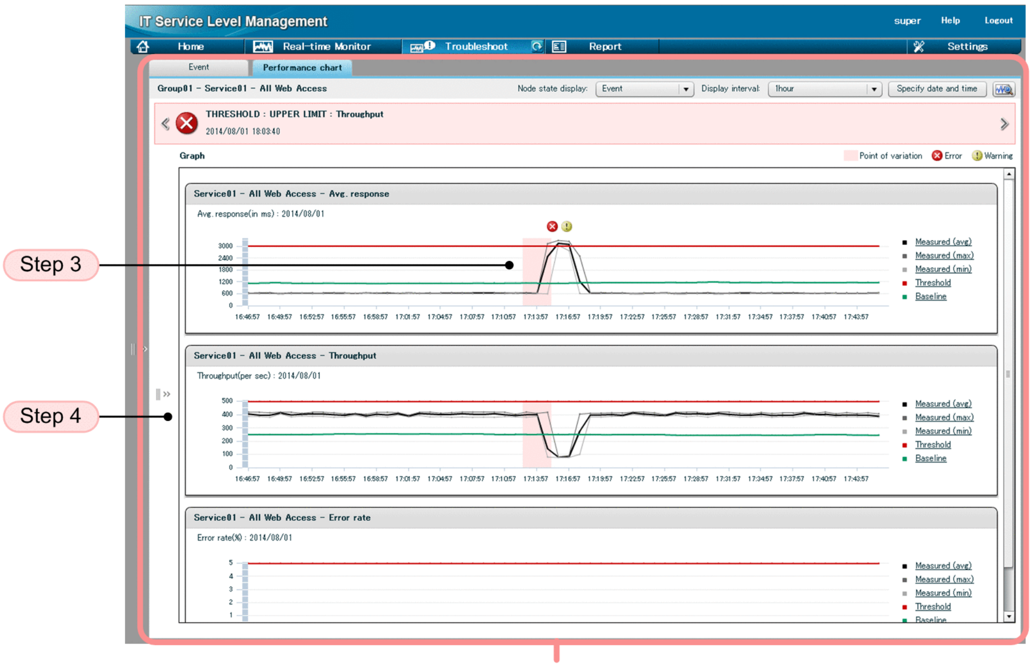
◀ Total: 19 Showing: 1 - 19 ▶

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	✕	2014/08/01 18:03:40	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 18:03:40	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 17:16:50	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	✕	2014/08/01 17:15:30	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2014/08/01 16:33:00	TREND	2014/08/01 17...	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	✕	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response

Step 2

Events in the last 7 days area

- Troubleshoot window



Group01 - Service01 - All Web Access   Node state display: Event   Display interval: 1hour

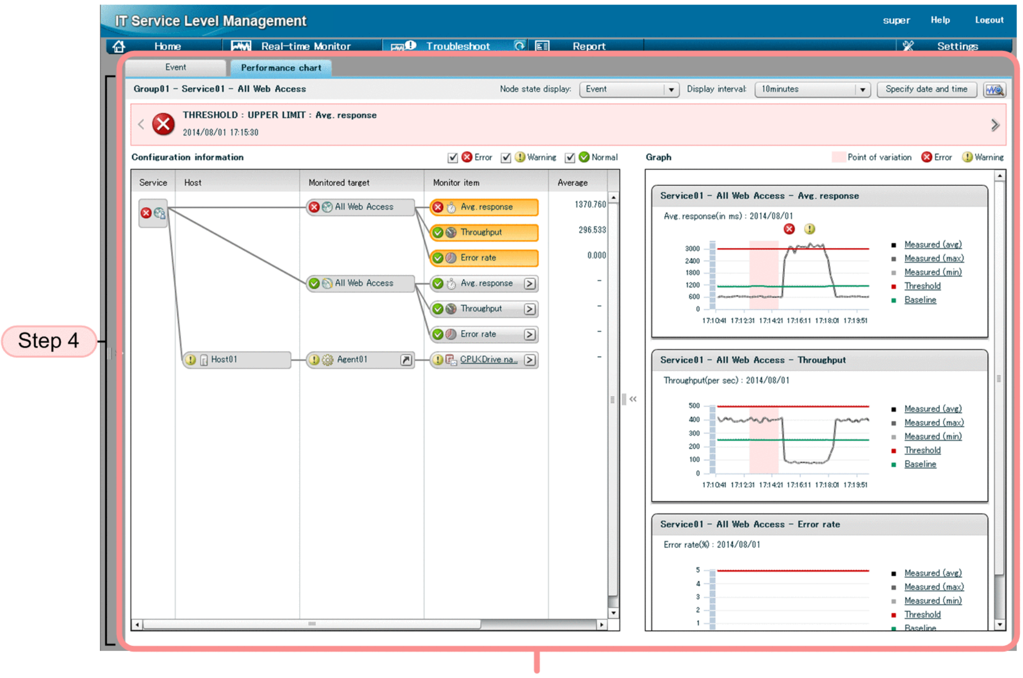
THRESHOLD : UPPER LIMIT : Throughput
2014/08/01 18:03:40

Step 3

Step 4

Event and **Performance chart** tabs area

- Troubleshoot window (displaying configuration information)



Group01 - Service01 - All Web Access

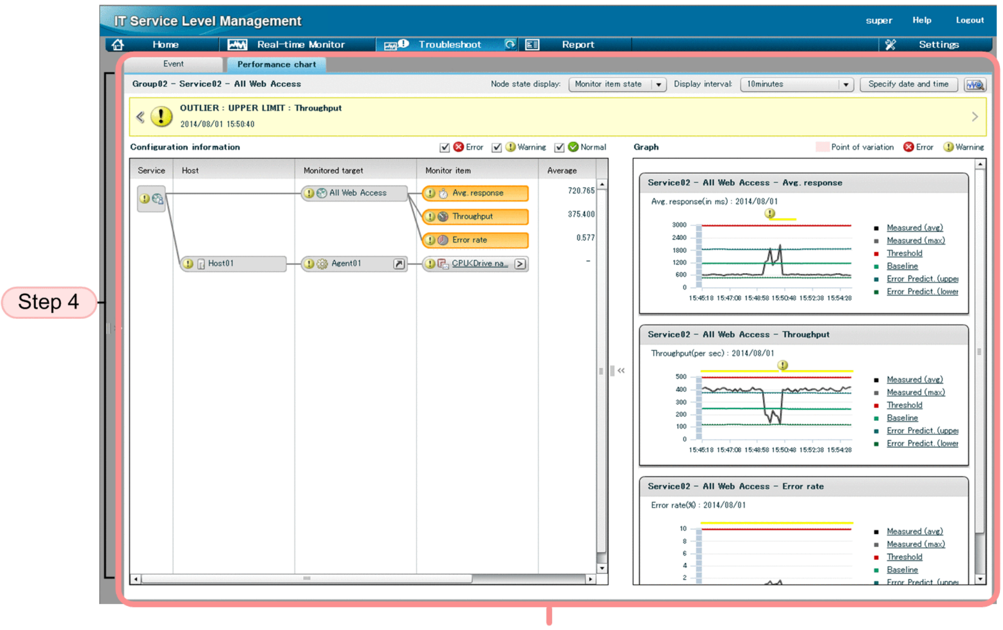
Node state display: Event

Display interval: 10minutes

Specify date and time

Event and **Performance chart** tabs area

- Troubleshoot window (displaying **Monitor item state** on the **Performance chart** tab)



Group02 - Service02 - All Web Access

Node state display: Monitor item state

Display interval: 10minutes

Specify date and time

Event and **Performance chart** tabs area

To check the timing of an event causing an error or warning:

1. If the Home window is not displayed, click the **Home** button.

   The **Current service group status summary**, **Caution service**, and **Events in the last 7 days** areas are displayed.

   If you need to determine the monitored service to be investigated from the event issuance status, go to step 2.

   If you know which monitored service is to be investigated, go to step 3.

2. In the Home window, from the **Events in the last 7 days** area, select an error or warning that you want to check, then click the **Details** column of the corresponding line.

   For the selected error or warning, the **Performance chart** tab on the Troubleshoot window is displayed. Note that the **Performance chart** tab is displayed only when an event related to service performance is selected.

3. In the Troubleshoot window, in the **Event** and **Performance chart** tabs area, check the performance chart displayed on the **Performance chart** tab to determine the timing of the event that caused the error or warning.

   Check the performance chart and look for the time period in which the average value for service performance started to veer significantly from the baseline. On a performance chart, a colored band indicates a timeframe during which a significant change in service performance occurred. The timeframe indicated by the colored band might be when the event causing the error or warning occurred.

   You can also determine the timing of the event causing the error by selecting a node state display from the **Node state display** pull-down menu. If **Event** is selected from the **Node state display** pull-down menu, an icon indicating the event is displayed above the time the event occurred. This is useful for determining the base for troubleshooting because the status at the time the event occurred is displayed. If **Monitor item state** is selected from the **Node state display** pull-down menu, a band indicating the current events is displayed on the chart. You can check the transition of events by following the displayed band.

   You can change the item displayed in the performance chart. Click a display item to display the Select Items to Display dialog box, and then select the items that you want to display. For details about the display items, see *10.4.4 Event and Performance chart tabs area (Performance chart tab selected)*.

4. Click » to display configuration information.

   Configuration information helps you identify the monitoring item of the monitored service that resulted in the error. If necessary, you can display performance information as a graph by clicking the > button associated with the monitoring item. You can also check whether a problem has occurred in the system, such as with a host or middleware. If a problem has occurred in the system, click the ↗ button to connect to Performance Management for further investigation, if necessary.

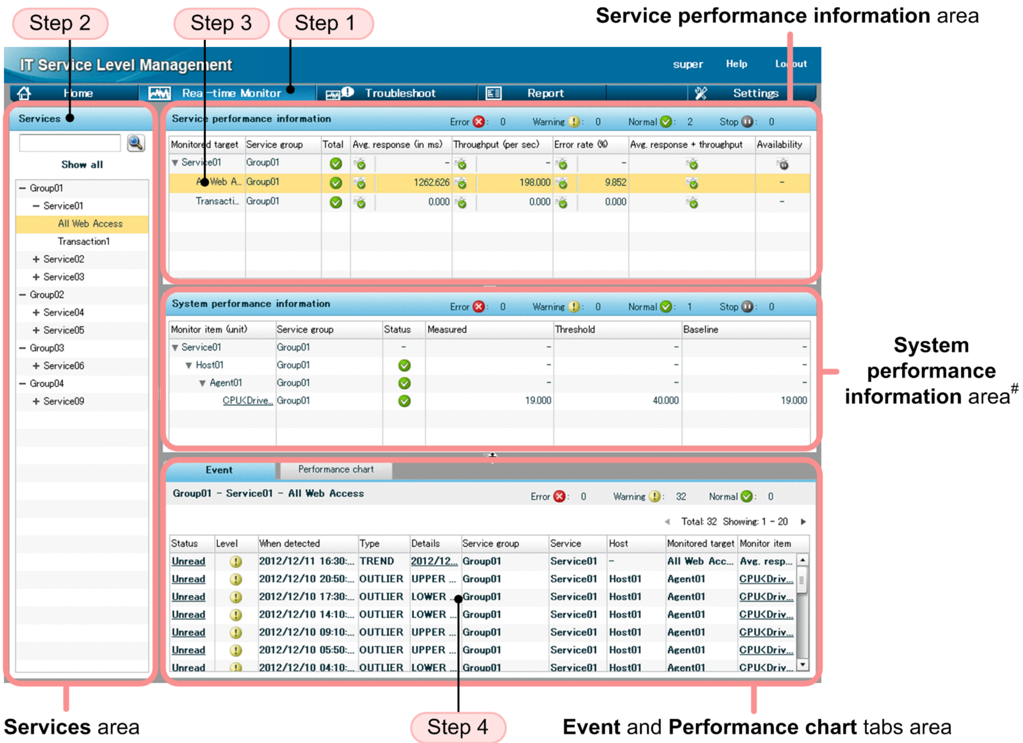
Based on the information for the specific time period, check the CPU usage, memory usage, or disk usage for that period to evaluate the cause of the error or warning.

You can also check in the performance chart past service performance. For details about how to check past service performance, see *4.4.2 Checking past data*.

Reference note

You can also display the Troubleshoot window from the Real-time Monitor window. The following explains how to check the timing of an event causing an error or warning from the Real-time Monitor window and shows the Real-time Monitor window used in the procedure:

- Real-time Monitor window



Service performance information Error: 0 Warning: 0 Normal: 2 Stop: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service01	Group01	✓	-	-	-	✓	●
All Web A...	Group01	✓	1262.626	198.000	9.852	✓	-
Transacti...	Group01	✓	0.000	0.000	0.000	✓	-

System performance information Error: 0 Warning: 0 Normal: 1 Stop: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service01	Group01	-	-	-	-
▼ Host01	Group01	✓	-	-	-
▼ Agent01	Group01	✓	-	-	-
CPU<Drive...	Group01	✓	19.000	40.000	19.000

Group01 - Service01 - All Web Access Error: 0 Warning: 32 Normal: 0

Total: 32 Showing: 1 - 20

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	!	2012/12/11 16:30:...	TREND	2012/12...	Group01	Service01	-	All Web Acc...	Avg. resp...
Unread	!	2012/12/10 20:50:...	OUTLIER	UPPER ...	Group01	Service01	Host01	Agent01	CPU<Driv...
Unread	!	2012/12/10 17:30:...	OUTLIER	LOWER ...	Group01	Service01	Host01	Agent01	CPU<Driv...
Unread	!	2012/12/10 14:10:...	OUTLIER	LOWER ...	Group01	Service01	Host01	Agent01	CPU<Driv...
Unread	!	2012/12/10 09:10:...	OUTLIER	UPPER ...	Group01	Service01	Host01	Agent01	CPU<Driv...
Unread	!	2012/12/10 05:50:...	OUTLIER	UPPER ...	Group01	Service01	Host01	Agent01	CPU<Driv...
Unread	!	2012/12/10 04:10:...	OUTLIER	LOWER ...	Group01	Service01	Host01	Agent01	CPU<Driv...

#: The **System performance information** area is displayed when ITSLM is linked with Performance Management.

1. Click the **Real-time Monitor** button.

   The **Services**, **Service performance information**, and **System performance information** areas and the **Event** and **Performance chart** tabs area are displayed.

2. In the **Services** area of the Real-time Monitor window, select a service group, a monitored service, or a monitored target of a monitored service that you want to investigate.

   If you select a monitored target of a monitored service, go to step 4 (the task in step 3 is not necessary).

3. In the **Service performance information** area of the Real-time Monitor window, select the monitored service's monitored target that you want to investigate.

   If threshold value monitoring, trend monitoring, or out-of-range value detection resulted in the error or warning, select the monitored target of a monitored service that you want to investigate based on the information, including icons, displayed in the **Service performance information** area. If you are monitoring system availability information by linking with Performance Management, the availability information is displayed in the **Availability** column in the **Service performance information** area. Check the displayed icon information and select the monitored service's monitored target that you want to investigate.

   Note that you can select a monitored target of a monitored service on the **Event** tab in step 4 without selecting it here.

4. In the Real-time Monitor window, on the **Event** tab in the **Event** and **Performance chart** tabs area, check information about the event, and then click the **Details** column of the error or warning that you want to check.

   On the **Event** tab, you can check information about events that occurred in threshold value monitoring, trend monitoring, or out-of-range value detection. If you click the **Details** column, messages and a performance chart for the service performance resulting in the error or warning are displayed in the **Event** and **Performance chart** tabs area in the Troubleshoot window.

5. In the Troubleshoot window, in the **Event** and **Performance chart** tabs area, check the performance chart displayed on the **Performance chart** tab to determine the timing of the event that caused the error or warning.

   Check the performance chart and look for a time period in which the average value for service performance started to veer significantly from the baseline. On the performance chart, a colored band indicates a timeframe during which a significant change in service performance occurred. The timeframe indicated by the colored band might be when the event causing the error or warning occurred.

   You can change the item displayed in the performance chart. Click a display item to display the Select Items to Display dialog box, and then select the items that you want to display. For details about the display items, see *10.4.4 Event and Performance chart tabs area (Performance chart tab selected)*.

6. Click » to display configuration information.

   Configuration information helps you identify the monitoring item of the monitored service that resulted in the error. If necessary, you can display performance information as a graph by clicking the > button associated with the monitoring item. You can also check whether a problem has occurred in the system, such as with a host or middleware. If a problem has occurred in the system, click the ↗ button to connect to Performance Management for further investigation, if necessary.

(3) Related topics

- *4.3.1 Checking the status of the monitored services of all service groups*
- *4.3.2 Checking the status of the monitored services in a specific service group*
- *4.4.3 Verifying recovery of monitored services after taking corrective action*
- *10.2.1 Configuration of the Home window*
- *10.2.2 Current service group status summary area*
- *10.2.3 Caution service area*
- *10.2.4 Events in the last 7 days area*
- *10.3.1 Configuration of the Real-time Monitor window*
- *10.1.2(3) Services area*
- *10.3.3 Service performance information area*
- *10.3.4 System performance information area*
- *10.3.5 Event and Performance chart tabs area (Event tab selected)*
- *10.3.6 Event and Performance chart tabs area (Performance chart tab selected)*
- *10.4.1 Configuration of the Troubleshoot window*
- *10.4.3 Event and Performance chart tabs area (Event tab selected)*
- *10.4.4 Event and Performance chart tabs area (Performance chart tab selected)*

4.4.2 Checking past data

You can check performance charts of a monitored service's past performance and use the information for root cause investigation.

If you find a warning sign in a performance chart or were contacted by users of a monitored service, you can check the monitored service's past service performance data as necessary.

If you link with Performance Management, you can also check the past data of the system, such as the host or middleware, that is providing the monitored service.

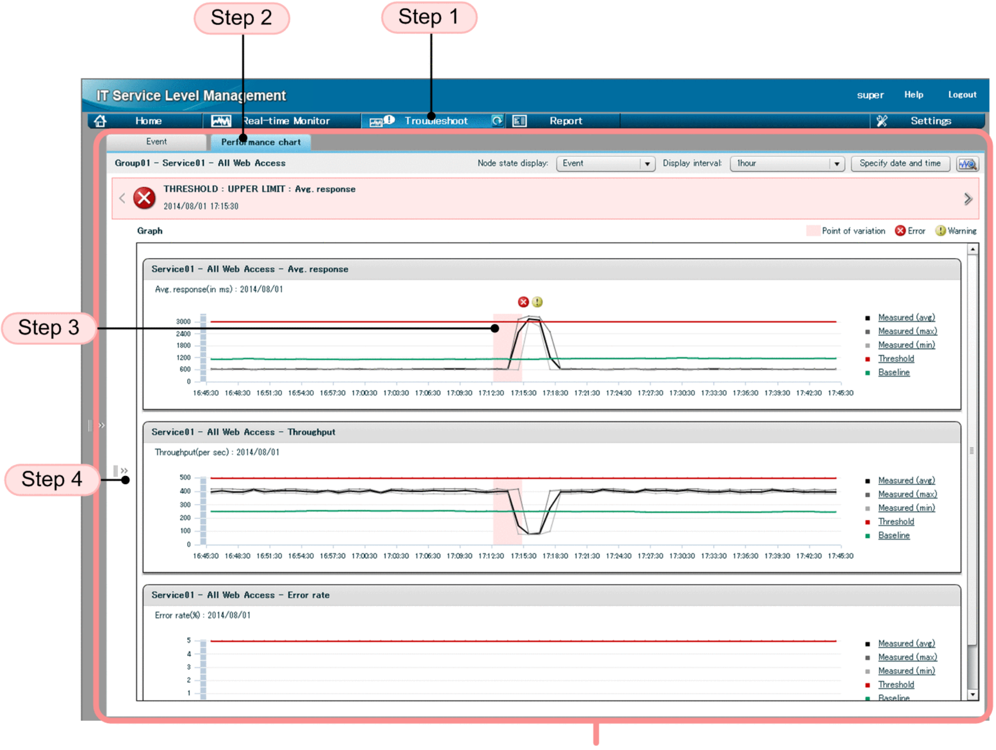
This subsection explains how to check past service performance only using the Troubleshoot window.

(1) Before you start

- Before you start ITSLM - Manager, specify the URL of PFM - Web Console in ITSLM's system definition file. For details about the settings in the system definition file, see *5.4 Setting up a linkage between ITSLM and Performance Management*.
- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.
- If you link ITSLM with Performance Management, verify that PFM - Manager is running. For details about how to start PFM - Manager, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
- If you link with Performance Management, verify that the prerequisites for PFM - Web Console are satisfied. For details about the prerequisites for PFM - Web Console, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Procedure

- Troubleshoot window

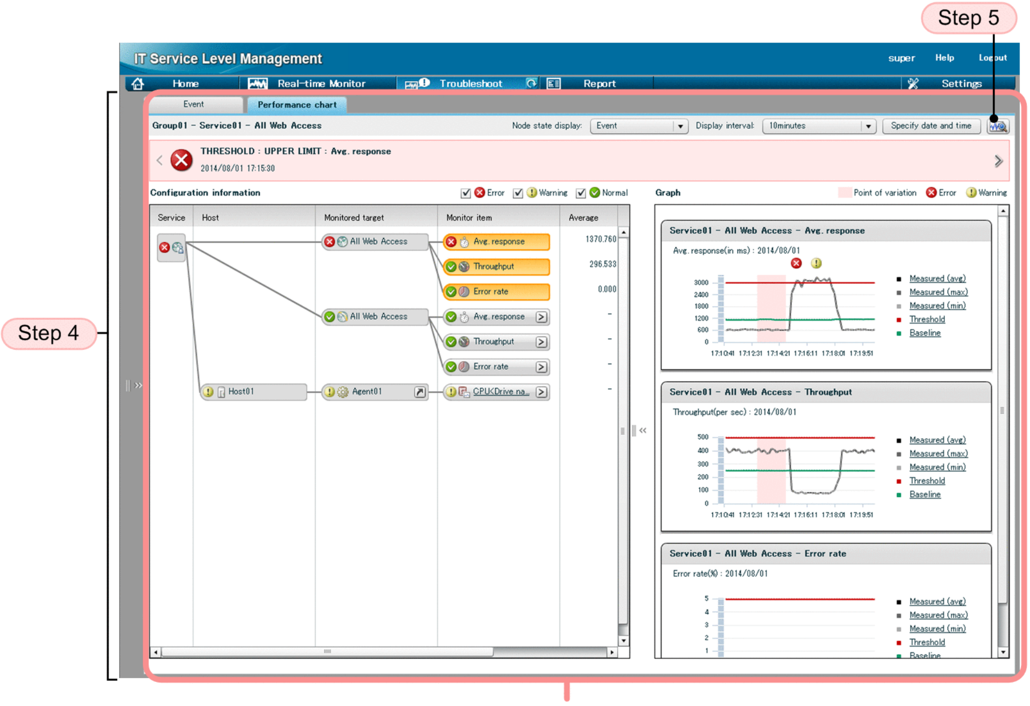


Group01 - Service01 - All Web Access

THRESHOLD : UPPER LIMIT : Avg. response
2014/08/01 17:15:30

Event and **Performance chart** tabs area

- Troubleshoot window (with the configuration information displayed)



Group01 - Service01 - All Web Access

THRESHOLD : UPPER LIMIT : Avg. response
2014/08/01 17:15:30

Monitor item	Average
Avg. response	1370.760
Throughput	296.533
Error rate	0.000
Avg. response	-
Throughput	-
Error rate	-
CPU(Drive na...	-

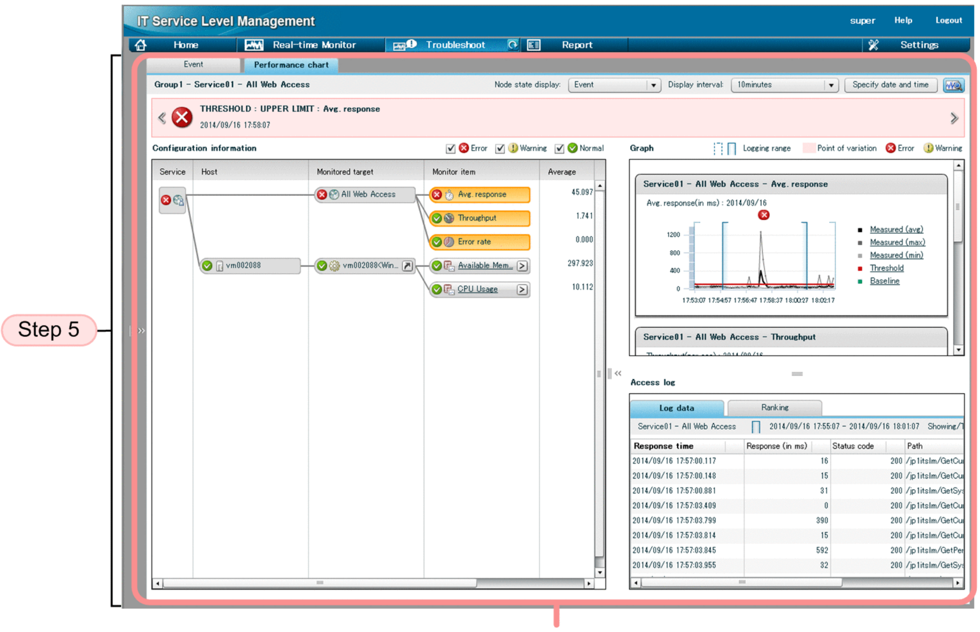
Service01 - All Web Access - Avg. response
Avg. response(in ms) : 2014/08/01

Service01 - All Web Access - Throughput
Throughput(per sec) : 2014/08/01

Service01 - All Web Access - Error rate
Error rate(%) : 2014/08/01

Event and **Performance chart** tabs area

- Troubleshoot window (with the access log displayed)



Group1 - Service01 - All Web Access

THRESHOLD : UPPER LIMIT : Avg. response
2014/09/16 17:58:07

Monitor item	Average
Avg. response	45.097
Throughput	1.741
Error rate	0.000
Available Mem...	297.923
CPU Usage	10.112

Service01 - All Web Access - Avg. response
Avg. response(in ms) : 2014/09/16

Service01 - All Web Access - Throughput

Service01 - All Web Access 2014/09/16 17:55:07 - 2014/09/16 18:01:07 Showing/T

Response time	Response (in ms)	Status code	Path
2014/09/16 17:57:00.117	16	200	/jp1itslm/GetCu
2014/09/16 17:57:00.148	15	200	/jp1itslm/GetCu
2014/09/16 17:57:00.881	31	200	/jp1itslm/GetSy
2014/09/16 17:57:03.409	0	200	/jp1itslm/GetCu
2014/09/16 17:57:03.799	390	200	/jp1itslm/GetCu
2014/09/16 17:57:03.814	15	200	/jp1itslm/GetCu
2014/09/16 17:57:03.845	592	200	/jp1itslm/GetPe
2014/09/16 17:57:03.955	32	200	/jp1itslm/GetSy

Event and **Performance chart** tabs area

To check past data:

1. Click the **Troubleshoot** button.
   The **Event** and **Performance chart** tabs area is displayed with the **Event** tab selected.

2. In the **Event** and **Performance chart** tabs area, click the **Performance chart** tab.
   Performance charts of monitored targets of the selected monitored service are displayed in the **Event** and **Performance chart** tabs area.

3. Use the performance charts to check past service performance.

Check the performance charts and look for a time period during which the average value for service performance started to veer significantly from the baseline. On a performance chart, a colored band indicates a timeframe during which a significant change in service performance occurred. The timeframe indicated by the colored band might be when the event causing the error or warning occurred.

4. Click » to display configuration information and add to the performance charts any monitoring item that you want to check.

   Display the configuration information and select a desired monitoring item. The performance chart for the selected monitoring item is displayed. Check the performance charts as needed.

   If ITSLM is linked with Performance Management, you can locate erroneous hosts in the ITSLM window, but not erroneous processes. Also, if errors and warnings have occurred in a Performance Management monitoring item that cannot be monitored by ITSLM, ITSLM cannot display such errors and warnings. Log in to Performance Management as needed to check for errors. Clicking the ↗ button displays the Performance Management login window. Log in to Performance Management using the user name you used for login to ITSLM.

   If you use a single sign-on to log in to Performance Management, the following conditions must be satisfied:

   - ITSLM - Manager and PFM - Web Console both use JP1/Base authentication and a common JP1/Base to manage users.
   - The user of the product to link with is defined in JP1/Base, and ITSLM - Manager operation permission (JP1_ITSLM_Admin or JP1_ITSLM_User) and PFM operation permission (JP1_PFM_Operator) are set for that user. For details, see "5.3.4 Setting up the users who will be using Performance Management (JP1 authentication mode)".
   - The user of the product to link with is logged in to ITSLM - Manager.

5. Click 🔍 to display the **Access log** area to investigate problems in Web system processing.

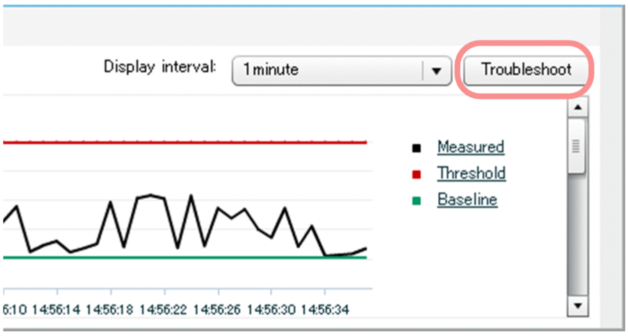
   If you are recording access log, click 🔍 to display the **Access log** area.

   You can then investigate any problems in Web system processing using the access log for the time period during which the error occurred.

You can use the displayed past service performance for troubleshooting purposes.

You can display the Troubleshoot window also from the Real-time Monitor window. To do this, select the monitored target of the monitored service in the **Services** area of the Real-time Monitor window, and then click the **Performance chart** tab.

In the **Event** and **Performance chart** tabs area, clicking the **Troubleshoot** button displays the Troubleshoot window.



Display interval: 1 minute

(3) Related topics

- *4.3.1 Checking the status of the monitored services of all service groups*

- *4.3.2 Checking the status of the monitored services in a specific service group*
- *4.4.3 Verifying recovery of monitored services after taking corrective action*
- *10.1.2(3) Services area*
- *10.4.1 Configuration of the Troubleshoot window*
- *10.4.3 Event and Performance chart tabs area (Event tab selected)*
- *10.4.4 Event and Performance chart tabs area (Performance chart tab selected)*
- *10.4.5 Access log area (Log data tab selected)*
- *10.4.6 Access log area (Ranking tab selected)*

4.4.3 Verifying recovery of monitored services after taking corrective action

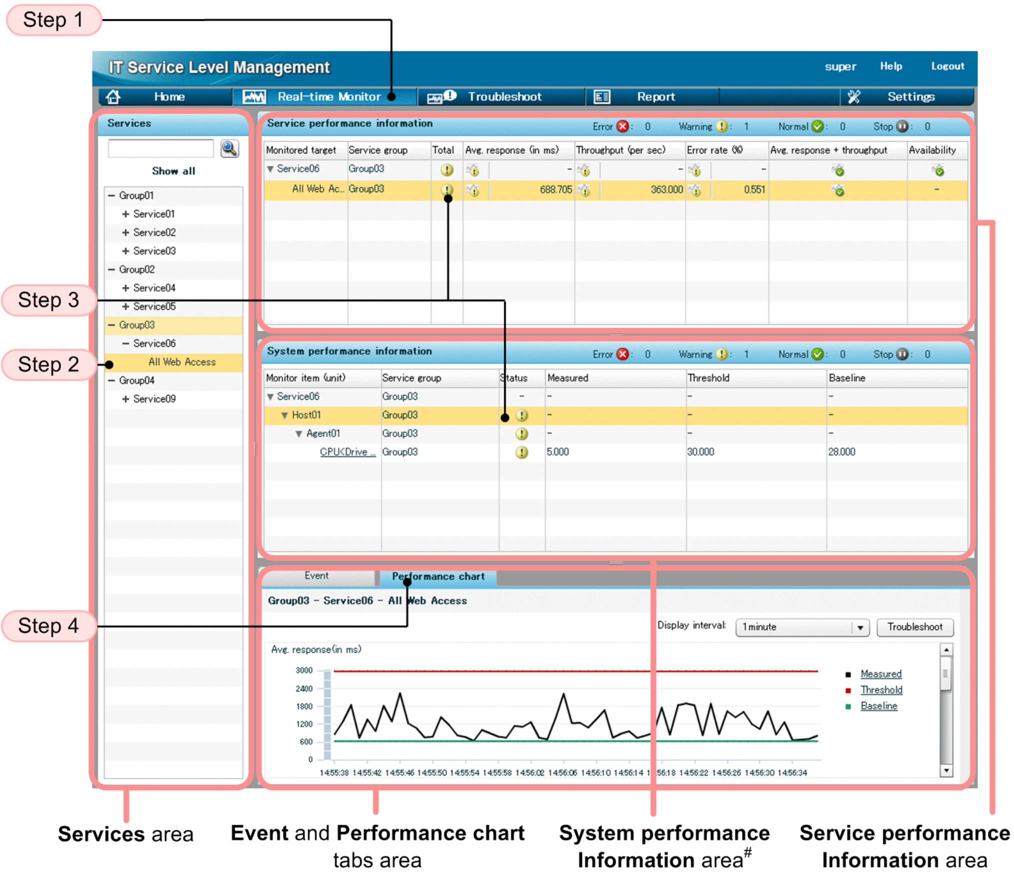
After you have taken the necessary corrective action to resolve an error or warning, you can verify that the monitored service has recovered and its status has returned to normal.

(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- If you link ITSLM with Performance Management, verify that PFM - Manager is running. For details about how to start PFM - Manager, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Procedure

The following shows the Real-time Monitor window that is used in this task:



Service performance information Error: 0 Warning: 1 Normal: 0 Stop: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service06	Group03	!	-	-	-	✓	✓
All Web Ac...	Group03	!	688.705	363.000	0.551	✓	-

System performance information Error: 0 Warning: 1 Normal: 0 Stop: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service06	Group03	-	-	-	-
▼ Host01	Group03	!	-	-	-
▼ Agent01	Group03	!	-	-	-
CPU<Drive ...	Group03	!	5.000	30.000	28.000

Group03 - Service06 - All Web Access

#: The **System performance information** area is displayed when ITSLM is linked with Performance Management.

To verify recovery of a monitored service after taking corrective action:

1. Click the **Real-time Monitor** button.

   The **Services**, **Service performance information**, and **System performance information**# areas and the **Event** and **Performance chart** tabs area are displayed. In the **Event** and **Performance chart** tabs area, the **Event** tab is selected.

2. From the **Services** area, select a monitored target of a monitored service.

3. In the **Service performance information** and **System performance information**# areas, check the status of the monitored target of the monitored service.

   Verify that the icon displayed under **Total** in the **Service performance information** area has returned to normal. If the icon for normal status is not displayed, the monitored service might not have recovered correctly. Check the cause again, and then take an appropriate corrective action.

   Also, verify that the icon displayed under **Status** in the **System performance information** area# has returned to normal. If the icon for normal status is not displayed, the monitored service might not have recovered correctly. Check the cause again, and then take an appropriate corrective action.

   If the monitored service has recovered from an error detected by out-of-range value detection, verification is complete. If it has recovered from an error detected by threshold value monitoring, go to step 4, if necessary.

4. In the **Event** and **Performance chart** tabs area, click the **Performance chart** tab to verify that the monitored target of the monitored service has recovered and its status has returned to normal.

The current status of the monitored target of the monitored service is displayed as a performance chart. Verify that the current status of the monitored target of the monitored service shown at the right end of performance chart is below the threshold.

If everything has returned to normal, verification of recovery is complete.

#

The **System performance information** area is displayed when ITSLM is linked with Performance Management. Selecting a monitoring item displayed in the **System performance information** area does not display performance information in the **Event** and **Performance chart** tabs area.

(3) Related topics

- *4.4.1 Checking the timing of an event causing an error or warning*
- *4.4.2 Checking past data*
- *10.3.1 Configuration of the Real-time Monitor window*
- *10.1.2(3) Services area*
- *10.3.3 Service performance information area*
- *10.3.4 System performance information area*
- *10.3.5 Event and Performance chart tabs area (Event tab selected)*
- *10.3.6 Event and Performance chart tabs area (Performance chart tab selected)*

4.5 Creating reports

ITSLM can assist you in reporting the service performance status of monitored services.

4.5.1 Overview of report creation

ITSLM helps you create reports efficiently by displaying monitoring items to be checked as reports and saving reports as CSV files.

ITSLM enables you to achieve the following:

- Displaying in windows as reports the accumulated service performance, system performance, and availability information data for monitored services.
- Saving as templates the view/hide settings for service performance, system performance, and availability information for monitoring items of monitored services.
- Outputting values in performance charts to CSV files.

For details about the Report window, see *10.5 Report window and the windows displayed from the Report window*.

(1) Items that can be displayed in reports

ITSLM enables you to display in windows the following items as reports for purposes of verification (note that this information cannot be output to CSV files):

Service performance

Displays the service monitoring status of monitored services that are monitored in ITSLM. The items that can be displayed as service performance for monitored services include the monitored targets, monitoring items (units), average values, SLO compliance rates, and comparisons (as percentages) to previous periods.

This is the service performance of **All Web Access** or Web transactions under a selected monitored service.

System performance

When ITSLM is linked with Performance Management for monitoring of monitored services, displays the monitoring status of the hosts that are providing the monitored services. The items that can be displayed as system performance include the hosts, monitored targets, monitoring items (units), average values, SLO compliance rates, and comparisons (as percentages) to previous periods.

If a selected monitored service is not linked with Performance Management, this information is all blanks.

Availability information

When ITSLM is linked with Performance Management for monitoring of monitored services, displays service availability, MTTR, and MTBF as availability information.

If the monitored service is not running availability monitoring, the hyphen (-) is displayed as the value of service availability, MTTR, and MTBF.

Service availability overview

Displays the service start and stop times during the report period for the monitored services for which availability monitoring is running.

If availability monitoring is not running for a selected monitored service, this information is blanks. However, if availability monitoring is not running currently but was run at some point during the specified report interval, those availability monitoring results are displayed.

The following table provides the details of the items that can be displayed in reports.

Table 4–3: Details of items that can be displayed in reports

No.	Item	Items in table	Value to be displayed
1	**Service performance**	**Monitored target**	Name of the selected monitored target
2		**Monitor item (unit)**	• Average response time • Throughput • Error rate
3		**Average**[#1]	• For average response time: *Total average response time during the report interval / number of requests during the report interval* (milliseconds) • For throughput: *Number of requests during the report interval (excluding requests whose responses timed out before ITSLM - UR could receive them) / operation time during the report interval* (count/second) • For error rate: (*Number of times HTTP status returned an error response during the report interval + number of requests whose responses timed out before ITSLM - UR could receive them*) / *number of requests during the report interval* (%)
4		**SLO compliance rate**[#1]	(1.0 - *duration of overages of a threshold / operation time for one month*) × 100 (%)
5		Comparison to a previous period (as a percentage)[#2, #3]	(*Average response time during report interval / average response time during comparison period for the report interval* - 1.0) × 100 (%)
6	**System performance**	**Host**	Host name of the selected monitored service
7		**Monitored target**	Name of the monitoring agent contained in the host
8		**Monitor item (unit)**	Name of a monitoring item contained in the monitoring agent
9		**SLO compliance rate**[#1]	(1.0 - *duration of overages of a threshold / operation time for one month*) × 100 (%)
10		**Average**[#1]	Average value for the monitoring item
11		Comparison to a previous period (as a percentage)[#2, #3]	(*Average response time during report interval / average response time during comparison period for the report interval* - 1.0) × 100) (%)
12	**Availability info**	**Service availability %**[#2]	(*Sum of all operation periods during report interval* / (*sum of all operation periods during report interval + sum of all error periods during report interval*) × 100) (%)
13		MTTR[#1]	*Sum of all error periods during report interval / number of error periods during report interval* (minutes)
14		MTBF[#1]	*Sum of all operation periods during report interval / number of error periods during report interval* (minutes)
15	**Service availability overview**	**Date and time**[#4]	Date and time an event related to availability monitoring occurred during the report interval

No.	Item	Items in table	Value to be displayed
16	**Service availability overview**	**Event**	One of the following events related to availability monitoring that occurred during the report interval: • **Service stop** • **Service recovery** • **Start of service monitoring** • **Stop of service monitoring**

#1

The value is rounded to the first decimal place.

#2

The value is rounded to the second decimal place.

#3

For a comparison to a previous period, the percentage is calculated for the monitored service's service performance or system performance, and the table header and the period used for comparison depend on the report interval setting.

The following table shows the relationship between the report interval and the previous period to which the percentage applies.

Table 4–4: Relationship between report interval and previous period to which percentage applies

No.	Report interval	Table header	Period used for comparison
1	1 day	**VS previous day**	Day immediately preceding the start date
2	1 week	**VS previous week**	Seven days immediately preceding the start date
3	1 month	**VS previous month**	From the same date in the previous month to the preceding day
4	3 months	**VS previous quarter**	From the same date three months ago to the preceding day

#4

Displayed in the format *YYYY*/*MM*/*DD hh*:*mm*, based on the ITSLM - Manager's time zone.

(2) Performance charts displayed in reports

You can display performance charts in reports in addition to the monitoring items described in subsection *(1)*. The displayed performance chart information can also be output to a CSV file.

A performance chart for a specified period (year or month) is displayed for each monitoring item. In the Preview report window, you can display a maximum of 10 monitoring items of your choice.

The axes and display range of each performance chart are as follows:

- Ordinate: Monitoring item
  The display range is from the minimum value in the report interval to the maximum value in the displayed month. If an SLO threshold value is greater than the maximum value, the SLO threshold value becomes the maximum value.
- Abscissa: Date (days)
  The display range is from 1 to the last day of the report interval.

The following table describes the information that can be displayed in performance charts for the monitoring items.

Table 4–5: Information displayed in performance charts

No.	Type of line graph	Information that is displayed
1	Maximum-value line	Line graph connecting the maximum measurement values.
2	Minimum-value line	Line graph connecting the minimum measurement values.

No.	Type of line graph	Information that is displayed
3	Average-value line	Line graph connecting the average measurement values.
4	SLO threshold value	Line graph connecting the monitoring item's threshold values.

Note: Measurement values obtained when the throughput is 0 are not used.

Plotting intervals of performance charts depend on the report interval settings.

The following table shows the relationship between the report interval and the performance chart's plotting interval.

Table 4–6: Relationship between report interval and performance chart's plotting interval

No.	Report interval	Plotting interval of performance chart
1	1 day	Aggregate value for every 30 minutes
2	1 week	Aggregate value for two hours
3	1 month	Daily aggregate value
4	3 months	Daily aggregate value

Note that the plotting interval of a performance chart is the same as the interval of data output to a CSV file.

(3) CSV file format

ITSLM enables you to output the data for performance charts displayed in reports to CSV files. You can output a maximum of 50 monitoring items to a CSV file.

This subsection explains the CSV file name, output format, and output character encoding. It also presents output examples.

File names

The following table shows the file names that are displayed by default.

Table 4–7: Default file names

No.	Report interval	File name	Interval in graph display
1	1 day	`report_`*YYYYMMDD*`_d.csv`	30 minutes
2	1 week	`report_`*YYYYMMDD*`_w.csv`	2 hours
3	1 month	`report_`*YYYYMM*`_m.csv`	1 day
4	3 months	`report_`*YYYYMM*`_q.csv`	1 day

Legend:

YYYYMMDD

YYYY, *MM*, and *DD* indicate the report start date selected in the Report window. You can change the file names.

Output format

The first line displays header information and the lines beginning with line 2 display data. The data is displayed in the same order as on performance charts displayed in the Report window.

- Correspondence between header information and data

  The table below describes the correspondence between the header information that is output to the first line and the data that is output to the lines beginning with line 2.

  You can select the monitoring items to be output to a CSV file. If necessary, you can edit or add templates and set the monitoring items to be output to CSV files.

Table 4–8: Correspondence between the header information and the data beginning on line 2

No.	Monitoring item	Header information#	Data beginning on line 2
1	--	`Date`	Date and time ITSLM acquired the data
2	Average response time	`Average`	Average value of the average response times
3		`Max`	Maximum value of the average response times
4		`Min`	Minimum value of the average response times
5	Throughput	`Average`	Average throughput value
6		`Max`	Maximum throughput value
7		`Min`	Minimum throughput value
8	Error rate	`Average`	Average error rate value
9		`Max`	Maximum error rate value
10		`Min`	Minimum error rate value
11	Name of a monitoring item for a monitoring agent	`Average`	Monitoring item's average value
12		`Max`	Monitoring item's maximum value
13		`Min`	Monitoring item's minimum value

Legend:

--: Not applicable

Note

An average response time obtained when the average response time and throughput values are both `0` is treated as no data obtained, and is therefore not included in the average, maximum, and minimum values.

Similarly, an error rate obtained when the error rate and throughput values are both `0` is treated as no data obtained, and is therefore not included in the average, maximum, and minimum values.

#

Under the header information output to a CSV file, the entries for `Average`, `Max`, and `Min` are displayed in this order for each monitoring item. The header information is displayed in the following format:

monitored-target-name / *monitoring-item-name*

For *monitored-target-name* and *monitoring-item-name*, the following information is displayed:

monitored-target-name = `All Web Access` | *Web-transaction-name* | *host-name* / *monitoring-agent-name*

monitoring-item-name = *average-response-time* | *throughput* | *error-rate* | *name-of-monitoring-agent's-monitoring-item*

- Format of data

  The data that begins on line 2 is displayed in the following format:

  YYYY/*MM*/*DD hh*:*mm*,*AA....AA*

  YYYY/*MM*/*DD hh*:*mm* indicate the date (*year*/*month*/*date*) and time (*hour*:*minute*) the data was acquired by ITSLM.

  AA....AA indicates the comma-separated data items (values) acquired for each monitoring item. Average response time is in milliseconds.

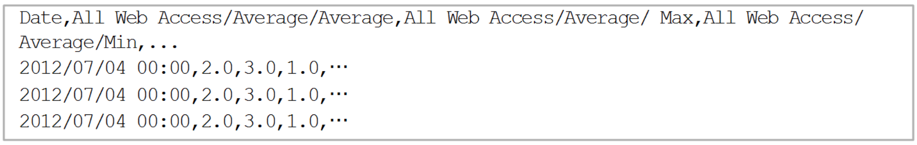
Output character encoding

The character encoding used is UTF-8.

Output examples

Performance charts are output to a CSV file in the same order they are displayed in the Preview report window.

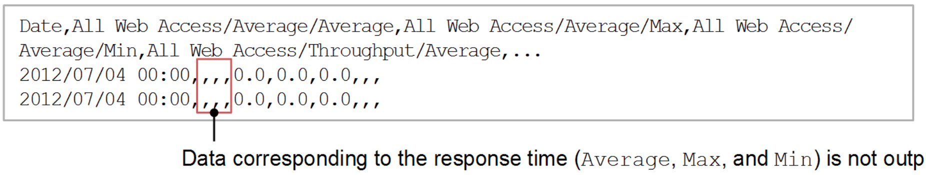
In the output example below, the monitored target is All Web Access and some of the data is omitted.



```
Date,All Web Access/Average/Average,All Web Access/Average/ Max,All Web Access/
Average/Min,...
2012/07/04 00:00,2.0,3.0,1.0,…
2012/07/04 00:00,2.0,3.0,1.0,…
2012/07/04 00:00,2.0,3.0,1.0,…
```

Note that in a report output for a month, if some of a day's data is missing for a reason such as the number of responses acquired by ITSLM - UR was zero, the header information is displayed, but no values are displayed.

Output example when some of a day's data is missing

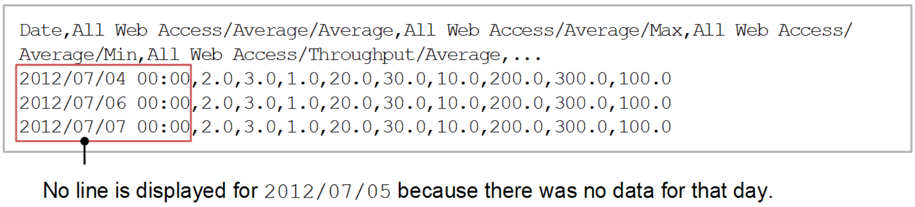


```
Date,All Web Access/Average/Average,All Web Access/Average/Max,All Web Access/
Average/Min,All Web Access/Throughput/Average,...
2012/07/04 00:00,,,,0.0,0.0,0.0,,,
2012/07/04 00:00,,,,0.0,0.0,0.0,,,
```

Data corresponding to the response time (`Average`, `Max`, and `Min`) is not output.

If the aggregate data for a day is missing for a reason such as monitoring of the monitored target of the monitored service was stopped, the entire line for that day is omitted.

Output example when aggregate data for a day is omitted

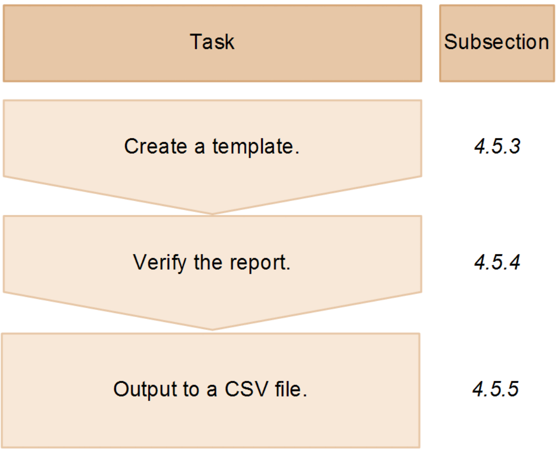


```
Date,All Web Access/Average/Average,All Web Access/Average/Max,All Web Access/
Average/Min,All Web Access/Throughput/Average,...
2012/07/04 00:00,2.0,3.0,1.0,20.0,30.0,10.0,200.0,300.0,100.0
2012/07/06 00:00,2.0,3.0,1.0,20.0,30.0,10.0,200.0,300.0,100.0
2012/07/07 00:00,2.0,3.0,1.0,20.0,30.0,10.0,200.0,300.0,100.0
```

No line is displayed for `2012/07/05` because there was no data for that day.

4.5.2 General procedure for creating a report

The following figure shows the general procedure when ITSLM is used to create a report:



Task	Subsection
Create a template.	*4.5.3*
Verify the report.	*4.5.4*
Output to a CSV file.	*4.5.5*

1. Create a template.

   You can create a template with desired monitoring items specified. This eliminates the need to specify the monitoring items for each monitored service.

   For details about how to create templates, see *4.5.3 Creating report templates*.

2. Verify the report.

   You can display the monitoring items specified in the template in the window. For details about verifying the report, see *4.5.4 Verifying report data in the window*.

3. Output to a CSV file.
   You can output the items displayed in the window in step 2 to a CSV file.
   For details about how to output to CSV files, see *4.5.5 Outputting report data*.

4.5.3 Creating report templates

You can use templates when you output reports for monitored services.

ITSLM supports two types of templates, as described in the following table.

Table 4–9: Types of templates

No.	Type	Description
1	Default template	When a new monitored service is added in ITSLM, a default template is provided for that monitored service. This template is named `Default`. You can change the default template settings, but you cannot create, rename, or delete a default template.
2	User-created template	This is user-created report settings saved as a template. You can create a template for each monitored service and share it with other users who are permitted to access that monitored service. Once you have created a template, you can change its settings, as well as rename or delete the template.

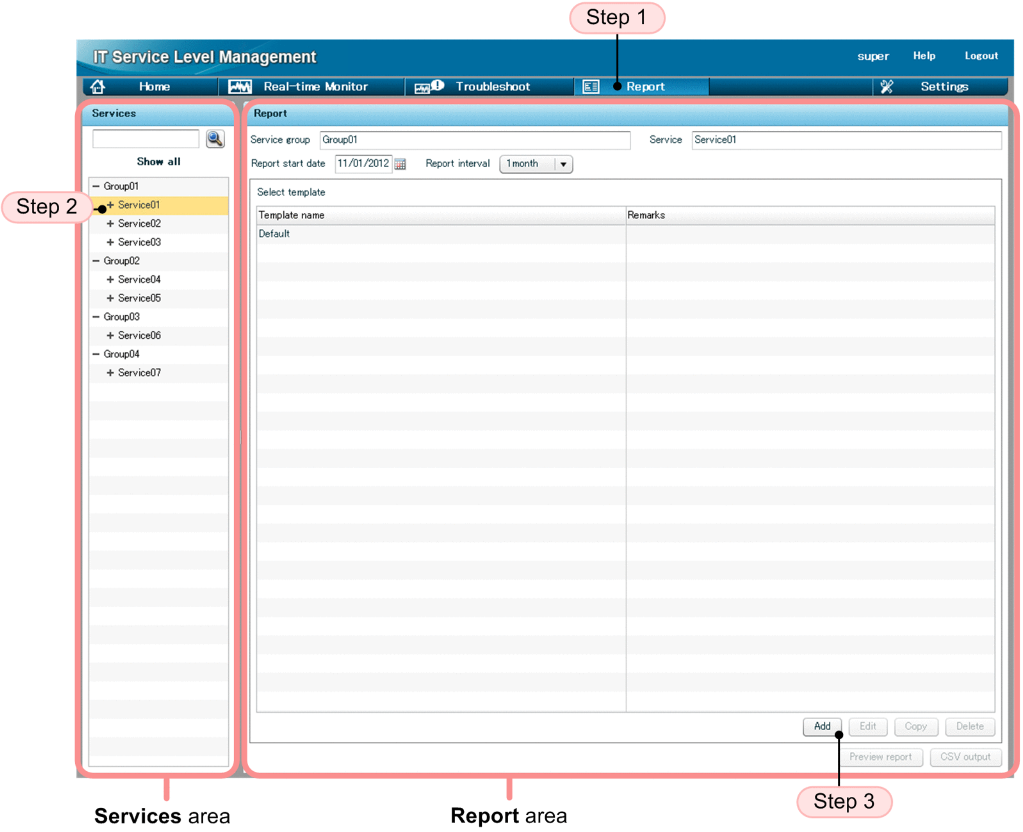
(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.

(2) Procedure

The following shows the Report window and the Add template window that are used in this task:

- Report window



Services: Group01 (Service01, Service02, Service03), Group02 (Service04, Service05), Group03 (Service06), Group04 (Service07)

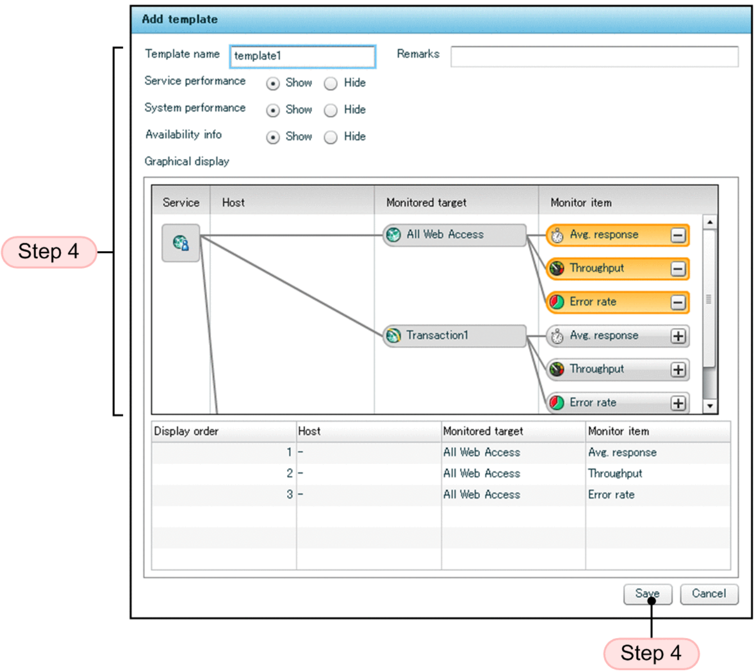
Service group: Group01 Service: Service01

Report start date: 11/01/2012 Report interval: 1month

Select template

Template name	Remarks
Default	

- Add template window



Template name: template1 Remarks:

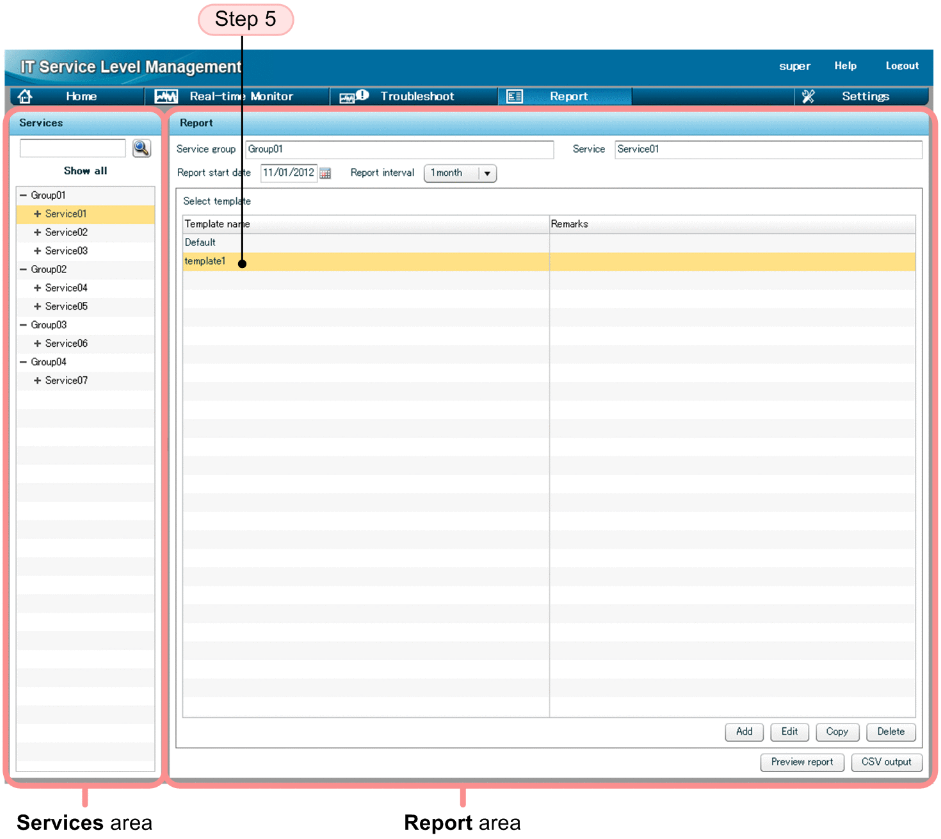
Service performance: ● Show ○ Hide

System performance: ● Show ○ Hide

Availability info: ● Show ○ Hide

Display order	Host	Monitored target	Monitor item
1	–	All Web Access	Avg. response
2	–	All Web Access	Throughput
3	–	All Web Access	Error rate

- Report window (with a template added)



Service group: Group01
Service: Service01
Report start date: 11/01/2012
Report interval: 1month

Select template

Template name	Remarks
Default	
template1	

To create a report template:

1. Click the **Report** button.
2. From the **Services** area, select the monitored service for which a report is to be output.
3. In the **Report** area, click the **Add** button.
   The Add template window is displayed. You define a new template in this window.
4. Specify a name for the template and the items that you want to display, and then click the **Save** button.
   When you select monitoring items for graphical display, the selected items are displayed in a table. After you have specified the items that you want to display and you then click the **Save** button, the template is saved.
5. Verify that the added template is displayed in the **Report** area.
   Verify that the new template has been added to **Template name**.

If you want to change the contents of a saved template, select the template and then click the **Edit** button. After you change settings, click the **Save** button to apply the changes.

(3) Related topics

- *10.1.2(3) Services area*
- *10.5.1 Configuration of the Report window*
- *10.5.3 Report area*
- *10.5.4 Add template window*
- *10.5.6 Copy template window*

4.5.4 Verifying report data in the window

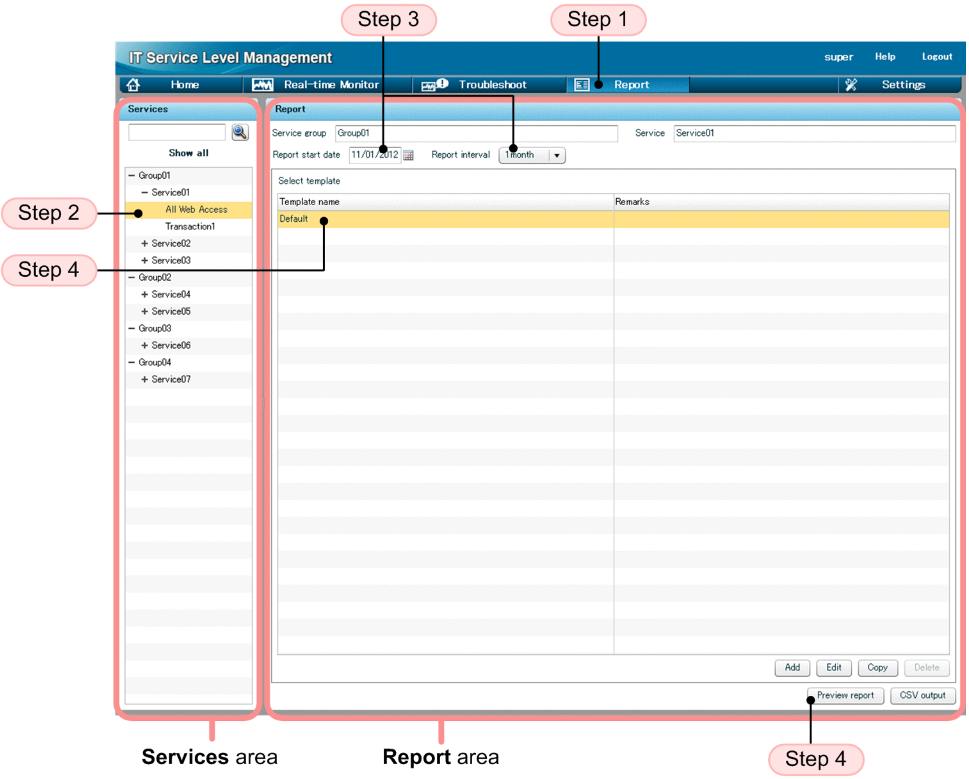
(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.

(2) Procedure

The following shows the Report window and the Preview report window that are used in this task:

- Report window



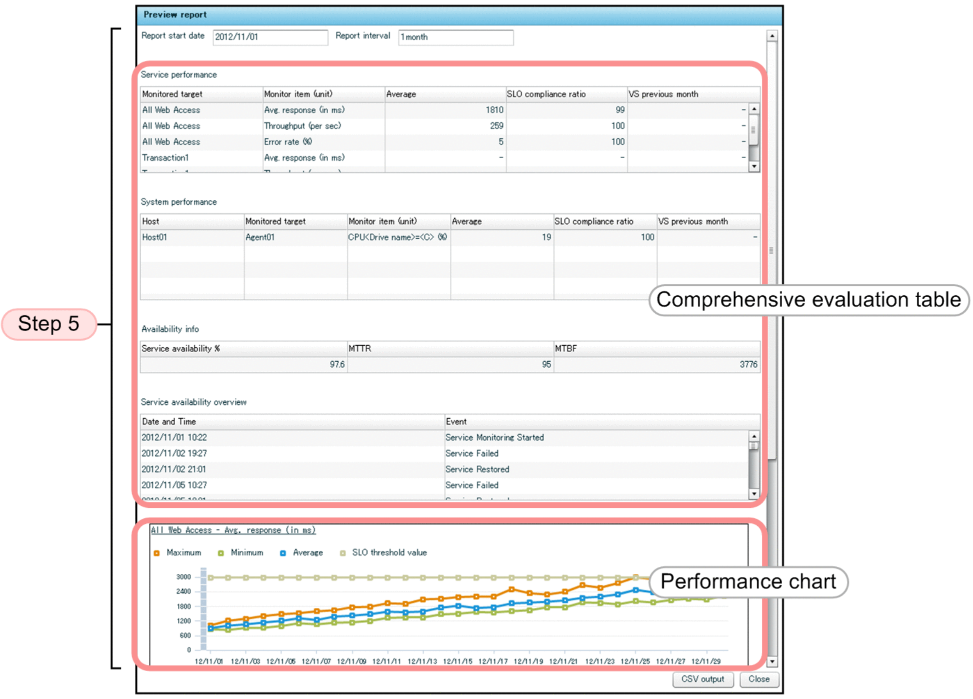
Service group: Group01

Service: Service01

Report start date: 11/01/2012

Report interval: 1 month

- Preview report window



Preview report

Report start date: 2012/11/01 Report interval: 1month

Service performance

Monitored target	Monitor item (unit)	Average	SLO compliance ratio	VS previous month
All Web Access	Avg. response (in ms)	1810	99	-
All Web Access	Throughput (per sec)	259	100	-
All Web Access	Error rate (%)	5	100	-
Transaction1	Avg. response (in ms)	-	-	-

System performance

Host	Monitored target	Monitor item (unit)	Average	SLO compliance ratio	VS previous month
Host01	Agent01	CPU<Drive name>=<C> (%)	19	100	-

Availability info

Service availability %	MTTR	MTBF
97.6	95	3776

Service availability overview

Date and Time	Event
2012/11/01 10:22	Service Monitoring Started
2012/11/02 19:27	Service Failed
2012/11/02 21:01	Service Restored
2012/11/05 10:27	Service Failed

To verify report data in a window:

1. Click the **Report** button.

2. From the **Services** area, select the monitored service for which a report is to be output.

3. In **Report start date**, specify the start date for the report. Alternatively, from the **Report interval** pull-down menu, select the period that you want to check.
   If you want to output data for the current month, you can skip this step.

4. Select a template and then click the **Preview report** button.
   The Preview report window is displayed.
   Select either **Default** or an added template, and then display the report. The Preview report window displays a comprehensive evaluation table and a performance chart for the specified period for the monitored target of the monitored service.

5. In the Preview report window, check the status of the monitored target of the monitored service over the specified period.
   Check the information output to the report for the status of the monitored target of the monitored service.

(3) Related topics

- *4.5.5 Outputting report data*
- *4.5.6 Notes on when some service performance data has not been acquired*
- *4.5.7 Notes on when a threshold is changed during the specified report interval*
- *4.5.8 Notes about time zone differences from one host to another*
- *10.1.2(3) Services area*
- *10.5.1 Configuration of the Report window*
- *10.5.3 Report area*

- *10.5.7 Preview report window*

4.5.5 Outputting report data

This subsection explains how to output service performance for a specified period to a CSV file.

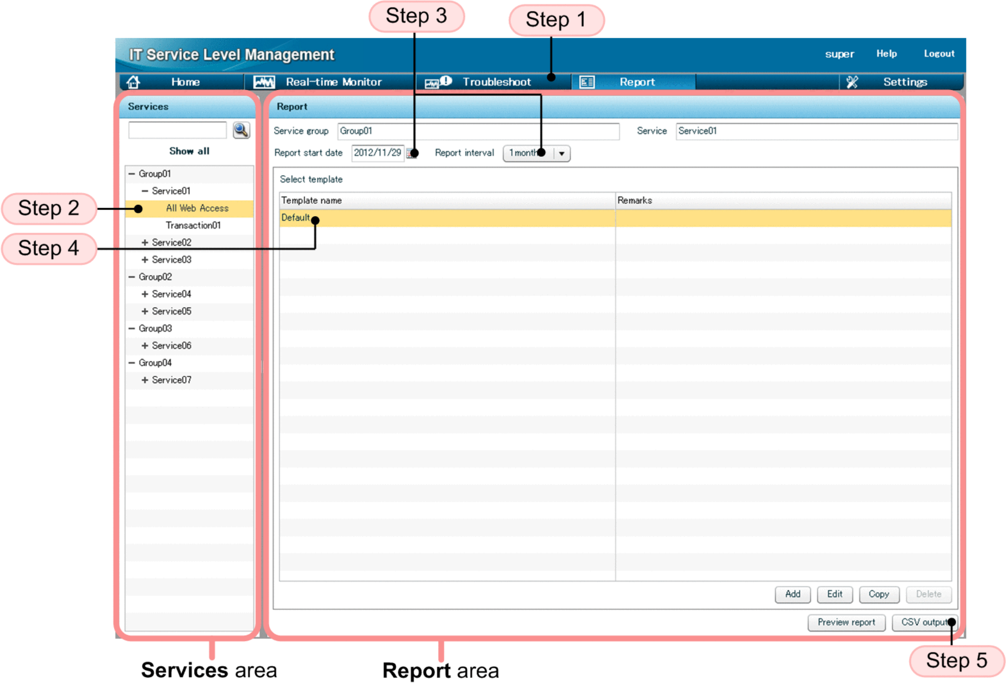
(1) Before you start

- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.
- Verify that monitoring has started.
  For details about how to start monitoring, see *4.2.1 Starting monitoring*.

(2) Procedure

The following shows the Report window that is used in this task:

- Report window



Service group: Group01
Service: Service01
Report start date: 2012/11/29
Report interval: 1month

Template name	Remarks
Default	

To output report data:

1. Click the **Report** button.

2. From the **Services** area, select a monitored service for which a report is to be output.
   The status of the monitored target of the selected monitored service for the current month is displayed in the **Report** area.
   This status is displayed as a comprehensive evaluation table and a performance chart. To check the status for the current month, go to step 5.

3. In **Report start date**, specify a start date for the report. Alternatively, from the **Report interval** pull-down menu, select a desired period that you want to check.

If you want to output data for the current month, you can skip this step.

A comprehensive evaluation table and a performance chart for the specified period are displayed in the **Report** area for the monitored target of the monitored service.

4. Select a template.

   This step is necessary if you use a template to output a report of the monitored service. If you do not use a template or you output a report of system performance, you can skip this step.

5. Click the **CSV output** button.

   The Download Files dialog box is displayed. Save the file at a desired location.

   > **Important note**
   >
   > If the selected monitored service or template had been deleted when the **CSV output** button is clicked, an empty CSV file is output. In such a case, an error message indicating that the selected monitored service or template had been deleted is output to the message logs.

If the CSV file has been saved, report output is complete.

If no aggregate data is available for a monitoring item in the data output as a CSV file, no value is displayed for that item in the performance chart.

If no aggregate data is available for all monitoring items in the data output as a CSV file, no line is output for the corresponding time in the performance chart.

(3) Related topics

- *4.5.4 Verifying report data in the window*
- *4.5.6 Notes on when some service performance data has not been acquired*
- *4.5.7 Notes on when a threshold is changed during the specified report interval*
- *4.5.8 Notes about time zone differences from one host to another*
- *10.1.2(3) Services area*
- *10.5.1 Configuration of the Report window*
- *10.5.3 Report area*

4.5.6 Notes on when some service performance data has not been acquired

If service performance data has not been acquired for some periods and a report is displayed in the window, some limitations apply to display of the report data.

This subsection explains how report data is displayed in comprehensive evaluation tables and performance charts when some service performance data has not been acquired.

Tip

Limitations to the report data displayed in a comprehensive evaluation table and performance chart depend on the report interval. The available report intervals are one day, one week, one month, and three months, and their service performance acquisition intervals are different. The report interval is one month in the examples presented in *(1) Comprehensive evaluation table that is displayed when some service performance data has not been acquired* and *(2) Performance chart that is displayed when some service performance data has not been acquired*. This means that the interval at which service performance is acquired is one day. The values in comprehensive evaluation tables and performance charts are based on the interval at which service performance is acquired.

The table below shows the interval at which service performance is acquired for each report interval. Based on the specified report interval, replace the corresponding information provided in *(1) Comprehensive evaluation table that is displayed when some service performance data has not been acquired* and *(2) Performance chart that is displayed when some service performance data has not been acquired* with the correct information.

Table 4–10: Display interval for each report interval

No.	Report interval	Display interval
1	1 day	30 minutes
2	1 week	2 hours
3	1 month	1 day
4	3 months	1 day

(1) Comprehensive evaluation table that is displayed when some service performance data has not been acquired

If some of the service performance data has not been acquired, there are limitations to the data that is displayed in a comprehensive evaluation table. The limitations differ depending on the specified report interval. The table below describes the data that is displayed in a comprehensive evaluation table when the report interval is set to one month. For the data that is displayed when the report interval is one day, one week, or three months, see *Hint*, above.

Table 4–11: Data displayed in a comprehensive evaluation table when some service performance data has not been acquired (for a report interval of one month)

No.	Evaluation item	Period for which data is missing		
		Less than one day	At least one day but less than one month	One month or more
1	Average value	Displays the average value for the month, including days for which there is less than a full day's worth of data. If the number of days on which data has been acquired is less than the full month, the average value for the month is calculated from only the acquired data.	Displays the average value for the month, excluding the missing days.	Displays a hyphen (–).
2	SLO compliance rate	Displays the SLO compliance rate for the month, including	Displays the SLO compliance rate for the month, excluding the missing days.	

No.	Evaluation item	Period for which data is missing		
		Less than one day	At least one day but less than one month	One month or more
2	SLO compliance rate	the days for which there is less than one day's worth of data.	Displays the SLO compliance rate for the month, excluding the missing days.	Displays a hyphen (−).
3	Comparison to previous period (percentage)#	Displays the comparison to the previous period of item 1 above. If data for the previous period has not been acquired, displays a hyphen (−).		

#

The displayed table headers depend on the specified report interval. For the table header that is displayed for each report interval, see Table *4-4 Relationship between report interval and previous period to which percentage applies*.

(2) Performance chart that is displayed when some service performance data has not been acquired

If some of the service performance data has not been acquired, there are limitations to the data that is displayed in a performance chart. The limitations differ depending on the specified report interval. The table below describes the data that is displayed in a performance chart when the report interval is set to one month. For the data that is displayed when the report interval is one day, one week, or three months, see *Hint*, above.

Table 4–12: Data displayed in a performance chart when some service performance data has not been acquired (for a report interval of one month)

No.	Type of line graph	Period for which data is missing		
		Less than one day	At least one day but less than one month	One month or more
1	Threshold-value line	The threshold for each day is plotted, including for the days with less than a full day's worth of data, and a line graph is drawn based on those values.	The threshold for each day is plotted, excluding the missing days, and a line graph is displayed based on those values.	Not displayed.
2	Maximum-value line	The maximum value of each day is plotted, including the days with less than a full day's worth of data, and a line graph is drawn based on those values.	The maximum value for each day is plotted, excluding the missing days, and a line graph is displayed based on those values.#2	
3	Average-value line	The average value for each day is plotted, including the days with less than a full day's worth of data, and a line graph is drawn based on those values.#1	The average value for each day is plotted, excluding the missing days, and a line graph is displayed based on those values.#2	
4	Minimum-value line	The minimum value for each day is plotted, including the days with less than a full day's worth of data, and a line graph is drawn based on those values.	The minimum value for each day is plotted, excluding the missing days, and a line graph is displayed based on those values.#2	

Note

An average response time obtained when the average response time and throughput values are both `0` is treated as no data obtained. Therefore, it is not included in the average, maximum, and minimum values.

Similarly, an error rate obtained when the error rate and throughput values are both `0` is treated as no data obtained. Therefore, it is not included in the average, maximum, and minimum values.

#1

When using a day for which less than a full day's worth of data was acquired, the average value for that day is calculated using only the acquired data.

#2

A missing day is displayed as a gap in the line graph. If a day for which a full day's worth of data is available is both preceded and followed by a missing day, that day is displayed as a point.

(3) Related topics

- *4.5.4 Verifying report data in the window*
- *4.5.5 Outputting report data*
- *10.5.7 Preview report window*

4.5.7 Notes on when a threshold is changed during the specified report interval

If a threshold is changed during the specified report interval and a report is displayed in the window, some limitations apply to the display of report data.

This subsection explains how report data is displayed in comprehensive evaluation tables and performance charts when a threshold is changed during the specified report interval.

(1) Comprehensive evaluation table that is displayed when a threshold is changed during the specified report interval

If a threshold is changed during the specified report interval, there are limitations to the data that is displayed in a comprehensive evaluation table. The table below describes the data that is displayed in a comprehensive evaluation table.

Table 4–13: Comprehensive evaluation table that is displayed when a threshold is changed during the specified report interval

No.	Evaluation item	Data that is displayed
1	Average value	Displays the average value for the specified report interval.
2	SLO compliance rate	Displays the compliance rate of the thresholds for the specified report interval. For the threshold compliance rate, data is retained at the plotting interval#1 for each specified report interval. Therefore, when the report interval is one month and threshold is not monitored for a 30-minute period, the threshold for that period is not used for the calculation of the threshold compliance rate. However, if a period during which threshold value monitoring was not running is intermixed with periods during which threshold value monitoring was running in a 30-minute interval, the threshold compliance rate is calculated assuming that the threshold compliance was met for the period during which threshold value monitoring was not running.
3	Comparison to previous period (percentage)#2	Displays the percentage of the average value for the specified report interval compared to that for the previous period.

#1

The plotting interval depends on the specified report interval. For the correspondence between report interval and plotting interval, see Table *4-6 Relationship between report interval and performance chart's plotting interval*.

If the plotting interval is 30 minutes, the ranges are *XX*`:00:00` to *XX*`:29:59` and *XX*`:30:00` to *XX*`:59:59` (in the format *hour*:*minute*:*second*, where *XX* is `00` to `23`).

#2

The displayed table headers depend on the specified report interval. For the table header that is displayed for each report interval, see Table *4-4 Relationship between report interval and previous period to which percentage applies*.

(2) Performance chart that is displayed when a threshold is changed during the specified report interval

If a threshold is changed during the specified report interval, there are limitations to the data that is displayed in a performance chart. The table below describes the data that is displayed in a performance chart.

Table 4–14: Performance chart that is displayed when a threshold is changed during the specified report interval

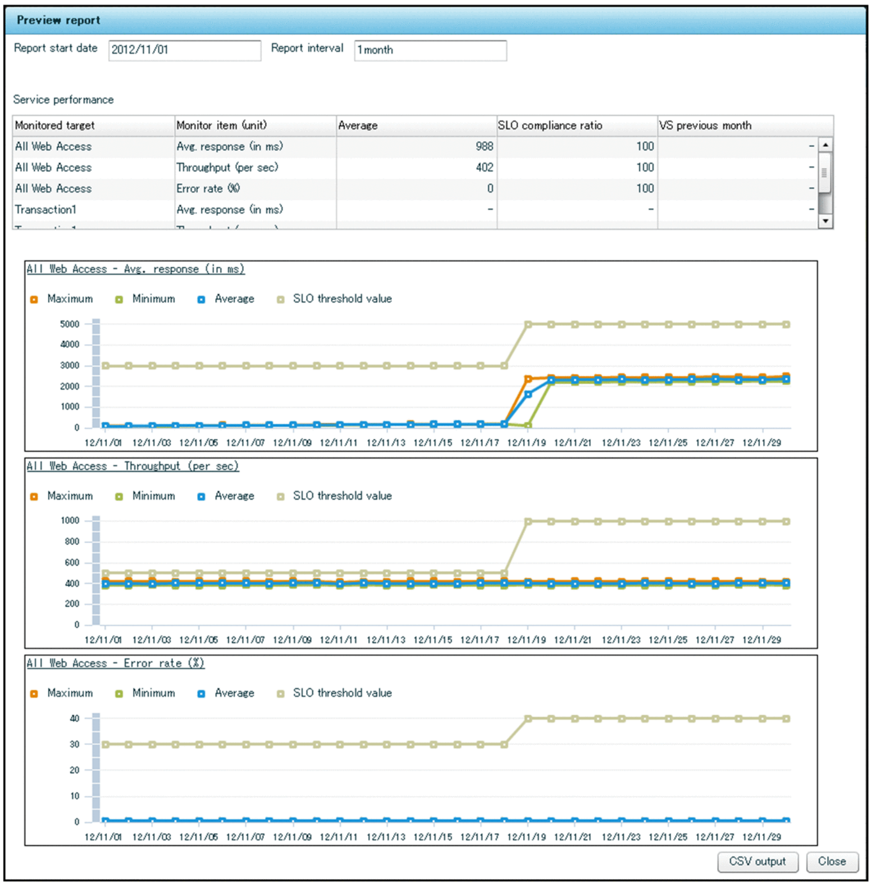
No.	Type of line graph	Data that is displayed
1	Threshold-value line	The thresholds are plotted at the plotting intervals# for the specified report interval, and a line graph is drawn based on those values. For example, if the report interval is one month, the maximum value is displayed for the day on which the threshold is changed.
2	Maximum-value line	The maximum values are plotted at the plotting intervals# for the specified report interval, and a line graph is drawn based on those values.
3	Average-value line	The average values are plotted at the plotting intervals# for the specified report interval, and a line graph is drawn based on those values.
4	Minimum-value line	The minimum values are plotted at the plotting intervals# for the specified report interval, and a line graph is drawn based on those values.

#

The plotting interval depends on the specified report interval. For the correspondence between the report interval and the plotting interval, see Table *4-6 Relationship between report interval and performance chart's plotting interval*.

The following figure shows a comprehensive evaluation table and performance chart example when a threshold was changed during the specified report interval.

Figure 4–2: Comprehensive evaluation table and performance chart example when a threshold was changed during the specified report interval



Preview report

Report start date: 2012/11/01

Report interval: 1month

Service performance

Monitored target	Monitor item (unit)	Average	SLO compliance ratio	VS previous month
All Web Access	Avg. response (in ms)	988	100	-
All Web Access	Throughput (per sec)	402	100	-
All Web Access	Error rate (%)	0	100	-
Transaction1	Avg. response (in ms)	-	-	-

This example displays report data beginning on November 1, 2012. It shows that the threshold for monitoring item average response time was changed on November 19, 2012.

(3) Related topics

- *4.5.4 Verifying report data in the window*
- *4.5.5 Outputting report data*
- *10.5.7 Preview report window*

4.5.8 Notes about time zone differences from one host to another

To display reports correctly, the time zone of the host on which ITSLM - Manager is installed must match the time zone of the computer from which the monitoring person is logged in to ITSLM - Manager.

This subsection explains the totals time and data for reports when the time zones do not match.

(1) Time periods subject to monthly or daily totals

The monthly and daily totals in reports are obtained from the values aggregated for one month and for one day, respectively, based on the time zone of the host on which ITSLM - Manager is installed. For example, if the time zone at the host where ITSLM - Manager is installed is GMT + 0900 and the time zone of the computer where the monitoring person is logged in to ITSLM - Manager is GMT, the time period subject to data collection for April 1, 2012 is from 2012/04/01 00:00:00 + 0900 to 2012/04/01 23:59:59 + 0900.

(2) Date and time display in performance charts

The time displayed in a performance chart might be shifted depending on the time zone of the host on which ITSLM - Manager is installed and the time zone of the computer from which the monitoring person is logged in to ITSLM - Manager.

The following describes the cases where the time displayed in a performance chart is shifted.

- When the time of the host on which ITSLM - Manager is installed is ahead of the time of the computer from which the monitoring person is logged in to ITSLM - Manager, the time displayed in a performance chart is shifted behind by the time difference (rounded up by a day).

  For example, if the time zone of the host on which ITSLM - Manager is installed is GMT + 0900 and the time zone of the computer from which the monitoring person is logged in to ITSLM - Manager is GMT, the service performance for 2012/04/30 is displayed in a performance chart in a report as being for 2012/04/29.
- When the time of the computer from which the monitoring person is logged in to ITSLM - Manager is more than 24 hours ahead of the host on which ITSLM - Manager is installed, the time displayed in a performance chart is shifted ahead by the time difference (rounded down by a day).

  For example, if the time zone of the host on which ITSLM - Manager is installed is GMT - 1200 and the time zone of the computer from which the monitoring person is logged in to ITSLM - Manager is GMT + 1200, the service performance for 2012/04/29 is displayed in a performance chart in a report as being for 2012/04/30.

(3) Time displayed in CSV files

When reports are output to CSV files, each line displays the date the data was totaled by the host on which ITSLM - Manager is installed.

For example, if the time zone of the host on which ITSLM - Manager is installed is GMT + 0900 and the time zone of the computer from which the monitoring person is logged in to ITSLM - Manager is GMT, the time displayed in graphs in the window is shifted behind by one day but the time displayed in CSV files is not shifted; that is, the time at the host on which ITSLM - Manager is installed is displayed.

(4) Related topics

- *4.5.4 Verifying report data in the window*
- *4.5.5 Outputting report data*
- *10.5.7 Preview report window*

4.5.9 Other notes about report creation

(1) A nonexistent calendar date

A nonexistent date in a specified report interval is not displayed for the items or performance charts in reports or in CSV files. For example, if a report's start date is May 31 and the report interval is one month, the dates subject to totaling in the report interval are from May 31 through June 30, and June 31 is excluded because it does not exist in the calendar. For a comparison percentage to the previous month, the dates subject to totaling would be May 1 through May 30 (because April 31 does not exist in the calendar).

(2) Handling of data that exceeds the report retention period

ITSLM retains report data for five years. A report start date must be less than five years prior to the current system time of the computer on which the Home window is displayed (it cannot be for the exact same date five years ago or any earlier date).

If the report interval and the period for calculating comparison percentages to previous periods includes a point in time that falls before the report retention period, see the information provided in *4.5.6 Notes on when some service performance data has not been acquired*.

(3) Report output when a monitoring item name includes a comma or a double quotation mark

If the name of a monitoring item added in the **Configuration information settings** area includes a comma (`,`) or a double quotation mark (`"`), that character is replaced with an underscore (_) in CSV files.

4.6 Examples of execution of monitoring

This section provides execution examples for the following scenarios, which were described in Chapter 1 and in *3.3 Examples of setup of the monitoring items*:

- Predictive error detection in the performance of monitored services and the corrective action support methodology
- Predictive error detection in the performance of processes in monitored services and the corrective action support methodology
- Predictive error detection in the performance of systems running monitored services and the corrective action support methodology
- Periodic evaluation of the status of monitored services

4.6.1 Example of execution for predictive error detection in the performance of monitored services and the corrective action support methodology

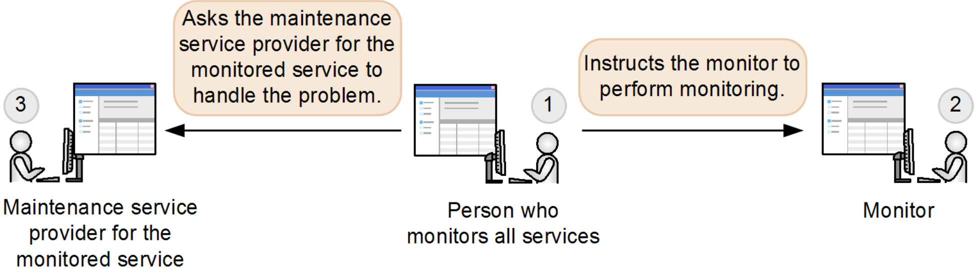
This subsection explains by way of example how to use ITSLM to execute predictive error detection in the performance of monitored services and the corrective actions to take, based on given conditions.

(1) Prerequisites

The conditions for this execution example are as follows:

- Registration of monitored services and the setup required for predictive error detection have been completed and monitoring has already started.
- The following figure shows the relationship among the personnel involved in this task.

Figure 4–3: Relationship among personnel involved in predictive error detection in the performance of monitored services and the corrective action support methodology (execution example)


Asks the maintenance service provider for the monitored service to handle the problem.
Instructs the monitor to perform monitoring.
3
1
2
Maintenance service provider for the monitored service
Person who monitors all services
Monitor

1. Person who monitors all services
   Instructs the monitor to perform monitoring. If notified of a warning sign of a service performance error, this person investigates the cause. Upon determining that further investigation is needed, this person asks the maintenance service provider for the monitored service to investigate.
2. Monitor
   Uses the Home window to monitor the monitoring items for all monitored services that have been set up by the person who monitors all services.
3. Maintenance service provider for the monitored service

If requested by the person who monitors all services, this person investigates the monitored service and takes corrective action, as necessary.

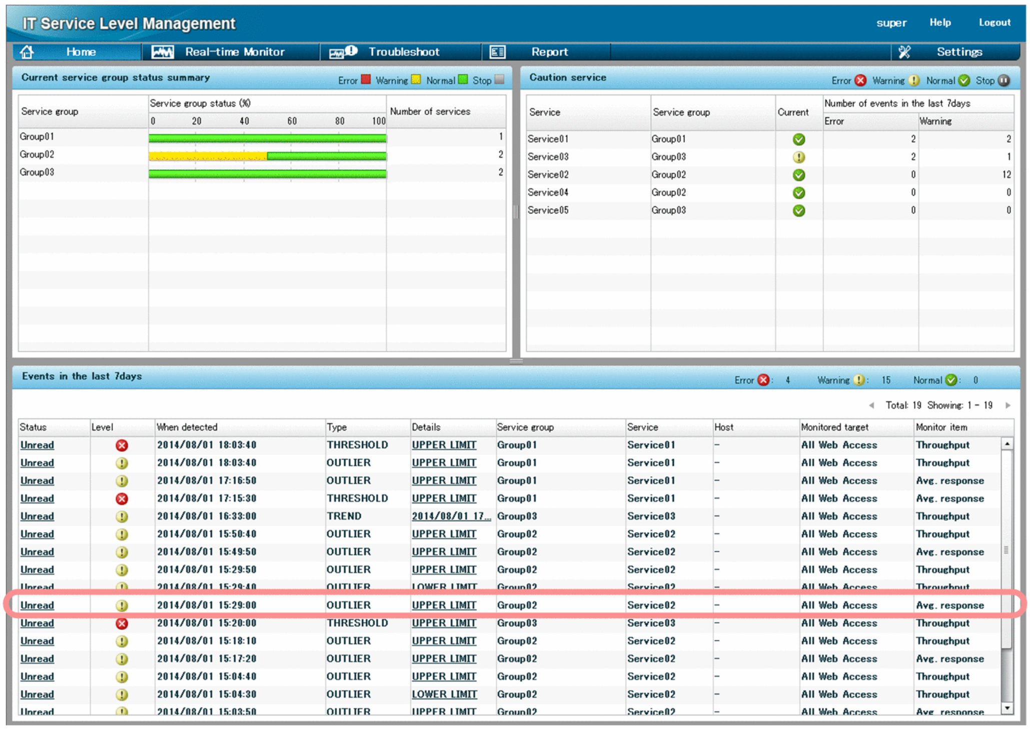
(2) Predictive error detection in the performance of a monitored service

Tasks in ITSLM

While the person who monitors all services was monitoring the status of the monitored services in the Home window, a warning constituting a warning sign of a service performance error was displayed.

The following figure shows a display example of the Home window when a warning is displayed for a monitored service.

Figure 4–4: Display example of the Home window that contains a warning for a monitored service



Current service group status summary

Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%)	Number of services
Group01	🟩	1
Group02	🟨🟩	2
Group03	🟩	2

Caution service

Error ✖ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
Service05	Group03	✓	0	0

Events in the last 7days

Error ✖: 4 Warning !: 15 Normal ✓: 0

Total: 19 Showing: 1 - 19

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	✖	2014/08/01 18:03:40	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 18:03:40	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 17:16:50	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	✖	2014/08/01 17:15:30	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2014/08/01 16:33:00	TREND	2014/08/01 17...	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	✖	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response

Details of the warning displayed in this figure are as follows:

- When detected: `2014-08-01 15:29:00`
- Type: `OUTLIER`
- Details: `UPPER LIMIT`
- Service group: `Group01`
- Service: `Service01`
- Monitored target: `All Web Access`
- Monitor item: `Avg. response`

This warning indicates that the average response time of `Service02` belonging to `Group02` that was obtained at 15:29:00 on August 1, 2014, constituted an out-of-range value (a value exceeding the upper limit) and differed significantly from the usual value for the monitored service.

Results of the task

The monitor reported the warning to the person who monitors all services.

Because the warning might lead to an error if left unattended, the person who monitors all services decided to take corrective action immediately.

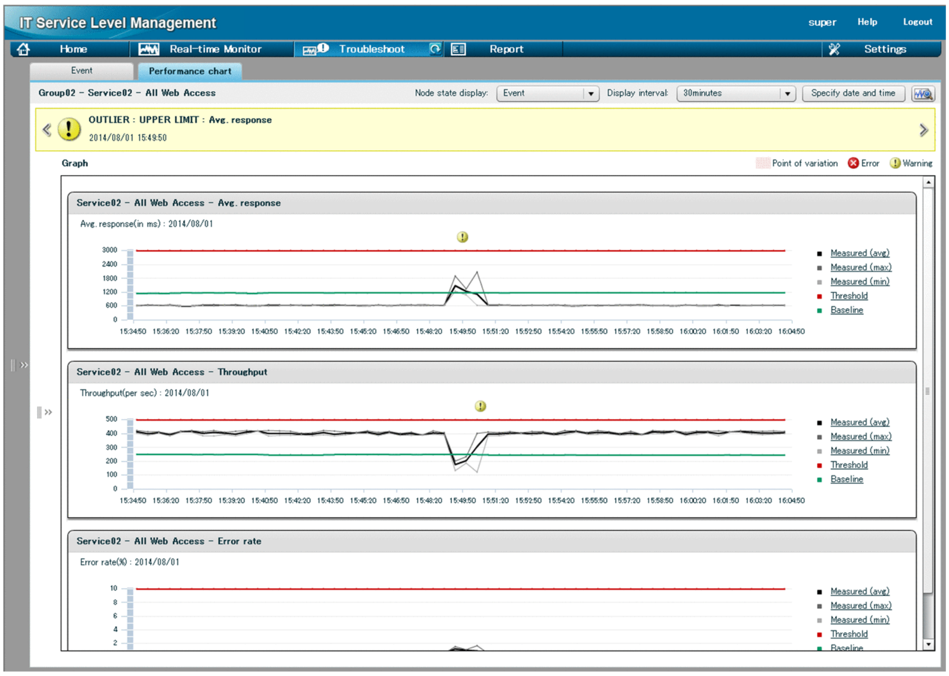
(3) Corrective action taken after a warning sign was detected in the performance of a monitored service

Tasks in ITSLM

After being notified of the warning displayed in the Home window, the person who monitors all services decided to use the Troubleshoot window to investigate the timing of the event detected as a warning, and then take corrective action.

The following figure shows a display example of the Troubleshoot window in which a warning is displayed for a monitored service.

Figure 4–5: Display example of the Troubleshoot window in which a warning is displayed for a monitored service



Group02 – Service02 – All Web Access

Node state display: Event

Display interval: 30minutes

OUTLIER : UPPER LIMIT : Avg. response
2014/08/01 15:49:50

Service02 – All Web Access – Avg. response

Avg. response(in ms) : 2014/08/01

Service02 – All Web Access – Throughput

Throughput(per sec) : 2014/08/01

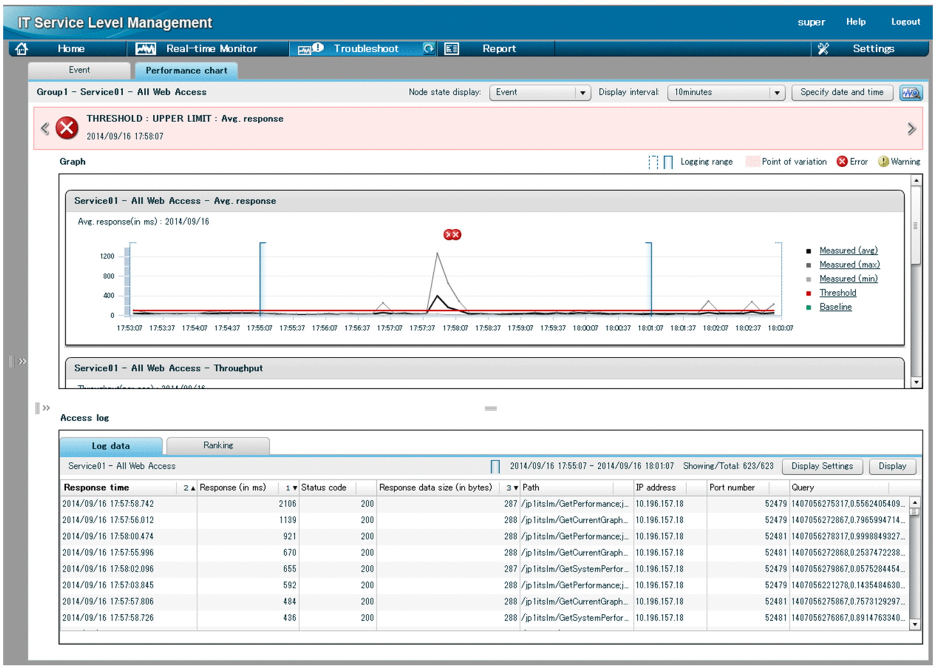
Service02 – All Web Access – Error rate

Error rate(%) : 2014/08/01

This performance chart of average response time indicates that the event causing the warning occurred between 15:48:18 and 15:51:18.

The access log for the time period during which the warning occurred include requests from the users of the Web system service and the corresponding responses. This information can be used to investigate any problems in Web system processing.

Figure 4–6: Display example of an access log in which a warning for a monitored service is displayed



Group1 - Service01 - All Web Access

Node state display: Event

Display interval: 10minutes

THRESHOLD : UPPER LIMIT : Avg. response

2014/09/16 17:58:07

Service01 - All Web Access

2014/09/16 17:55:07 - 2014/09/16 18:01:07 Showing/Total: 623/623

Response time 2 ▲	Response (in ms) 1 ▼	Status code	Response data size (in bytes) 3 ▼	Path	IP address	Port number	Query
2014/09/16 17:57:58.742	2106	200	287	/jp1itslm/GetPerformance;j...	10.196.157.18	52479	1407056275317,0.5562405409...
2014/09/16 17:57:56.012	1139	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52479	1407056272867,0.7965994714...
2014/09/16 17:58:00.474	921	200	288	/jp1itslm/GetPerformance;j...	10.196.157.18	52481	1407056278317,0.9998849327...
2014/09/16 17:57:55.996	670	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52481	1407056272868,0.2537472238...
2014/09/16 17:58:02.096	655	200	287	/jp1itslm/GetSystemPerfor...	10.196.157.18	52479	1407056279867,0.0575284454...
2014/09/16 17:57:03.845	592	200	288	/jp1itslm/GetPerformance;j...	10.196.157.18	52479	1407056221278,0.1435484630...
2014/09/16 17:57:57.806	484	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52481	1407056275867,0.7573129297...
2014/09/16 17:57:58.726	436	200	288	/jp1itslm/GetSystemPerfor...	10.196.157.18	52481	1407056276867,0.8914763340...

Results of tasks

Because the details of the warning and the timing of the event causing the warning became clear from the data provided in the Troubleshoot window, the person who monitors all services notified the maintenance service provider for the monitored service and requested a root cause investigation and corrective action.

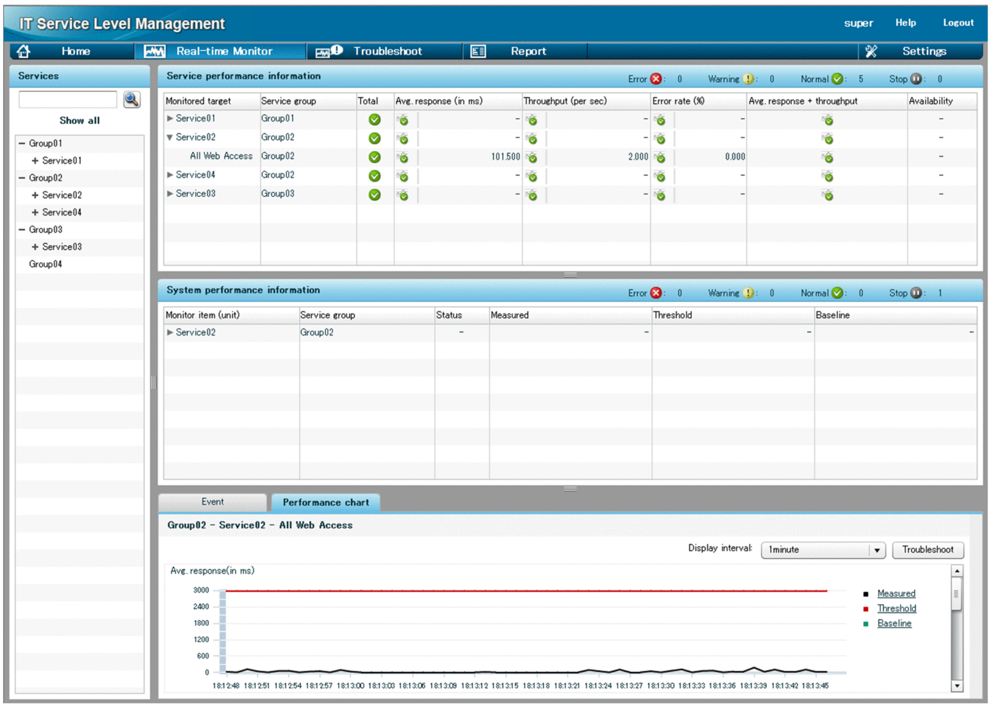
(4) Verifying the service performance after taking corrective action

Tasks in ITSLM

After corrective action was taken by the maintenance service provider for the monitored service based on the results of a root cause investigation, the person who monitors all services decided to use the Real-time Monitor window to verify that service performance had returned to normal.

The following figure shows a display example of the Real-time Monitor window showing that service performance has returned to normal after corrective action was taken.

Figure 4–7: Display example of the Real-time Monitor window showing that service performance has returned to normal



Service performance information

Error: 0 Warning: 0 Normal: 5 Stop: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▶ Service01	Group01	✓	✓ -	✓ -	✓ -	✓	-
▼ Service02	Group02	✓	✓ -	✓ -	✓ -	✓	-
All Web Access	Group02	✓	✓ 101.500	✓ 2.000	✓ 0.000	✓	-
▶ Service04	Group02	✓	✓ -	✓ -	✓ -	✓	-
▶ Service03	Group03	✓	✓ -	✓ -	✓ -	✓	-

System performance information

Error: 0 Warning: 0 Normal: 0 Stop: 1

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▶ Service02	Group02	-	-	-	-

Group02 - Service02 - All Web Access

Display interval: 1minute

As shown in this figure, when service performance has returned to normal, the ✓ (normal) icon is displayed in the **Service performance information** area.

Results of tasks

The person who monitors all services has verified that service performance has returned to normal. This concludes the handling of the warning sign of a service performance error in a monitored service.

4.6.2 Example of execution for predictive error detection in the performance of processes in monitored services and the corrective action support methodology

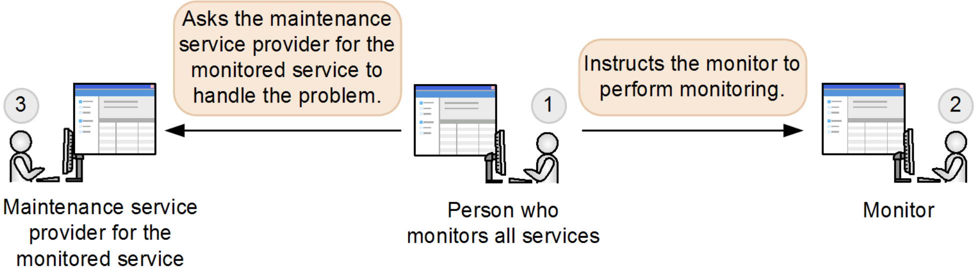
This subsection explains by way of example how to use ITSLM to execute predictive error detection in the performance of processes in monitored services and the corrective actions to take, based on given conditions.

(1) Prerequisites

The conditions for this execution example are as follows:

- Registration of monitored services and Web transactions and the setup required for predictive error detection have been completed and monitoring has already started.
- The following figure shows the relationship among personnel involved in this task.

Figure 4–8: Relationship among personnel involved in predictive error detection in the performance of processes in monitored services and the corrective action support methodology (execution example)


Asks the maintenance service provider for the monitored service to handle the problem.
Instructs the monitor to perform monitoring.
3
1
2
Maintenance service provider for the monitored service
Person who monitors all services
Monitor

1. Person who monitors all services

   Instructs the monitor to perform monitoring. If notified of a warning sign of a service performance error, this person investigates the cause. Upon determining that further investigation is needed, this person asks the maintenance service provider for the monitored service to investigate.

2. Monitor

   Uses the Home window to monitor the status of the monitored services of all service groups and the status of the processes of each monitored service.

3. Maintenance service provider for the monitored service

   If requested by the person who monitors all services, this person investigates the monitored service and takes correction action, as necessary.

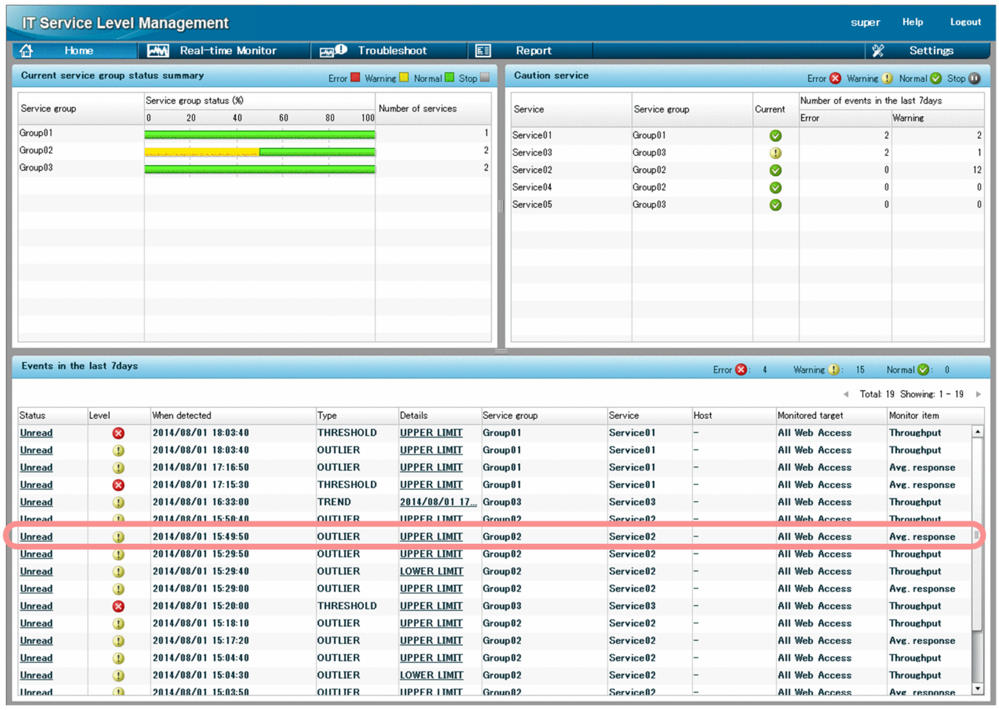
(2) Predictive error detection in the performance of a process in a monitored service

Tasks in ITSLM

While the person who monitors all services was monitoring the status of the monitored services and the status of the processes of the monitored services in the Home window, a warning sign of a service performance error was displayed for a Web transaction corresponding to a process.

The following figure shows a display example of the Home window when a warning is displayed for a Web transaction of a monitored service.

Figure 4–9: Display example of the Home window that contains a warning for a Web transaction of a monitored service



Current service group status summary — Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%) 0 20 40 60 80 100	Number of services
Group01	🟩	1
Group02	🟨🟩	2
Group03	🟩	2

Caution service — Error ✖ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
Service05	Group03	✓	0	0

Events in the last 7days — Error ✖: 4 Warning !: 15 Normal ✓: 0

Total: 19 Showing: 1 - 19

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	✖	2014/08/01 18:03:40	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 18:03:40	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 17:16:50	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	✖	2014/08/01 17:15:30	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2014/08/01 16:33:00	TREND	2014/08/01 17...	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	✖	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response

Details of the warning displayed in this figure are as follows:

- When detected: `2014-08-01 15:49:50`
- Type: `OUTLIER`
- Details: `UPPER LIMIT`
- Service group: `Group02`
- Service: `Service02`
- Monitored target: `All Web Access`
- Monitor item: `Avg. response`

This warning indicates that the average response time of `All Web Access` of `Service02` belonging to `Group02` that was obtained at 15:49:50 on August 1, 2014, constituted an out-of-range value (a value exceeding the upper limit) and differed significantly from the usual value for the monitored service.

Results of the task

The monitor reported the warning to the person who monitors all services.

Because the warning might lead to an error if left unattended, the person who monitors all services decided to take corrective action immediately.

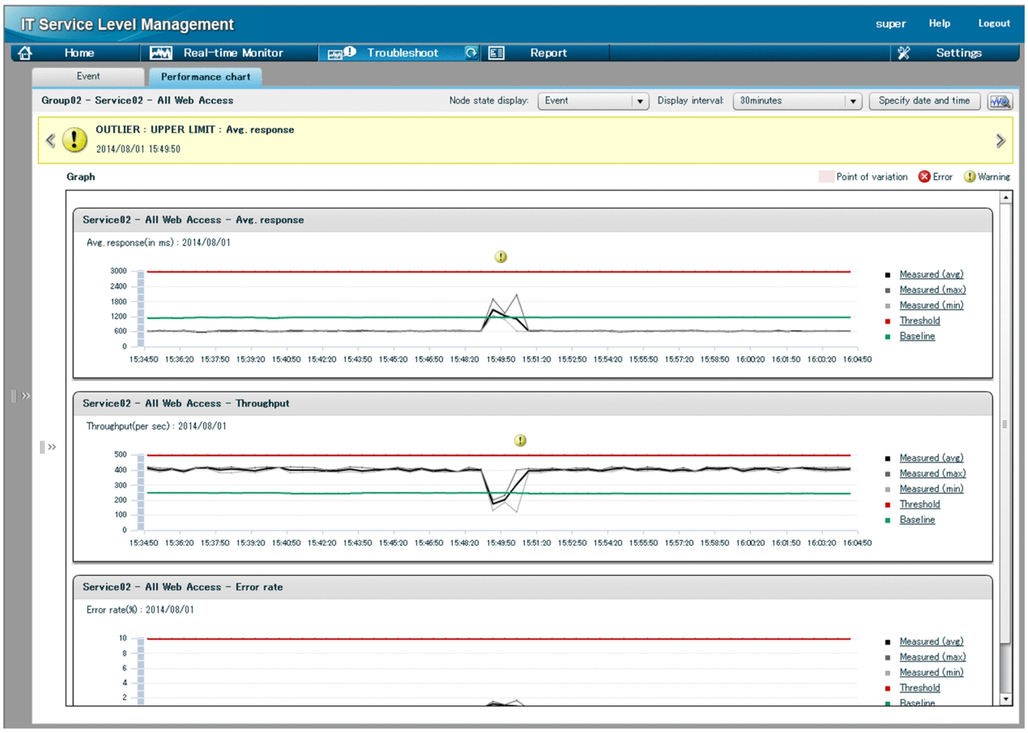
(3) Corrective action taken after a warning sign was detected in the service performance for a process of a monitored service

Tasks in ITSLM

After being notified of the warning displayed in the Home window, the person who monitors all services decided to use the Troubleshoot window to investigate the timing of the event detected as a warning, and then take corrective action.

The following figure shows a display example of the Troubleshoot window in which a warning is displayed for a Web transaction of a monitored service.

Figure 4–10: Display example of the Troubleshoot window in which a warning is displayed for a Web transaction of a monitored service



Group02 - Service02 - All Web Access

Node state display: Event

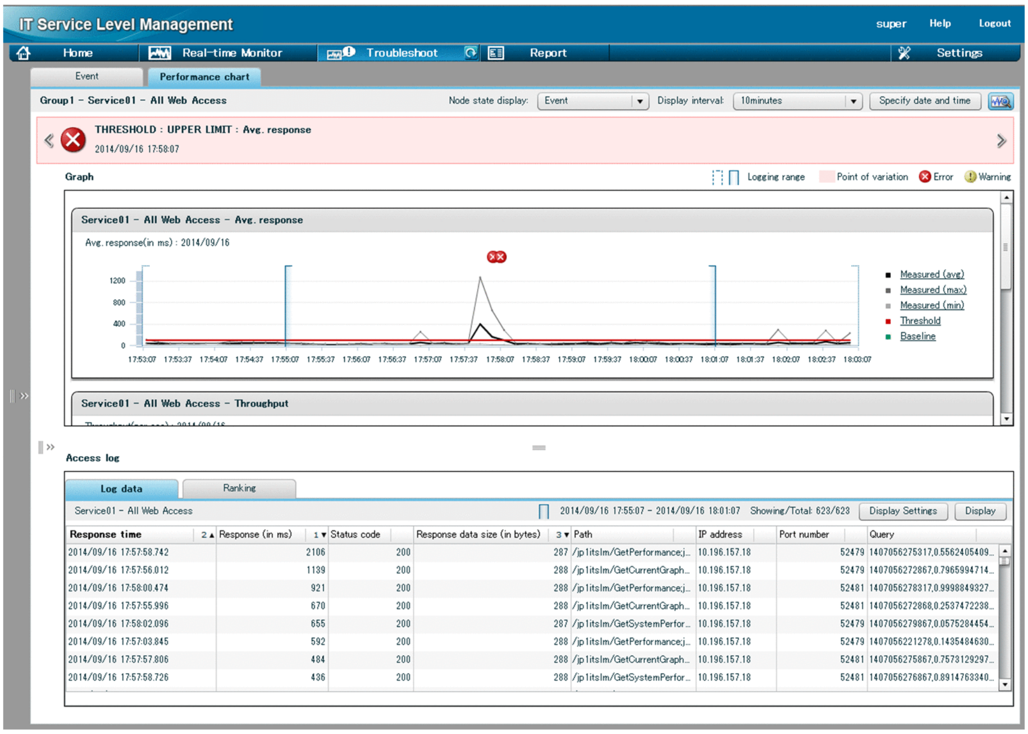
Display interval: 30minutes

OUTLIER : UPPER LIMIT : Avg. response
2014/08/01 15:49:50

This performance chart of average response time indicates that the event causing the warning occurred between 15:48:18 and 15:51:18.

The access log for the time period during which the warning appeared include the Web transactions of the monitored service. This information can be used to investigate any problems in Web system processing.

Figure 4–11: Display example of the access log in which a warning for a monitored service is displayed



Group1 – Service01 – All Web Access   Node state display: Event   Display interval: 10minutes   Specify date and time

THRESHOLD : UPPER LIMIT : Avg. response
2014/09/16 17:58:07

Service01 – All Web Access   2014/09/16 17:55:07 – 2014/09/16 18:01:07   Showing/Total: 623/623

Response time	2 ▲ Response (in ms)	1 ▼ Status code	Response data size (in bytes)	3 ▼ Path	IP address	Port number	Query
2014/09/16 17:57:58.742	2106	200	287	/jp1itslm/GetPerformance;j...	10.196.157.18	52479	1407056275317,0.5562405409...
2014/09/16 17:57:56.012	1139	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52479	1407056272867,0.7965994714...
2014/09/16 17:58:00.474	921	200	288	/jp1itslm/GetPerformance;j...	10.196.157.18	52481	1407056278317,0.9998849327...
2014/09/16 17:57:55.996	670	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52481	1407056272868,0.2537472238...
2014/09/16 17:58:02.096	655	200	287	/jp1itslm/GetSystemPerfor...	10.196.157.18	52479	1407056279867,0.0575284454...
2014/09/16 17:57:03.845	592	200	288	/jp1itslm/GetPerformance;j...	10.196.157.18	52479	1407056221278,0.1435484630...
2014/09/16 17:57:57.806	484	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52481	1407056275867,0.7573129297...
2014/09/16 17:57:58.726	436	200	288	/jp1itslm/GetSystemPerfor...	10.196.157.18	52481	1407056276867,0.8914763340...

Results of tasks

Because the details of the warning and the timing of the event causing the warning became clear from the data provided in the Troubleshoot window, the person who monitors all services notified the maintenance service provider for the monitored service and requested a root cause investigation and corrective action.

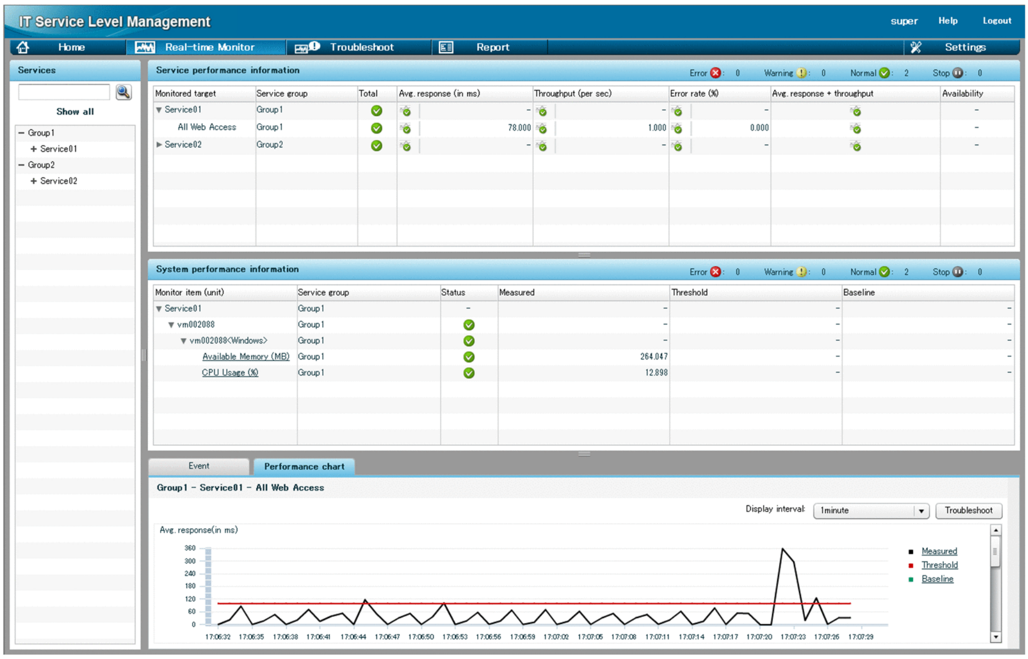
(4) Verifying the service performance after taking corrective action

Tasks in ITSLM

After corrective action was taken by the maintenance service provider for the monitored service based on the results of a root cause investigation, the person who monitors all services decided to use the Real-time Monitor window to verify that the service performance of the Web transaction had returned to normal.

The following figure shows a display example of the Real-time Monitor window showing that the service performance of the Web transaction has returned to normal after corrective action was taken.

Figure 4–12: Display example of the Real-time Monitor window showing that service performance of the Web transaction has returned to normal



Service performance information — Error: 0 Warning: 0 Normal: 2 Stop: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service01	Group1	✓	✓ -	✓ -	✓ -	✓	-
All Web Access	Group1	✓	✓ 78.000	✓ 1.000	✓ 0.000	✓	-
▶ Service02	Group2	✓	✓ -	✓ -	✓ -	✓	-

System performance information — Error: 0 Warning: 0 Normal: 2 Stop: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service01	Group1	-	-	-	-
▼ vm002088	Group1	✓	-	-	-
▼ vm002088<Windows>	Group1	✓	-	-	-
Available Memory (MB)	Group1	✓	264.047	-	-
CPU Usage (%)	Group1	✓	12.898	-	-

Group1 − Service01 − All Web Access

As shown in this figure, when service performance of the Web transaction has returned to normal, the ✓ (normal) icon is displayed in the **Service performance information** area.

Results of tasks

The person who monitors all services has verified that service performance of the Web transaction has returned to normal. This concludes the handling of the warning sign of a service performance error for a process of a monitored service.

4.6.3 Example of execution for predictive error detection in the performance of systems running monitored services and the corrective action support methodology (working with Performance Management)

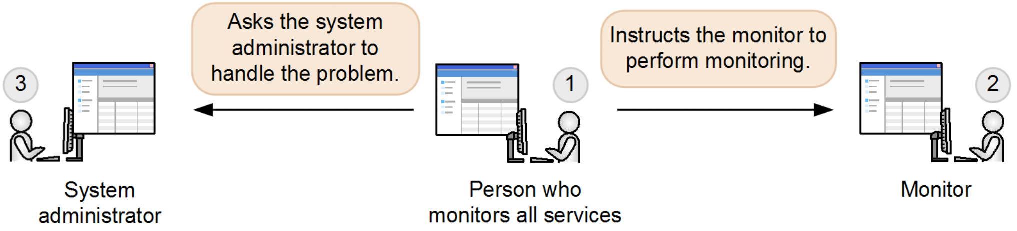
This subsection explains by way of example how to use ITSLM to execute predictive error detection in the performance of systems running monitored services and the corrective actions to take (when working with Performance Management), based on given conditions.

(1) Prerequisites

The conditions for this execution example are as follows:

- Registration of monitored services and the setup required for predictive error detection have been completed and monitoring has already started.
- The following figure shows the relationship among personnel involved in this task.

Figure 4–13: Relationship among personnel involved in predictive error detection in the performance of systems running monitored services and the corrective action support methodology (execution example)


Asks the system administrator to handle the problem.
Instructs the monitor to perform monitoring.
3
1
2
System administrator
Person who monitors all services
Monitor

1. Person who monitors all services

   Instructs the monitor to perform monitoring. If notified of a warning sign of a system performance error, this person investigates the cause. Upon determining that further investigation is needed, this person asks the system administrator to investigate.

2. Monitor

   Uses the Home window to monitor the monitoring items for all monitored services that have been set up by the person who monitors all services. In the event of a warning or error, this person reports it immediately to the person who monitors all services.

3. System administrator

   If requested by the person who monitors all services, this person investigates the status of the system that is providing the monitored service, such as a host or middleware, and takes corrective action.

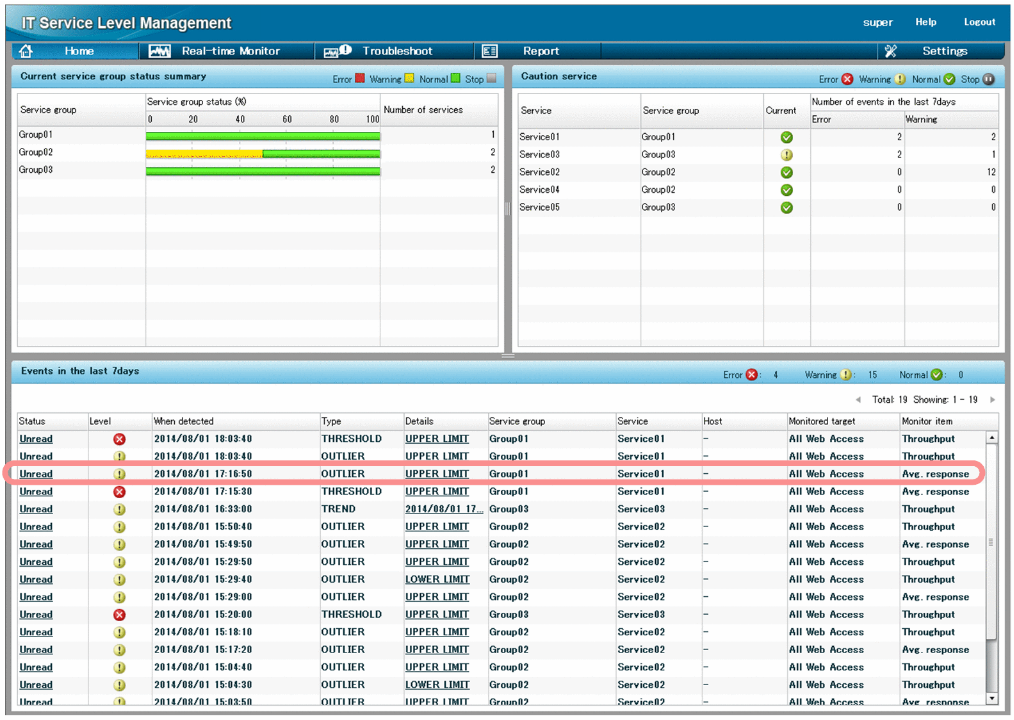
(2) Predictive error detection in the performance of a monitored service

Tasks in ITSLM

While the monitor was monitoring the status of monitored services in the Home window, a warning constituting a warning sign of a service performance error was displayed.

The following figure shows a display example of the Home window when a warning is displayed for a monitored service.

Figure 4–14: Display example of the Home window that contains a warning for a monitored service



Current service group status summary

Error 🟥 Warning 🟨 Normal 🟩 Stop ▨

Service group	Service group status (%) 0 20 40 60 80 100	Number of services
Group01		1
Group02		2
Group03		2

Caution service

Error ✕ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service01	Group01	✓	2	2
Service03	Group03	!	2	1
Service02	Group02	✓	0	12
Service04	Group02	✓	0	0
Service05	Group03	✓	0	0

Events in the last 7days

Error ✕: 4 Warning !: 15 Normal ✓: 0

◂ Total: 19 Showing: 1 - 19 ▸

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	✕	2014/08/01 18:03:40	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 18:03:40	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2014/08/01 17:16:50	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	✕	2014/08/01 17:15:30	THRESHOLD	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2014/08/01 16:33:00	TREND	2014/08/01 17...	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:50:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:49:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:29:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:40	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:29:00	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	✕	2014/08/01 15:20:00	THRESHOLD	UPPER LIMIT	Group03	Service03	–	All Web Access	Throughput
Unread	!	2014/08/01 15:18:10	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:17:20	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response
Unread	!	2014/08/01 15:04:40	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:04:30	OUTLIER	LOWER LIMIT	Group02	Service02	–	All Web Access	Throughput
Unread	!	2014/08/01 15:03:50	OUTLIER	UPPER LIMIT	Group02	Service02	–	All Web Access	Avg. response

Details of the warning displayed in this figure are as follows:

- When detected: `2014-08-01 17:16:50`
- Type: `OUTLIER`
- Details: `UPPER LIMIT`
- Service group: `Group01`
- Service: `Service01`
- Monitored target: `All Web Access`
- Monitor item: `Avg. response`

This warning indicates that the average response time of `Service01` belonging to `Group01` that was obtained at 17:16:50 on August 1, 2014, constituted an out-of-range value (a value exceeding the upper limit) and differed significantly from the usual value for the monitored service.

This example indicates that an abnormality was also detected on the monitored host.

Results of the task

The monitor reported the warning to the person who monitors all services.

Because the warning might lead to an error if left unattended, the person who monitors all services decided to take corrective action immediately.

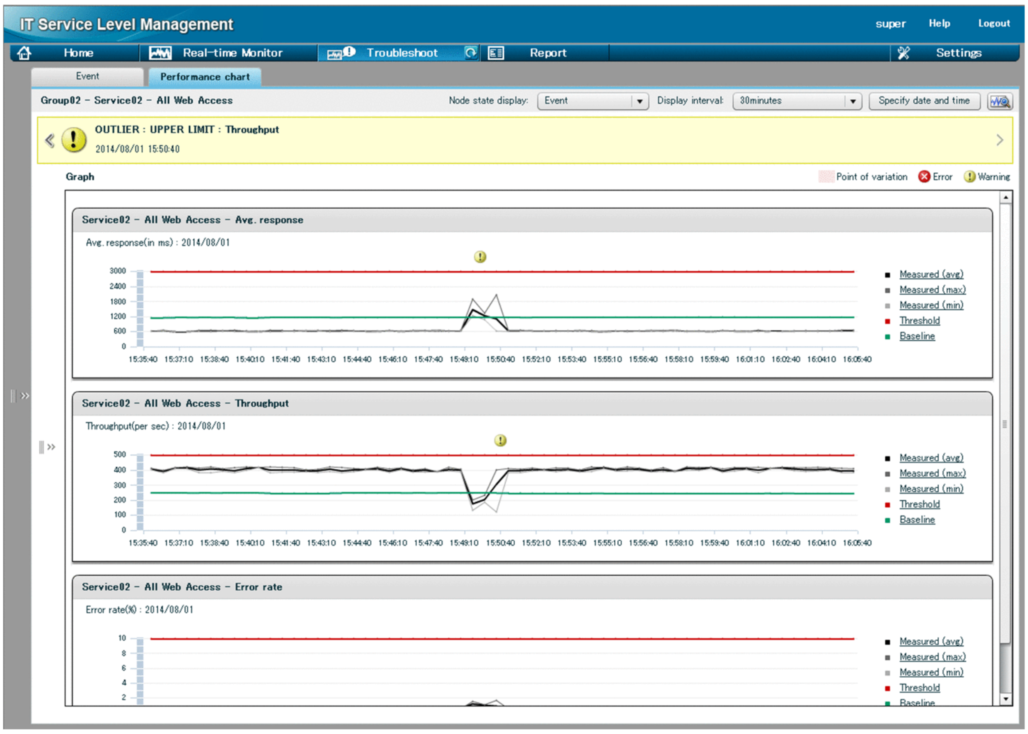
(3) Corrective action taken after a warning sign was detected in the performance of a monitored service

Tasks in ITSLM

After being notified of the warning displayed in the Home window, the person who monitors all services decided to use the Troubleshoot window to investigate the timing of the event detected as warning, and then take corrective action.

The following figure shows a display example of the Troubleshoot window in which a warning is displayed for a monitored service.

Figure 4–15: Display example of the Troubleshoot window in which a warning is displayed for a monitored service


Group02 - Service02 - All Web Access

Node state display: Event

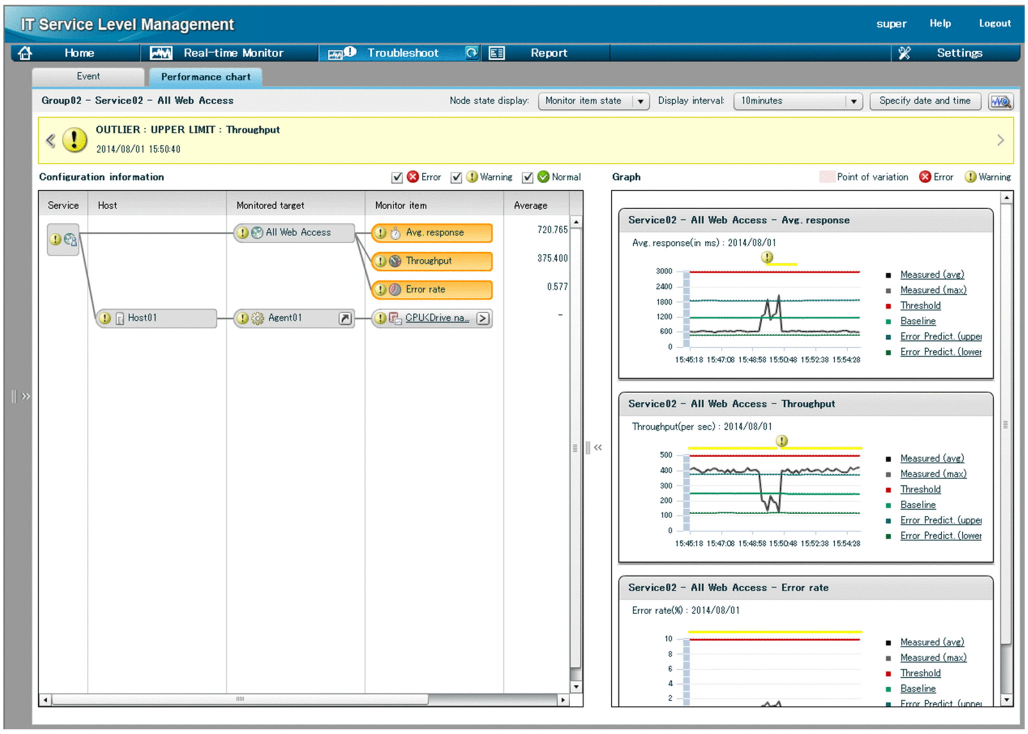
Display interval: 30minutes

OUTLIER : UPPER LIMIT : Throughput
2014/08/01 15:50:40

This performance chart of average response time indicates that the event causing the warning occurred between 15:49:10 and 15:51:10.

The person who monitors all services decided to display configuration information to check system performance. The following figure shows a display example of the Troubleshoot window that displays the configuration information.

Figure 4–16: Display example of Troubleshoot window displaying the configuration information



Group02 - Service02 - All Web Access

Node state display: Monitor item state

Display interval: 10minutes

OUTLIER : UPPER LIMIT : Throughput
2014/08/01 15:50:40

Service	Host	Monitored target	Monitor item	Average
		All Web Access	Avg. response	720.765
			Throughput	375.400
			Error rate	0.577
	Host01	Agent01	CPU<Drive na...	-

In this example, a warning occurred concerning the CPU of `Agent01`. This indicates that some problem occurred in the computer that is providing the monitored service.

Results of tasks

The details of the warning and the timing of the event causing the warning, which became clear from the data provided in the Troubleshoot window, indicate that this is most likely a system performance problem. Therefore, the person who monitors all services contacted the system administrator and requested a root cause investigation and corrective action.

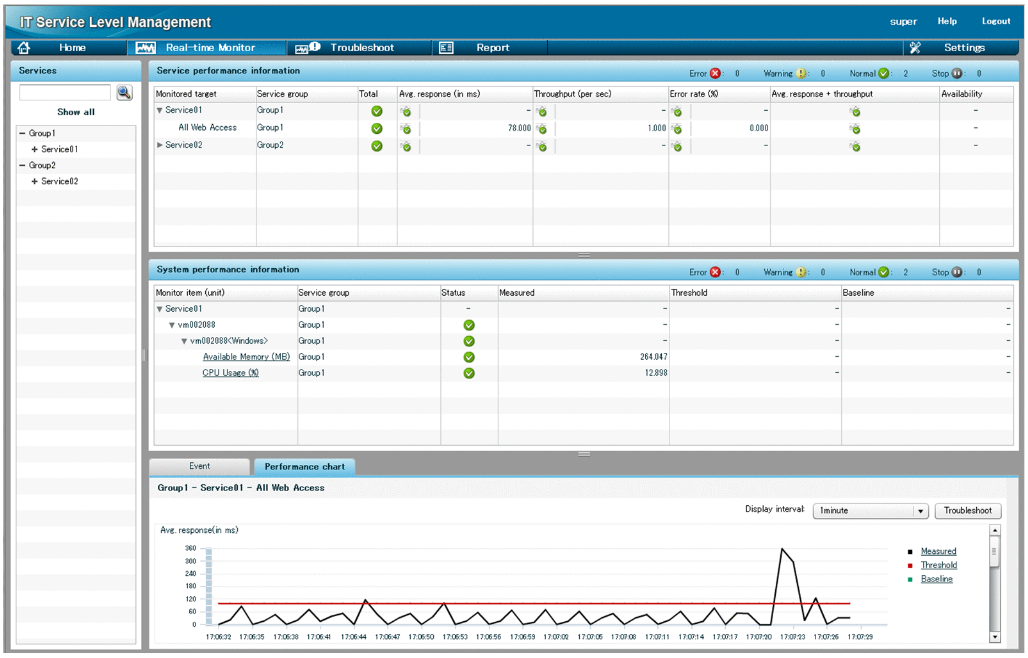
(4) Verifying the system performance after taking corrective action

Tasks in ITSLM

After corrective action was taken by the system administrator based on the results of the root cause investigation, the person who monitors all services decided to use the Real-time Monitor window to verify that system performance has returned to normal.

The following figure shows a display example of the Real-time Monitor window showing that the system performance has returned to normal after corrective action was taken.

Figure 4–17: Display example of the Real-time Monitor window showing that system performance has returned to normal



Service performance information

Error ✕: 0 Warning !: 0 Normal ✓: 2 Stop ⏸: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service01	Group1	✓	✓ -	✓ -	✓ -	✓	-
All Web Access	Group1	✓	✓ 78.000	✓ 1.000	✓ 0.000	✓	-
▶ Service02	Group2	✓	✓ -	✓ -	✓ -	✓	-

System performance information

Error ✕: 0 Warning !: 0 Normal ✓: 2 Stop ⏸: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service01	Group1	-	-	-	-
▼ vm002088	Group1	✓	-	-	-
▼ vm002088<Windows>	Group1	✓	-	-	-
Available Memory (MB)	Group1	✓	264.047	-	-
CPU Usage (%)	Group1	✓	12.898	-	-

Group1 − Service01 − All Web Access

As shown in this figure, when system performance has returned to normal, the ✓ (normal) icon is displayed in the **System performance information** area.

Results of tasks

The person who monitors all services has verified that service performance and system performance have returned to normal. This concludes the handling of the warning sign of an error in a monitored service.

4.6.4 Example of execution for periodic evaluation of the status of monitored services

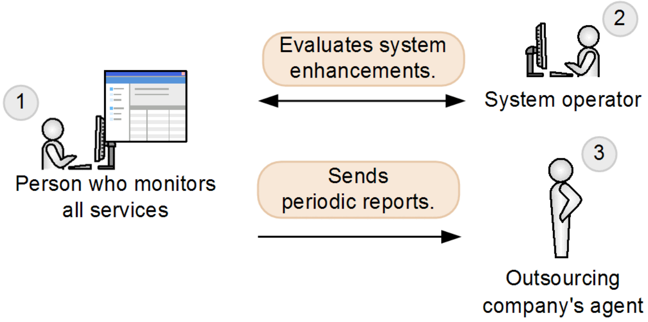
This subsection explains by way of example how to use ITSLM to execute periodic evaluation of the status of monitored services, based on given conditions.

(1) Prerequisites

The conditions for this execution example are as follows:

- Registration of monitored services and the setup required for monitoring have been completed and a specified period of time has elapsed since monitoring started.
- The following figure shows the relationship among the personnel involved in this task.

Figure 4–18: Relationship among personnel involved in periodic evaluation of the status of monitored services (execution example)


1
Person who monitors all services
Evaluates system enhancements.
Sends periodic reports.
2
System operator
3
Outsourcing company's agent

1. Person who monitors all services

   Evaluates the status of the monitored services periodically and evaluates with the system operator whether current system performance (such as server memory and CPU) is adequate to maintain the service level. This person also creates monthly reports on service levels and reports periodically to the outsourcing company's (service provider's) agent. This person might use these reports to suggest system enhancements when appropriate.

2. System operator

   Runs the system, including IT equipment and networks in the company. When system enhancements are suggested by the person who monitors all services, this person evaluates them.

3. Outsourcing company's agent

   This person is in charge of providing the outsourced services. This person receives periodic reports from the person who monitors all services at the outsourced contractor. If requested during periodic reporting, this person evaluates suggestions for system enhancements and authorizes them if determined to be appropriate.

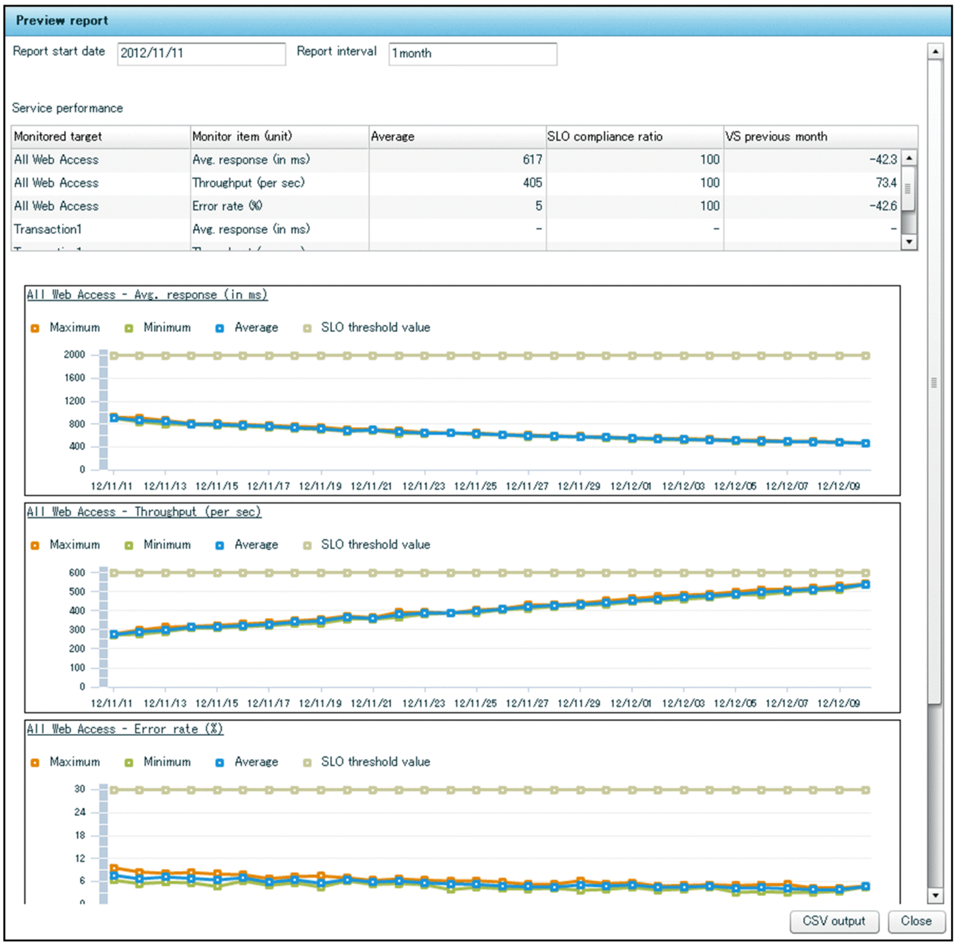
(2) Checking the status of the monitored services

Tasks in ITSLM

The person who monitors all services decided to display the Preview report window to check the status of currently monitored services for the past month. This person displayed the report using a template in which report items have already been set up.

The following figure shows a display example of the Preview report window that contains the status of a monitored service for the past month.

Figure 4–19: Display example of the Preview report window that contains the status of a monitored service for the past month



Preview report

Report start date: 2012/11/11

Report interval: 1month

Service performance

Monitored target	Monitor item (unit)	Average	SLO compliance ratio	VS previous month
All Web Access	Avg. response (in ms)	617	100	-42.3
All Web Access	Throughput (per sec)	405	100	73.4
All Web Access	Error rate (%)	5	100	-42.6
Transaction1	Avg. response (in ms)	-	-	-

This window shows for the one-month period starting November 11, 2012, the average value, SLO compliance rate, comparison to the previous month for average response time (as a percentage), throughput, and error rate. The graphs show the one-month trend in changes in service performance.

Results of the task

While reviewing data in the Preview report window, the person who monitors all services noticed upward trends in the maximum and average values for each of the monitoring items. Because these trends might lead to overage of the SLO threshold if left unattended, this person decided to contact the system administrator to evaluate whether system enhancement is needed and then, if appropriate, to suggest system enhancements to the outsourcing company's agent at the time of the next periodic reporting.

(3) Periodic report of the status of the monitored services

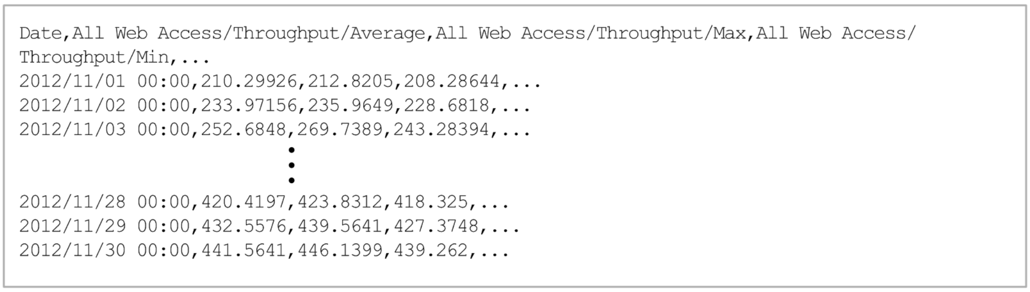
Tasks in ITSLM

Because the time for a periodic report has approached, the person who monitors all services decided to create a report to the outsourcing company's agent.

To create the report, this person decided to output from the Preview report window to a CSV file the results of monitoring the status of the monitored services.

The following figure shows the results of monitoring the status of the monitored services that have been output to a CSV file.

Figure 4–20: Results of monitoring the status of monitored services that have been output to a CSV file



```
Date,All Web Access/Throughput/Average,All Web Access/Throughput/Max,All Web Access/
Throughput/Min,...
2012/11/01 00:00,210.29926,212.8205,208.28644,...
2012/11/02 00:00,233.97156,235.9649,228.6818,...
2012/11/03 00:00,252.6848,269.7389,243.28394,...
                          ⋮
2012/11/28 00:00,420.4197,423.8312,418.325,...
2012/11/29 00:00,432.5576,439.5641,427.3748,...
2012/11/30 00:00,441.5641,446.1399,439.262,...
```

The service performance average, maximum, and minimum values and their times are output to the CSV file.

Results of tasks

A graph was created from the results of monitoring the status of the monitored services that was output to a CSV file by using a spreadsheet program, and the graph was included in the report.

The person who monitors all services explained in the periodic report that based on the graph, some system enhancement is needed in order to maintain the service level. Approval for the proposed enhancements was obtained from the outsourcing company's agent.

5 Preparations Before Starting

This chapter explains the preparations before starting ITSLM, including installation, setup, and user settings.

This chapter also explains optional preparations, such as linking with JP1/IM to report monitoring results by means such as email, linking with Performance Management to monitor hosts and middleware that provide the services, and editing system definition files (`jp1itslm.properties` or `jp1itslmur.properties`) to change ITSLM operations.

For details about the preparations before you start running ITSLM in a cluster system, see *6. Preparations Before Starting (Cluster System)*.

5.1 Deploying ITSLM

To deploy ITSLM, you must install ITSLM, create an execution environment by setting it up, and then install the HTML manual in the execution environment.

When you upgrade ITSLM or link ITSLM with Performance Management, you must pay attention to the sequence of tasks.

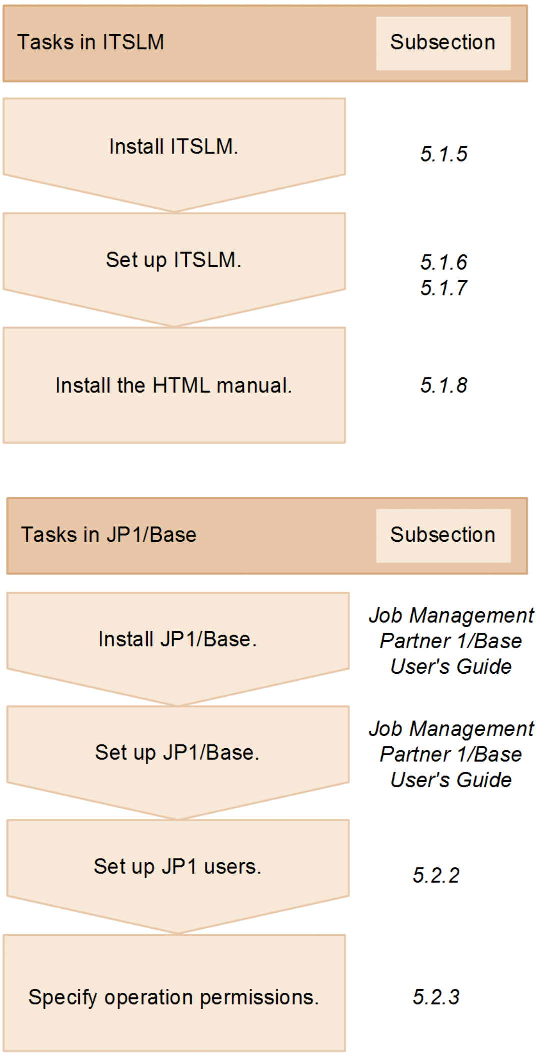
This section explains four different procedures for deploying ITSLM:

- Deploying a new ITSLM
- Upgrading ITSLM
- Deploying a new ITSLM (when linking with a newly deployed Performance Management)
- Deploying a new ITSLM (when linking with an existing Performance Management)

5.1.1 General procedure for deploying a new ITSLM

The figure below shows the general procedure for a new deployment of ITSLM. This procedure includes tasks performed in JP1/Base as well as the tasks performed in ITSLM. You can perform the tasks in JP1/Base before or after the tasks in ITSLM.

Figure 5–1: General procedure for deploying ITSLM



5.1.2 General procedure for upgrading ITSLM

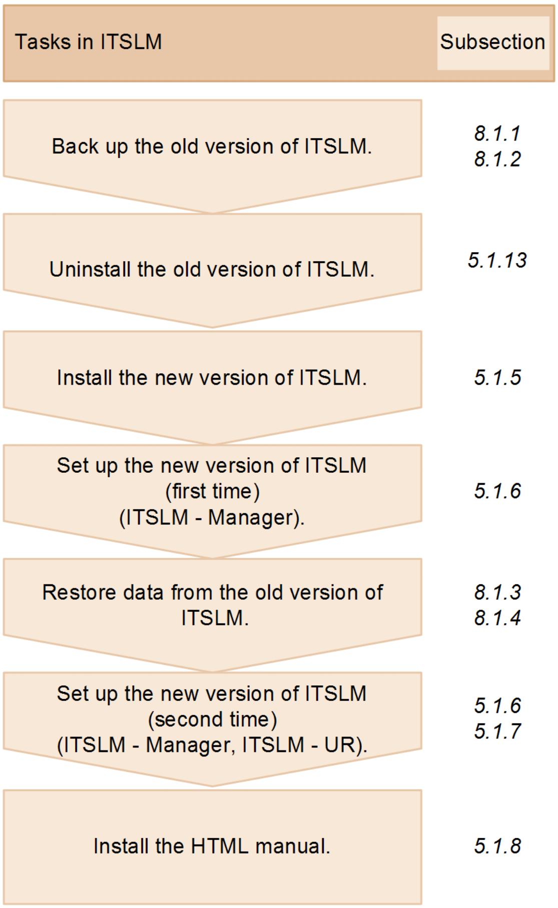
This subsection explains the general procedure for upgrading an ITSLM that has already been deployed. During upgrading, there is no need to redo the JP1/Base tasks that were performed when ITSLM was deployed initially.

The procedure for upgrading from 09-50 differs from the procedure for upgrading from 09-51 or later. In addition, when ITSLM - Manager is upgraded from 09-51 or later, the upgrade procedure differs depending on whether the capacity of the database that will be used after upgrading will be greater than the capacity before upgrading.

(1) Upgrading ITSLM - Manager and ITSLM - UR version 09-50

The figure below shows the general procedure for upgrading ITSLM - Manager and ITSLM - UR version 09-50.

Figure 5‒2: General procedure for upgrading ITSLM that has already been deployed (upgrading from 09-50)


Tasks in ITSLM
Subsection
Back up the old version of ITSLM.
8.1.1
8.1.2
Uninstall the old version of ITSLM.
5.1.13
Install the new version of ITSLM.
5.1.5
Set up the new version of ITSLM (first time) (ITSLM - Manager).
5.1.6
Restore data from the old version of ITSLM.
8.1.3
8.1.4
Set up the new version of ITSLM (second time) (ITSLM - Manager, ITSLM - UR).
5.1.6
5.1.7
Install the HTML manual.
5.1.8

When you back up data from the old version of ITSLM, see *8.1.1 Backing up the definition files* and *8.1.2 Backing up the database*.

When you restore data from the old version of ITSLM, see *8.1.4 Restoring the definition files* and *8.1.5 Restoring the database*.

When you upgrade a version of ITSLM that has already been deployed, you must set up ITSLM - Manager twice, as described in the procedure. The first setup prepares for restore processing, and the second setup migrates the database. You perform the second setup using the same command line arguments and options file contents as were used for the first setup.

After you have finished upgrading ITSLM, verify that the displays in the following windows are the same as they were before upgrading:

- Home window
- Troubleshoot window
- Report window
- Settings window

If the displays in these windows differ from before upgrading, you must apply the following procedure to redo the installation, and then perform setup:

1. Uninstall ITSLM

2. Install the old version of ITSLM.

3. Restore the backup data obtained before upgrading.

4. Re-install the new version of ITSLM.

(2) Upgrading ITSLM - Manager version 09-51 or later

When ITSLM - Manager 09-51 or later is upgraded, the upgrade procedure differs depending on whether the capacity of the database that will be used after upgrading will be greater than the capacity before upgrading. For this reason, before you start the procedure, estimate the database capacity that will be needed after upgrading. For details, see the description of how to estimate the size of the database area in *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

Compare the estimated value and the value shown in the table below to determine whether the capacity of the database that will be used after the upgrade will be greater than the capacity of the database before upgrading.

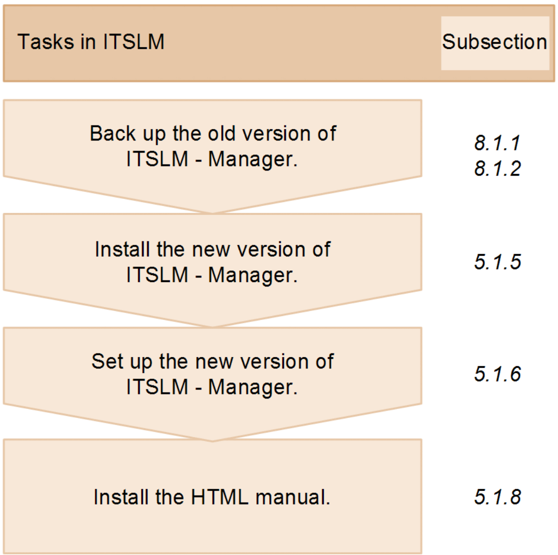
Table 5–1: Database capacity before upgrading

No.	ITSLM - Manager version before upgrading	Database capacity before upgrading
1	09-51	39,000 MB
2		5,000 MB#
3	10-00 or later	Value of the `hdb_area_size` definition item in the `jslmmgrsetup` command's options file that was specified when ITSLM - Manager was newly set up.

#: This is the value used at the time of setup of ITSLM - Manager 09-51 when the number of monitored services was about 10 and `pdi_small_s.ini` was set to the default value `pdi_s.ini`.

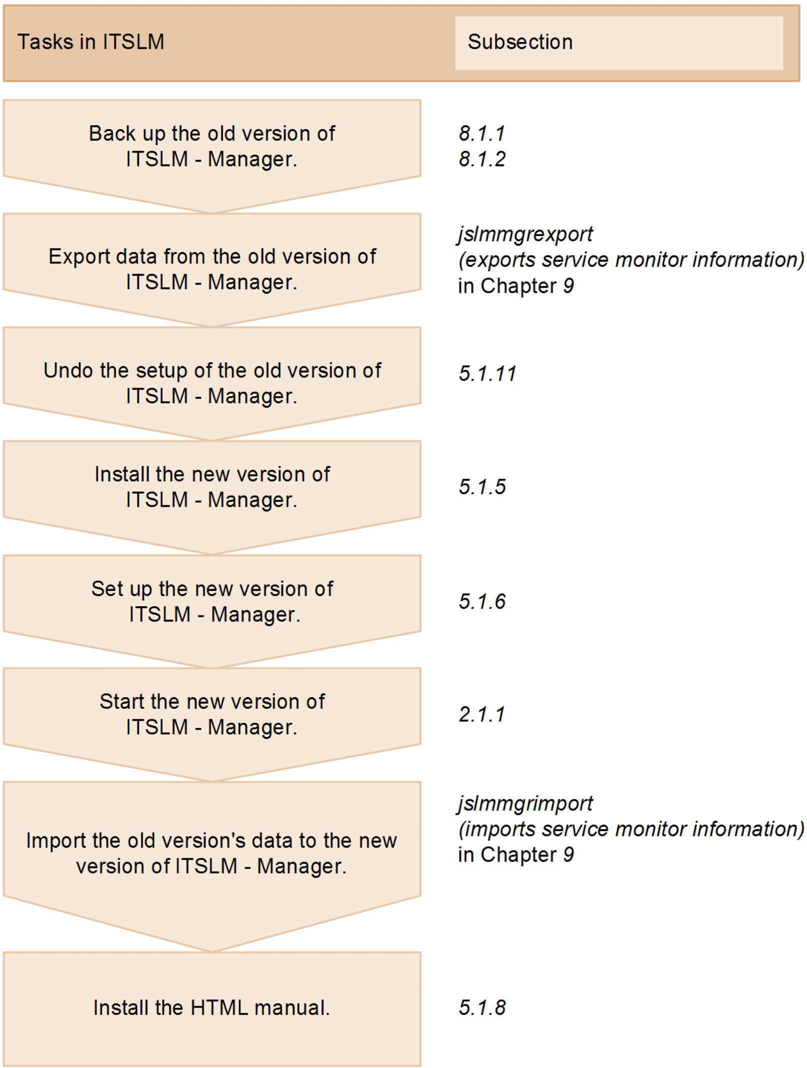
If the capacity of the database that will be used after upgrading will not exceed the database capacity before upgrading, you must re-create the database area. Use the general procedure shown in the following figure for upgrading ITSLM - Manager.

Figure 5–3: General procedure for upgrading ITSLM - Manager that has already been deployed (when upgrading from 09-51 or later and the database capacity after upgrading will not exceed the database capacity before upgrading)


Tasks in ITSLM
Subsection
Back up the old version of ITSLM - Manager.
8.1.1
8.1.2
Install the new version of ITSLM - Manager.
5.1.5
Set up the new version of ITSLM - Manager.
5.1.6
Install the HTML manual.
5.1.8

If the capacity of the database that will be used after upgrading will exceed the database capacity before upgrading, you must re-create the database area. Use the general procedure shown in the following figure for upgrading ITSLM - Manager.

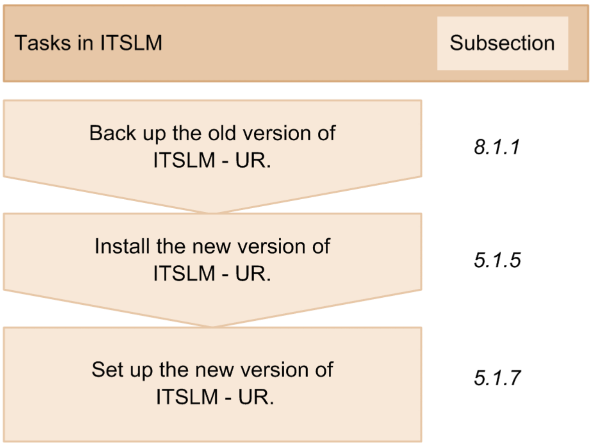
Figure 5–4: General procedure for upgrading ITSLM - Manager that has already been deployed (when upgrading from 09-51 or later and the database capacity after upgrading will exceed the database capacity before upgrading)


Tasks in ITSLM
Subsection
Back up the old version of ITSLM - Manager.
8.1.1
8.1.2
Export data from the old version of ITSLM - Manager.
jslmmgrexport (exports service monitor information) in Chapter 9
Undo the setup of the old version of ITSLM - Manager.
5.1.11
Install the new version of ITSLM - Manager.
5.1.5
Set up the new version of ITSLM - Manager.
5.1.6
Start the new version of ITSLM - Manager.
2.1.1
Import the old version's data to the new version of ITSLM - Manager.
jslmmgrimport (imports service monitor information) in Chapter 9
Install the HTML manual.
5.1.8

(3) Upgrading ITSLM - UR version 09-51 or later

The following figure shows the general procedure for upgrading ITSLM - UR 09-51 or later.

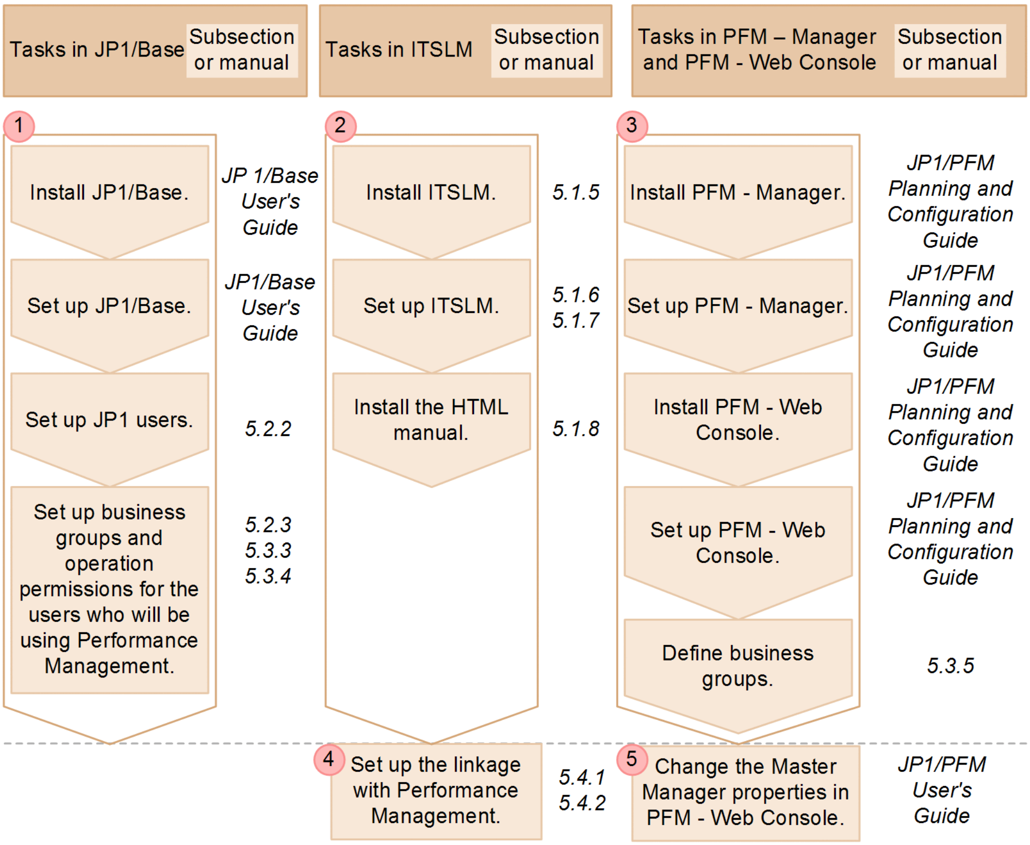
Figure 5–5: General procedure for upgrading ITSLM - UR that has already been deployed (upgrading from 09-51 or later)


Tasks in ITSLM
Subsection
Back up the old version of ITSLM - UR.
8.1.1
Install the new version of ITSLM - UR.
5.1.5
Set up the new version of ITSLM - UR.
5.1.7

5.1.3 General procedure for deploying ITSLM (when linking with a newly deployed Performance Management)

The figure below shows the general procedure for deploying ITSLM when ITSLM is to be linked with a newly deployed Performance Management. In the figure, steps 1 through 3 can be performed in any order; similarly, steps 4 and 5 can be performed in either order.

Figure 5–6: General procedure for deploying ITSLM when ITSLM is linked to a newly deployed Performance Management


Tasks in JP1/Base
Subsection or manual
Tasks in ITSLM
Subsection or manual
Tasks in PFM – Manager and PFM - Web Console
Subsection or manual
1
Install JP1/Base.
JP 1/Base User's Guide
Set up JP1/Base.
JP1/Base User's Guide
Set up JP1 users.
5.2.2
Set up business groups and operation permissions for the users who will be using Performance Management.
5.2.3
5.3.3
5.3.4
2
Install ITSLM.
5.1.5
Set up ITSLM.
5.1.6
5.1.7
Install the HTML manual.
5.1.8
3
Install PFM - Manager.
JP1/PFM Planning and Configuration Guide
Set up PFM - Manager.
JP1/PFM Planning and Configuration Guide
Install PFM - Web Console.
JP1/PFM Planning and Configuration Guide
Set up PFM - Web Console.
JP1/PFM Planning and Configuration Guide
Define business groups.
5.3.5
4
Set up the linkage with Performance Management.
5.4.1
5.4.2
5
Change the Master Manager properties in PFM - Web Console.
JP1/PFM User's Guide

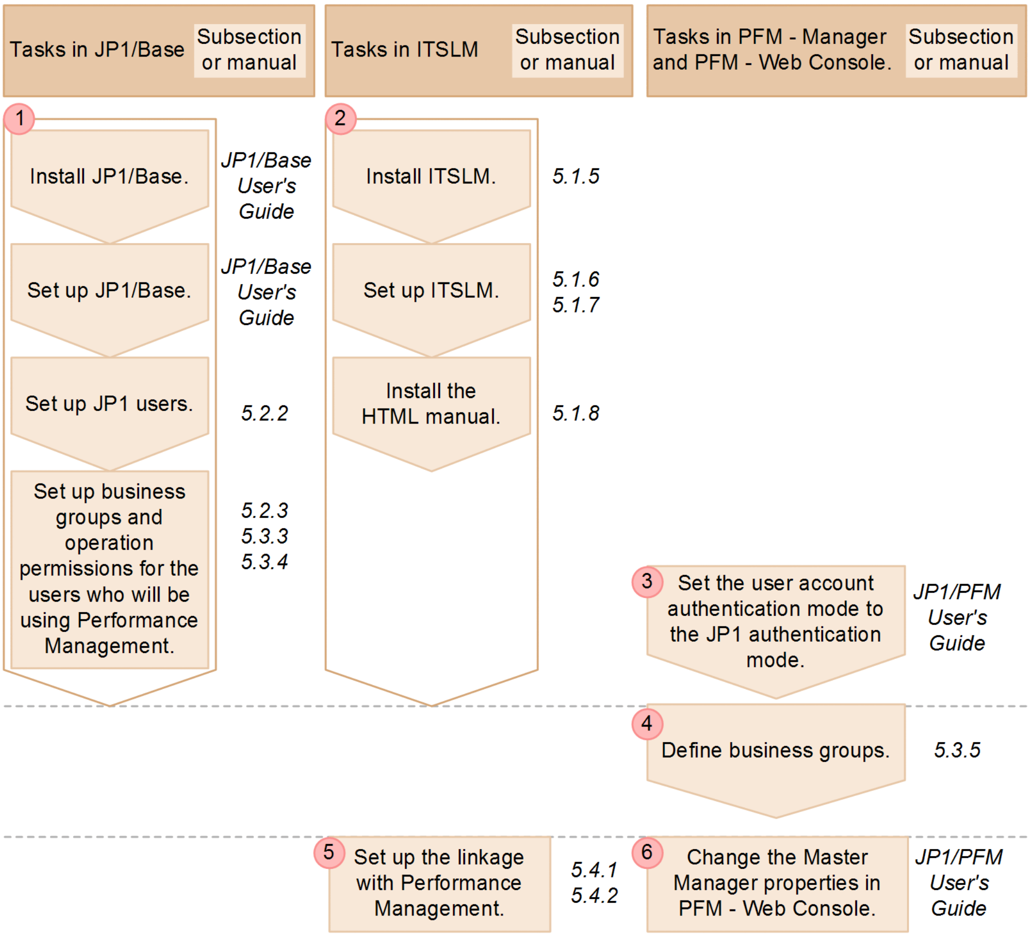
Note: In manual titles in the figure, *JP1* is an abbreviation for *Job Management Partner 1* and *PFM* is an abbreviation for *Performance Management*.

In addition, Performance Management requires installation and setup of monitoring agents corresponding to the monitored targets. For details about installation and setup of monitoring agents, see the applicable PFM - Agent or PFM - RM manual.

5.1.4 General procedure for deploying ITSLM (when linking with an existing Performance Management)

The figure below shows the general procedure for deploying ITSLM when ITSLM is to be linked with an existing Performance Management. In the figure, steps 1 through 3 can be performed in any order; similarly, steps 5 and 6 can be performed in either order.

Figure 5–7: General procedure for deploying ITSLM when ITSLM is linked to an existing Performance Management



Note: In manual titles in the figure, *JP1* is an abbreviation for *Job Management Partner 1* and *PFM* is an abbreviation for *Performance Management*.

5.1.5 Installing ITSLM

The procedure for installing ITSLM is the same for both ITSLM - Manager and ITSLM - UR. You can install either one first.

(1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- If you are upgrading an ITSLM that has already been deployed, first back up your data before upgrading. For details about how to make backups, see *8.1.1 Backing up the definition files* and *8.1.2 Backing up the database*.

(2) Procedure

To install ITSLM:

1. Insert the distribution medium into the correct drive.

2. Install ITSLM by following the installer's instructions.

   You will specify the following items during installation:

   User information

   User name

   Specify a character string of no more than 50 characters.

   Company name

   Specify a character string of no more than 80 characters.

   Installation folder

   By default, the following folder is used:

   system-drive`:\Program Files\HITACHI\JP1ITSLM`

Notes about the installation folder:

- If you change the installation folder, specify an absolute path consisting of no more than 35 characters.
- UNC representation is not supported.
- A network drive cannot be specified.
- The installation folder path cannot contain a hash mark (`#`).
- The folder name cannot begin with a lower-case letter `u`.
- If ITSLM - UR is being installed on the same host where ITSLM - Manager has already been installed, the installation folder for ITSLM - UR will already be set to the folder specified when ITSLM - Manager was installed; no other folder can be specified. Similarly, if ITSLM - Manager is being installed on the same host where ITSLM - UR has already been installed, the installation folder for ITSLM - Manager will already be set to the folder specified when ITSLM - UR was installed; no other folder can be specified.

When the installer terminates normally, the installation is complete.

(3) Supplementary information

- JP1/Base must be installed on the host where ITSLM - Manager has been installed.

  For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.
- The reference time of the host on which ITSLM - Manager and ITSLM - UR have been installed is GMT. On the other hand, the reference time of the computer from which a monitoring person logs in to ITSLM - Manager is based on that computer's time zone.

  To check and output ITSLM's monitoring results in reports, these hosts' time zones must match.

  For details about reports, see *4.5 Creating reports*.

- When ITSLM - Manager or ITSLM - UR is installed, Hitachi Network Objectplaza Trace Library (HNTRLib2) is also installed. At that time, the path for HNTRLib2 (*system-drive*`:\Program Files\Common Files\Hitachi`) is added to the `Path` Windows system environment variable.
- If you install ITSLM - Manager or ITSLM - UR on a host on which the same version of ITSLM - Manager or ITSLM - UR is already installed, select **Repair** in the installer. When **Repair** is selected, all folders and files created by the installer will be restored to their status immediately after the installation. Note that files created by the setup command and folders and files created by users remain unchanged.
- You can use JP1/Software Distribution's remote installation (software distribution) to install ITSLM - Manager or ITSLM - UR on a target host. In this case, the default user information and installation folder are used because the installation window is not displayed. When you use remote installation, you can repair the program by re-installing ITSLM - Manager or ITSLM - UR on a host on which the same version of ITSLM - Manager or ITSLM - UR has already been installed.
- If ITSLM is installed under *system-drive*`:\Program Files\`, the installation will fail if there is a folder or file named `Program` immediately under the system drive. Before you start installation, make sure that there is no folder or file named `Program`.

(4) Next task

- *5.1.6 Setting up ITSLM - Manager* or *5.1.7 Setting up ITSLM - UR*

(5) Related topics

- *5.1.13 Uninstalling ITSLM*

5.1.6 Setting up ITSLM - Manager

The purpose of setup is to create an execution environment.

You can set up either ITSLM - Manager or ITSLM - UR first.

This subsection explains how to set up ITSLM - Manager.

(1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- Before you start the setup, install the ITSLM - Manager that is to be set up.
  For details about the installation, see *5.1.5 Installing ITSLM*.
- Verify that JP1/Base has been installed on the host on which ITSLM - Manager is being installed.
  For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

(2) Procedure

To set up ITSLM - Manager:

1. Create the options file required for setup.
   For details about the options file, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

2. Store the created options file in a desired folder.

Make sure that the absolute path of the options file storage location does not exceed 255 bytes including the options file name (any name).

3. Execute the setup command.

   The following shows the setup command that is to be executed:

   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup` *absolute-path-of-options-file*

   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

When the command terminates normally, ITSLM - Manager setup is complete.

(3) Supplementary information

- If a firewall has been set up on the host on which ITSLM - Manager has been set up, you must release the port numbers that were specified for the `psb_Listen` and `manager_port` definition items in the options file used during setup. If you change the settings in the options file, you must also change the firewall settings, and then check the following:
  1. Check if ephemeral ports for communication between ITSLM - Manager and ITSLM - UR and between ITSLM - Manager and the browser have been released.

     If they have not been released, set up the firewall to release ephemeral ports or set it up to allow communication from the following programs:

     - ITSLM - Manager-installation-folder\mgr\bin\system\jslmmUR.exe

     - ITSLM - Manager-installation-folder\mgr\bin\system\jslmmRMI.exe

     - ITSLM - Manager-installation-folder\mgr\system\psb\CC\web\bin\cjstartweb.exe
  2. Check if the firewall is allowed to communicate with the loopback address of the host where ITSLM - Manager is set up.
- To adjust the time on the host on which ITSLM - Manager has been set up, you must first terminate all ITSLM - Managers and ITSLM - URs. To do this, first stop all services running on the ITSLM - Managers and ITSLM - URs.

  It is preferable to adjust ITSLM - Manager's time forward. If ITSLM - Manager's time is set earlier as a result of adjustment (adjusted backward), wait until the amount of time that was adjusted backward has elapsed, and then start ITSLM - Manager and ITSLM - UR. For example, if you moved the computer's time backward by five minutes, wait for at least five minutes before you start ITSLM - Manager.

  Note that you can adjust the time of a computer that displays windows used for monitoring at any time, regardless of whether ITSLM - Manager is running.
- Make sure that you specify a value in the range from `1` to `65535` for the `psb_Listen` definition item in the options file that is used when the `jslmmgrsetup` command is executed. If you have specified any other value and then performed the setup, perform setup again using the procedure described below after a setup error has been issued.
  1. Correct the `Listen` property value defined in the file shown below (`httpsd.conf`) to a value in the range from `1` to `65535`:

     ITSLM-Manager-installation-folder`\mgr\system\psb\httpsd\conf\httpsd.conf`
  2. Specify a value in the range from `1` to `65535` for the `psb_Listen` definition item in the `jslmmgrsetup` command's options file, and then perform setup again.
- If setup fails during upgrading, data in the database might have become corrupted. Therefore, when setup fails during upgrading, take the appropriate corrective action to eliminate the cause, install ITSLM again using the procedure below, and then perform setup:
  1. Uninstall the ITSLM that has been installed.
  2. Install the previous version of ITSLM.
  3. Restore the backup data that was acquired before upgrading.

4. Re-install the new version of ITSLM.

(4) Next task

- *5.1.7 Setting up ITSLM - UR* or *5.2.2 Setting up JP1 users in JP1/Base*

(5) Related topics

- *5.1.11 Undoing the ITSLM - Manager setup*
- *11.3 Messages*

5.1.7 Setting up ITSLM - UR

The purpose of setup is to create an execution environment.

You can set up either ITSLM - UR or ITSLM - Manager first.

This subsection explains how to set up ITSLM - UR.

(1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- Before you start the setup, install the ITSLM - UR that is to be set up.
  For details about the installation, see *5.1.5 Installing ITSLM*.

(2) Procedure

To set up ITSLM - UR:

1. Execute the command that checks the network interface number and IP address of the host on which ITSLM - UR has been installed.
   Execute the following command:
   ITSLM-UR-installation-folder`\ur\bin\jslmuripls`
   For details about the command that checks the network interface number and IP address, see *jslmuripls (displays network interface number and IP address)* in *9. Commands*.

2. Create the options file required for setup based on the information provided by executing the `jslmuripls` command.
   For details about the options file, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

3. Store the created options file in a desired folder.
   Make sure that the absolute path of the options file storage location does not exceed 255 bytes including the options file name (any name).

4. Execute the setup command.
   The following shows the setup command that is to be executed:
   ITSLM-UR-installation-folder`\ur\bin\jslmursetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

When the command terminates normally, ITSLM - UR setup is complete.

To log an access history, you must set the access log folder for the accesslogFilePath property in the ITSLM - UR system definition file (jp1itslmur.properties). For details about how to set this folder, see "5.6 Editing the system definition files to change settings".

(3) Supplementary information

- If a firewall has been set up on the host on which ITSLM - UR has been set up, you must release the port number that was specified for the `ur_port` definition item in the options file used during setup. If you change the settings in the options file, you must also change the firewall settings, and then check the following:
  1. Check if ephemeral ports for communication between ITSLM - UR and ITSLM - Manager are released.

     If they have not been released, set up the firewall to release the ephemeral ports or set up the firewall to allow communication from the following programs:
     - *ITSLM-UR-installation-folder*`\ur\bin\system\jslmuUR.exe`
     - *ITSLM-UR-installation-folder*`\ur\bin\system\jslmuRMI.exe`
- To adjust the time of the host on which ITSLM - UR has been set up, you must first terminate all ITSLM - Managers and ITSLM - URs.

  Adjust ITSLM - UR's time to ITSLM - Manager's time. If ITSLM - UR's time moved backward (earlier) as a result of adjustment, there is no need to wait to start ITSLM - UR until the amount of time that moved backwards has elapsed. However, if monitoring of monitored services starts while ITSLM - UR's time is in the past, the service performance data acquired by ITSLM - UR is discarded until the last monitoring period has elapsed.

(4) Next task

- *5.1.6 Setting up ITSLM - Manager* or *5.2.2 Setting up JP1 users in JP1/Base*

(5) Related topics

- *5.1.12 Undoing the ITSLM - UR setup*
- *11.3 Messages*

5.1.8 Installing the HTML manual

Copying the HTML manual to a specified folder enables you to reference the HTML manual by clicking **Help** in the upper right corner of a window (or by clicking the **Help** button in the login window).

(1) Before you start

- Set up ITSLM - Manager.

  For details about the setup, see *5.1.6 Setting up ITSLM - Manager*.

(2) Procedure

To install the HTML manual:

1. Locate the distribution medium for the manual that was provided with the program product.

2. On the host on which ITSLM - Manager has been set up, create the folder to which the manual is to be copied.

Create the following folder.

If the browser language is Japanese:

ITSLM-Manager-installation-folder`\mgr\system\psb\httpsd\htdocs\custom\jp1itslm\help\ja\SLM\HTML\`

If the browser language is English:

ITSLM-Manager-installation-folder`\mgr\system\psb\httpsd\htdocs\custom\jp1itslm\help\en\SLM\HTML\`

3. Copy the folders and files from the distribution medium for the manual to the folder created in step 2.

   Copy all folders and files stored in the following folder:

   applicable-drive`\MAN\3021\`*manual-number-folder*#

   #

   This folder name is based on the manual number provided on the first page of this manual. Omit the first three digits and the hyphens (`-`) and add `D` at the end.

   For example, if the manual number is `3021-X-YYY-ZZ`, *manual-number-folder* is `0XYYYZZD`. If there are no digits corresponding to `ZZ`, use `00`, such as `0XYYY00D`.

4. Copy files from the source to the target by overwriting.

   Source:

   ITSLM-Manager-installation-folder`\mgr\system\psb\httpsd\htdocs\custom\jp1itslm\help\INDEX.HTM`

   Target:

   - If the browser language is Japanese:

     ITSLM-Manager-installation-folder`\mgr\system\psb\httpsd\htdocs\custom\jp1itslm\help\ja\INDEX.HTM`

   - If the browser language is English:

     ITSLM-Manager-installation-folder`\mgr\system\psb\httpsd\htdocs\custom\jp1itslm\help\en\INDEX.HTM`

5. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

6. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service**.

When the service status is **Start**, the HTML manual has been installed.

(3) Supplementary information

- The installed HTML manual is deleted when ITSLM - Manager is uninstalled.

(4) Next task

- *2.2.1 Logging in to ITSLM - Manager*
- *5.4.1 Setting up the linkage between ITSLM and Performance Management (working with Performance Management)*

(5) Related topics

- *5.1.13 Uninstalling ITSLM*

5.1.9 Installing and setting up PFM - Manager and PFM - Web Console (working with Performance Management)

To link ITSLM with Performance Management, you must install and set up PFM - Manager and PFM - Web Console.

(1) Before you start

- Design an operation monitoring system that utilizes Performance Management. For details about design of the Performance Management system, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Procedure

For details about the installation and setup of PFM - Manager and PFM - Web Console, see the description of installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(3) Supplementary information

- To perform operation monitoring in Performance Management, not only PFM - Manager and PFM - Web Console but monitoring agents must be installed and set up. For details about installation and setup of monitoring agents, see the applicable PFM - Agent or PFM - RM manual.

(4) Next task

- *5.3.5 Defining business groups in Performance Management*

5.1.10 Undoing the setup of and uninstalling PFM - Manager and PFM - Web Console (working with Performance Management)

You can undo the setup of and uninstall PFM - Manager and PFM - Web Console when they are no longer needed. If you will continue to run Performance Management after releasing its linkage with ITSLM, there is no need to undo the setup of or uninstall PFM - Manager and PFM - Web Console.

(1) Before you start

- In ITSLM, release its linkage with Performance Management. For details about releasing linkage, see *5.4.3 Releasing the linkage between ITSLM and Performance Management (working with Performance Management)*.

(2) Procedure

For details about uninstallation and undoing the setup of PFM - Manager and PFM - Web Console, see the description of uninstallation and undoing the setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(3) Supplementary information

- For details about uninstallation and undoing the setup of monitoring agents, see the applicable PFM - Agent or PFM - RM manual.

(4) Next task

- *5.1.11 Undoing the ITSLM - Manager setup*

5.1.11 Undoing the ITSLM - Manager setup

You must undo the ITSLM - Manager setup before you can set up ITSLM - Manager again.

When setup is undone, the settings in the system definition files that have been edited by the user and the database information are initialized. Before you unto setup, be sure to back up the system definition files and database, if necessary.

For details about backing up the system definition files, see *8.1.1 Backing up the definition files*, and for details about backing up the database, see *8.1.2 Backing up the database*.

This subsection explains how to undo the setup of ITSLM - Manager.

(1) Before you start

- Verify that setup of ITSLM - Manager whose setup is to be undone has been completed.
- Terminate the ITSLM - Manager whose setup is to be undone.
  For details about the termination method, see *2.1.4 Terminating ITSLM - Manager*.

(2) Procedure

To undo the ITSLM - Manager setup:

1. Execute the unsetup command.
   Execute the following unsetup command:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrunsetup`
   For details about the unsetup command, see *jslmmgrunsetup (undoes ITSLM - Manager setup)* in *9. Commands*.

When the command terminates normally, undoing of the ITSLM - Manager setup is complete.

(3) Next task

- *5.1.6 Setting up ITSLM - Manager*

(4) Related topics

- *5.1.12 Undoing the ITSLM - UR setup*
- *11.3 Messages*

5.1.12 Undoing the ITSLM - UR setup

You must undo the ITSLM - UR setup before you can set up ITSLM - UR again.

When setup is undone, the settings in the system definition files that have been edited by the user are initialized. Before you unto setup, be sure to back up the system definition files, if necessary.

For details about backing up the system definition files, see *8.1.1 Backing up the definition files*.

This subsection explains how to undo the setup of ITSLM - UR.

(1) Before you start

- Verify that setup of ITSLM - UR whose setup is to be undone has been completed.
- Terminate the ITSLM - UR whose setup is to be undone.
  For details about the termination method, see *2.1.3 Terminating ITSLM - UR*.

(2) Procedure

To undo the ITSLM - UR setup:

1. Execute the unsetup command.
   Execute the following unsetup command:
   ITSLM-UR-installation-folder`\ur\bin\jslmurunsetup`
   For details about the unsetup command, see *jslmurunsetup (undoes the ITSLM - UR setup)* in *9. Commands*.

When the command terminates normally, undoing of the ITSLM - UR setup is complete.

(3) Next task

- *5.1.7 Setting up ITSLM - UR*

(4) Related topics

- *5.1.11 Undoing the ITSLM - Manager setup*
- *11.3 Messages*

5.1.13 Uninstalling ITSLM

Uninstalling ITSLM is the same for both ITSLM - Manager and ITSLM - UR.

This subsection explains how to uninstall ITSLM.

(1) Before you start

- Terminate the ITSLM - Manager or ITSLM - UR that is to be uninstalled.
  For details about the termination method, see *2.1.4 Terminating ITSLM - Manager* or *2.1.3 Terminating ITSLM - UR*.
- If any Windows service dialog box is open, close it.
- If ITSLM has been linked with Performance Management, verify that the linkage with Performance Management has been released. For details about releasing the linkage, see *5.4.3 Releasing the linkage between ITSLM and Performance Management (working with Performance Management)*.

(2) Procedure

To uninstall ITSLM:

1. From the Windows **Start** menu, select **Control Panel**, and then **Uninstall Program**.

2. From the list, select the ITSLM - Manager or ITSLM - UR to be uninstalled, and then click **Uninstall**.

3. Follow the instructions to uninstall ITSLM.

   The program is uninstalled.

4. Restart the computer, if requested.

5. Delete the user files.

   The installation process does not delete d user-created definition files and log files that were created after the program was installed. To delete these files, use Explorer to delete the folders in which ITSLM - Manager or ITSLM - UR was installed.

The uninstallation is now complete.

(3) Supplementary information

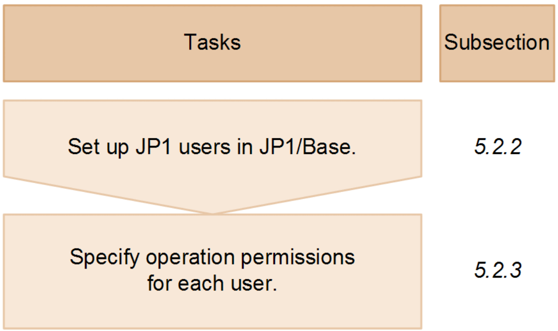
- Some folders might remain after installation is completed. If you do not need these folders or the files in the folders, delete them manually.
- When uninstallation is performed, Hitachi Network Objectplaza Trace Library (HNTRLib2) is also uninstalled automatically. However, if there are programs that are using HNTRLib2, HNTRLib2 will not be uninstalled until all those programs have been uninstalled.
- If you have uninstalled ITSLM - Manager, restore the initial settings for the ports whose firewall settings were changed and that were opened during setup (ports for which the `psb_Listen` and `manager_port` definition items were specified in the options file).
- If you have uninstalled ITSLM - UR, restore the initial settings for the port whose firewall settings were changed and that was opened during setup (port for which the `ur_port` definition item was specified in the options file).
- If ITSLM is linked with Performance Management and ITSLM - Manager is uninstalled while it is still linked with Performance Management, information about ITSLM and monitoring statuses remains in PFM - Manager. This leads to unneeded communications because Performance Management's monitoring agents will continue to send performance data to ITSLM. For details about how to release the linkage with ITSLM in Performance Management, see the descriptions of linkage and release of linkage with ITSLM in the *Job Management Partner 1/Performance Management User's Guide*.

5.2 User settings in ITSLM

To use ITSLM, you must prepare an *authentication server* (JP1/Base), set up JP1 users in the JP1/Base that will be used as the authentication server, and then specify operation permissions for the JP1 users in ITSLM.

The following figure shows the procedure.

Figure 5–8: Procedure for specifying user settings in ITSLM


Tasks
Subsection
Set up JP1 users in JP1/Base.
5.2.2
Specify operation permissions for each user.
5.2.3

For details about the authentication server that must be prepared before JP1 user settings can be specified in JP1/Base, see *5.2.1 Authentication server*.

5.2.1 Authentication server

To use ITSLM, you must have an authentication server for managing the users.

ITSLM uses JP1/Base as the authentication server. There are two ways to use JP1/Base as the authentication server:

- Use the JP1/Base on the host on which ITSLM - Manager is installed.
- Provide a host on which JP1/Base is installed that is separate from the host on which both JP1/Base and JP1/Software Distribution Manager have been installed, then use each host as either the *primary authentication server* or the *secondary authentication server*.

If you already have a JP1/Base that has been used as your authentication server because, for example, you are using other JP1 products, you can use your existing authentication server.

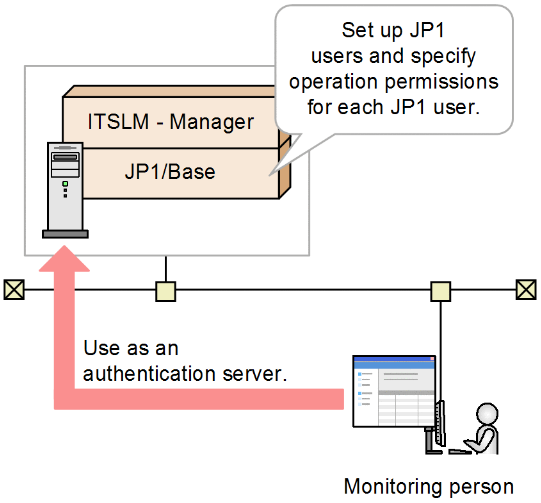
The host specified as the authentication server (primary authentication server) is used to manage JP1 users and operation permissions for JP1 resource groups (service groups).

Therefore, before you set up ITSLM users, evaluate how you want to use authentication servers.

When there is one authentication server:

The example shown in the following figure uses JP1/Base on the host on which ITSLM - Manager is installed as the authentication server.

Figure 5–9: Using JP1/Base on the host on which ITSLM - Manager is installed as the authentication server



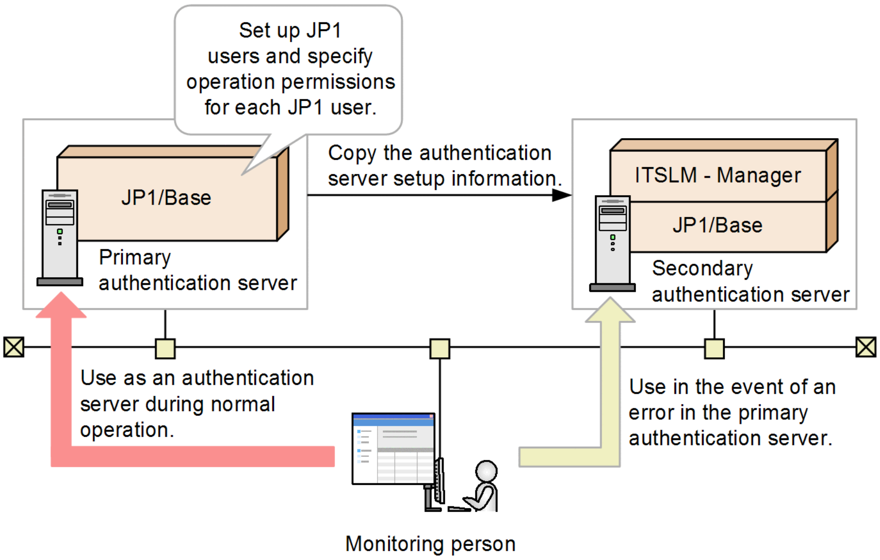
Set up JP1 users and specify operation permissions for each JP1 user.
ITSLM - Manager
JP1/Base
Use as an authentication server.
Monitoring person

If you use JP1/Base on the host on which ITSLM - Manager is installed as the authentication server, you can use ITSLM with the minimum system configuration. However, in the event of a problem in JP1/Base, applications using ITSLM will stop.

When there are two authentication servers:

The example shown in the following figure provides two hosts on which JP1/Base is installed and uses one as the primary authentication server and one as the secondary authentication server.

Figure 5–10: Using two hosts on which JP1/Base is installed and using them as primary and secondary authentication servers



Set up JP1 users and specify operation permissions for each JP1 user.
JP1/Base
Primary authentication server
Copy the authentication server setup information.
ITSLM - Manager
JP1/Base
Secondary authentication server
Use as an authentication server during normal operation.
Use in the event of an error in the primary authentication server.
Monitoring person

If you provide a primary authentication server that is used during normal operation and a secondary authentication server that is used as a backup (and which contains the same setup information as the primary authentication server), then if the primary authentication server cannot be connected for some reason, you can avoid application downtime by switching automatically to the secondary authentication server.

For details about primary and secondary authentication servers, see the section describing authentication servers in the *Job Management Partner 1/Base User's Guide*.

5.2.2 Setting up JP1 users in JP1/Base

The users of ITSLM must be set up as JP1 users in JP1/Base. To set up JP1 users, use the JP1/Base that serves as the authentication server (primary authentication server). When ITSLM is linked with Performance Management, these JP1 users also become Performance Management users.

For details about the authentication server, see *5.2.1 Authentication server*.

This subsection explains how to set up JP1 users who will be authenticated at login by the authentication server.

(1) Before you start

- Verify that JP1/Base is installed on the host on which ITSLM - Manager has been set up. If you use a separate primary authentication server, provide a host with JP1/Base installed that is separate from the host on which ITSLM - Manager has been set up.

  For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

(2) Procedure

To set up users as JP1 users, use JP1/Base's JP1/Base Environment Settings dialog box or a JP1/Base command. This subsection explains the procedure that uses the JP1/Base Environment Settings dialog box. For details, see the section that describes setup of JP1 users in the *Job Management Partner 1/Base User's Guide*.

To set up a JP1 user:

1. Specify the authentication server.

   Specify the authentication server in **Order of authentication server** on the **Authentication Server** tab.

   You can have a maximum of two authentication servers (primary and secondary authentication servers).

2. Register the JP1 user.

   On the **Authentication Server** tab, in **JP user**, register a JP1 user and a password for that user.

When the specified settings have been applied to JP1/Base's JP1/Base Environment Settings dialog box, setup of the user as a JP1 user is complete.

(3) Supplementary information

- For restrictions of the specification of JP1 users, see *Job Management Partner 1/Base User's Guide*.

(4) Next task

- *5.2.3 Specifying operation permissions for each JP1 user*

(5) Related topics

- *5.2.1 Authentication server*

5.2.3 Specifying operation permissions for each JP1 user

Specify operation permissions for each JP1 user in the JP1/Base that is used as the authentication server (primary authentication server).

This subsection explains how to specify operation permissions for ITSLM after users have been set up as JP1 users.

(1) Before you start

- Set up the users as JP1 users.

  For details about how to set up users as JP1 users, see *5.2.2 Setting up JP1 users in JP1/Base*.
- Evaluate how you want to set up JP1 resource groups (*service groups*#) and the JP1 permission level that is to be applied to each service group for the JP1 users.

  ITSLM's JP1 permission levels are `JP1_ITSLM_Admin` (*service group administrator*) and `JP1_ITSLM_User` (*service user*).

  #

  Same as the JP1 resource groups in JP1/Base. This is the unit of managing monitored services for each client (such as a company) that outsources business systems. Every monitored service belongs to a service group.

  In ITSLM, operation permissions are defined for each JP1 permission level as described in the following table.

Table 5–2: Operation permissions for each JP1 permission level

No.	JP1 permission level	User for which JP1 permission level is set	Operation permissions
1	`JP1_ITSLM_Admin`	Service group administrator	• Add and delete monitored services. • Set up monitoring items. • Start and stop monitoring. • Monitor the status of monitored services. • Investigate problems. • Output reports.
2	`JP1_ITSLM_User`	Service user	• Monitor the status of monitored services. • Investigate problems. • Output reports.

Because ITSLM does not allow a service group name beginning with a hyphen (-) to be specified in a command argument, we recommend that you use service group names that do not begin with a hyphen.

(2) Procedure

The JP1/Base Environment Settings dialog box or a JP1/Base command is used to specify operation permissions for each JP1 user. This subsection explains the procedure that uses the JP1/Base Environment Settings dialog box. For details, see the section that describes setup of JP1 users in the *Job Management Partner 1/Base User's Guide*.

To specify operation permissions for a JP1 user:

1. Specify operation permissions for a JP1 user.

   On the **Authentication Server** tab, in **Authority level for JP1 resource group**, specify the applicable operation permissions for the JP1 user.

When the specified settings have been applied in JP1/Base's JP1/Base Environment Settings dialog box, specification of operation permissions for the JP1 user is complete.

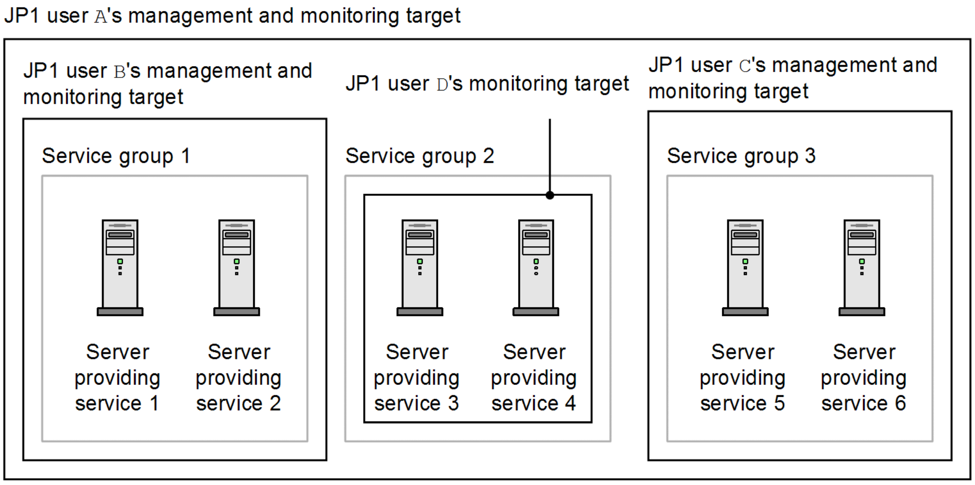
(3) Supplementary information

- This subsection explains an example of specifying operation permissions for JP1 users. This example specifies operation permissions for four JP1 users, `A` through `D`, who perform operations on service groups 1 through 3, each of which has two monitored services, as follows:

- JP1 user A manages and monitors the monitored services in service groups 1, 2, and 3.
- JP1 user B manages and monitors the monitored services in service group 1.
- JP1 user C manages and monitors the monitored services in service group 3.
- JP1 user D monitors the monitored services in service group 2 (this JP1 user does not manage monitored services).

The following figure illustrates these conditions.

Figure 5–11: Example of specifying operation permissions


JP1 user A's management and monitoring target
JP1 user B's management and monitoring target
JP1 user D's monitoring target
JP1 user C's management and monitoring target
Service group 1
Service group 2
Service group 3
Server providing service 1
Server providing service 2
Server providing service 3
Server providing service 4
Server providing service 5
Server providing service 6

To satisfy these conditions, operation permissions must be specified for these JP1 users as shown in the following table.

Table 5–3: Example of specifying operation permissions

No.	JP1 user	Service group		
		1	2	3
1	A	Admin	Admin	Admin
2	B	Admin	--	--
3	C	--	--	Admin
4	D	--	User	--

Legend:

Admin: Service group administrator permissions are specified.

User: Service user permissions are specified.

--: No operation permissions are specified.

(4) Related topics

- *2.1.1 Starting ITSLM - Manager*
- *5.5.1 Linking with JP1/IM*

5.2.4 Notes about user setup

The following notes apply to user setup.

- Deleting a JP1 resource group (service group) does not delete the monitored services that have been registered for the service group that is being deleted. When you want to delete a service group, first delete the monitored services that have been registered for the target service group.
- Once you start monitoring the status of monitored services in ITSLM, do not perform any of the change or deletion operations in JP1/Base shown below; if any of these operations are performed, ITSLM operation is not guaranteed:
  - Renaming JP1 users
  - Deleting JP1 users
  - Renaming JP1 resource groups (service groups)
  - Deleting JP1 resource groups (service groups)
  - Changing the operation permissions for a JP1 user

5.3 User setup in Performance Management (working with Performance Management)

Performance Management uses two methods to manage user accounts. These management methods are called the user authentication modes. Performance Management manages hosts in units called business groups.

If you link ITSLM with Performance Management, set up the JP1 users in JP1/Base based on Performance Management's user authentication modes. Also, set up in Performance Management the business groups that are to be associated with the JP1 users.

After these setups have been completed, Performance Management's user authentication can be performed when JP1 users log in to ITSLM. This enables smooth acquisition of system performance information related to monitored services in the event of a reduction in service level.

5.3.1 User authentication modes

Performance Management manages user accounts by applying one of the following authentication modes:

- *PFM authentication mode*

  This authentication mode manages user accounts in Performance Management's operation monitoring system.

  Performance management users created in Performance Management log in to PFM - Web Console. The user accounts are managed by PFM - Manager.

- *JP1 authentication mode*

  This authentication mode manages user accounts centrally in JP1/Base.

  JP1 users created in JP1/Base log in to PFM - Web Console. The user accounts are managed by JP1/Base. To use this authentication mode, JP1/Base must be installed on the host on which PFM - Manager is installed.

For details about user authentication in Performance Management, see the *Job Management Partner 1/Performance Management User's Guide*.

5.3.2 Business groups

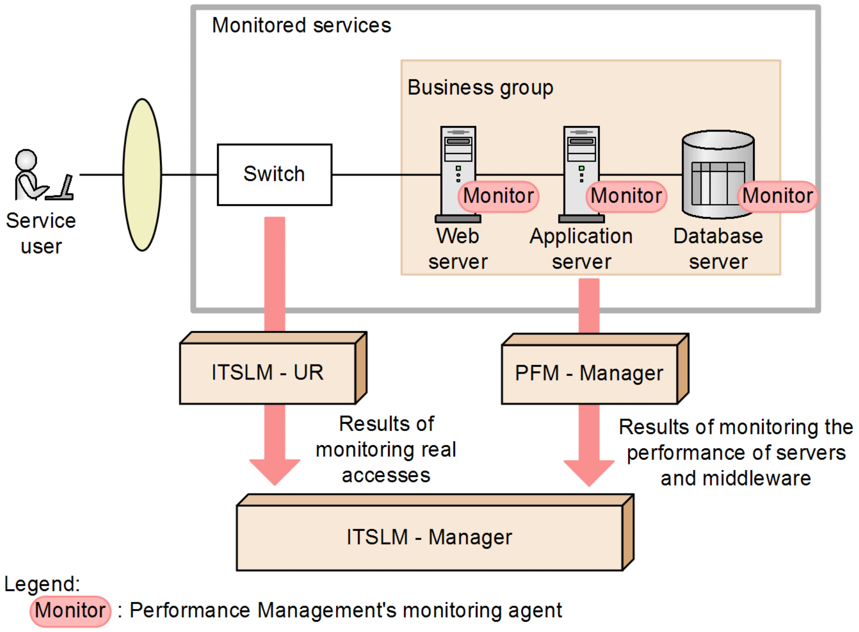
Performance Management manages hosts in business groups.

(1) About business groups

Business groups are the units used in Performance Management for grouping managed hosts. A user to whom a business group has been assigned can reference the information collected by the monitoring agent that monitors the hosts in that business group.

The following figure shows an example relationship between monitored services and business groups.

Figure 5–12: Example relationship between monitored services and business groups



In this example, the Web server, application program server, and database server that are monitored by Performance Management's monitoring agent are defined to belong to one business group. This business group has been defined in ITSLM's monitored service configuration information. When monitoring of the services begins in ITSLM, ITSLM - UR collects the results of monitoring real accesses to the services and ITSLM - Manager collects data including the OS performance on each host that belongs to the business group. Because ITSLM - Manager manages all this information, the status of all monitored services can be monitored.

For example, if ITSLM is to monitor a work timesheet management service, ITSLM - UR collects monitoring results including the average response times of real accesses from service users to the work timesheet management service. ITSLM - Manager collects performance data as the monitoring results of one business group, including the CPU and memory usage of individual hosts, that is, the Web server that accepts requests to the work timesheet management service, the application program server on which the service is actually running, and the database server that manages the data. All this information can be monitored in ITSLM windows.

Reference note

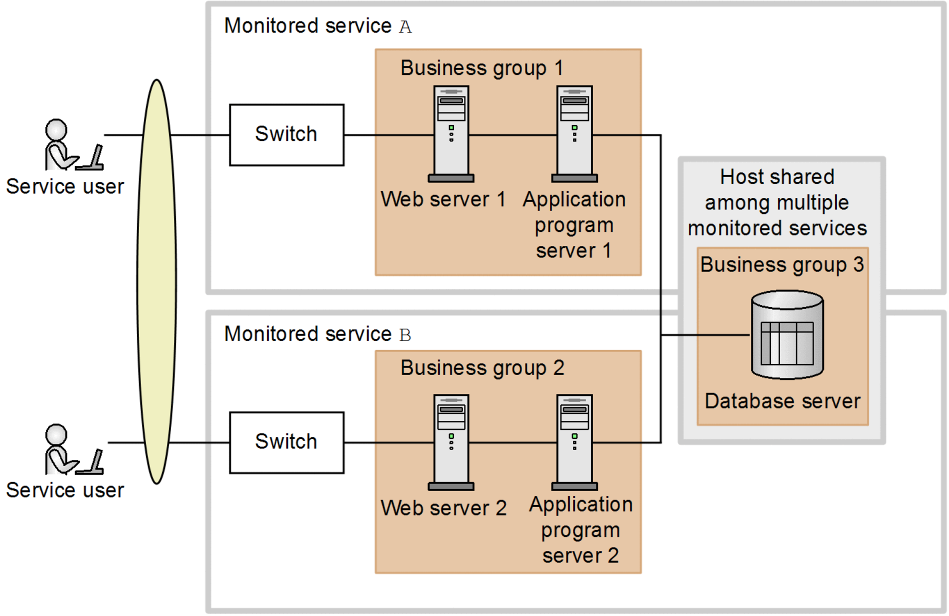
When there is a change to the number of monitored services in a business group that has been defined in the monitored service configuration information, there is no need to change the configuration information in the ITSLM windows.

(2) Concept of business group creation

In Performance Management, a managed host cannot belong to multiple business groups. In ITSLM, you might want to specify the same host, such as the database host, in multiple monitored services' configuration information.

In such a case, define a managed host that might be included in multiple services' configuration information as an independent business group, as shown in the following example.

Figure 5–13: Example of including a single managed host in multiple services' configuration information

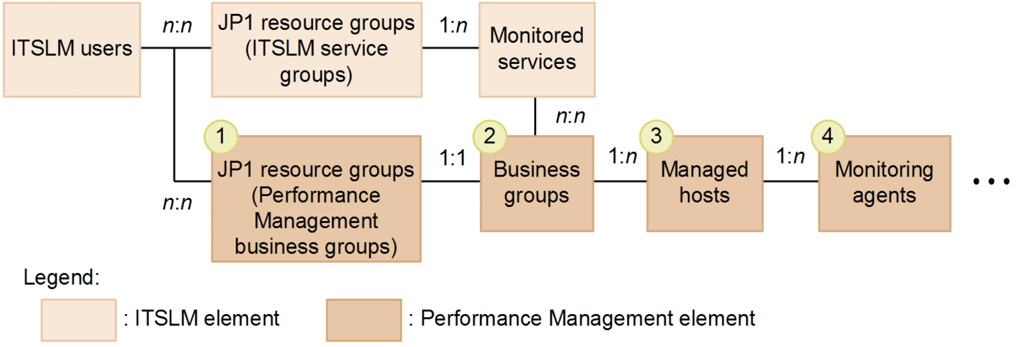


In this example, monitored services A and B share the same host for the database server. This is made possible by defining the database server to be shared as business group 3 separately from business groups 1 and 2. As a result, the database server can be specified in two monitored services' configuration information

(3) Elements used when ITSLM is linked with Performance Management

The following figure shows the relationship among elements used when ITSLM is linked with Performance Management and ITSLM's monitored services.

Figure 5–14: Elements used when ITSLM is linked with Performance Management


ITSLM users
n:n
JP1 resource groups (ITSLM service groups)
1:n
Monitored services
n:n
n:n
1
JP1 resource groups (Performance Management business groups)
1:1
2
Business groups
1:n
3
Managed hosts
1:n
4
Monitoring agents
...
Legend:
: ITSLM element
: Performance Management element

The following table explains the Performance Management elements.

Table 5–4: Performance Management elements

No.	Element	Description
1	JP1 resource group (Performance Management business group)	A group of logical resources in JP1/Base. In Performance Management, one JP1 resource group corresponds to one business group.
2	Business group	A group of one or more managed hosts in Performance Management. One business group can belong to only one JP1 resource group, not to multiple JP1 resource groups.

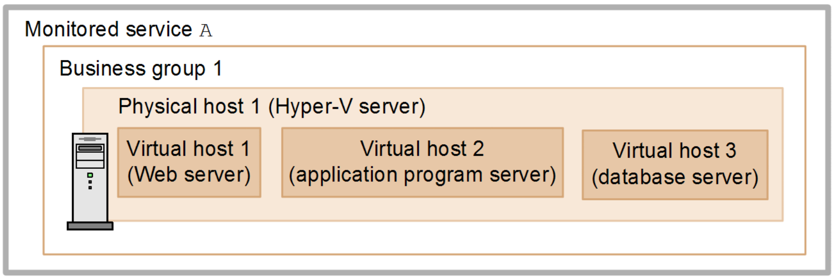
No.	Element	Description
2	Business group	The relationship between business groups and monitored services managed in ITSLM is multiple business groups to multiple monitored services.
3	Managed host	Host monitored by Performance Management. One managed host belongs to one business group.
4	Monitoring agent	Agent program that exists in each server and each middleware running on a managed host and that monitors the corresponding server or middleware. A monitoring agent collects more than one set of performance data. For PFM - RM, a virtual monitoring agent exists on each managed host, but its entity is located on the remote host.

(4) Supplementary information

- For a business group containing a host that is shared among multiple JP1 users, set up a separate JP1 resource group from any JP1 resource group for ITSLM's service group. If the JP1 resource group for the service group is set up for this business group and a monitored service is added to that service group, all the sharing users can monitor that added service.
- When monitoring a service running on a virtual host, ITSLM does not retain the relationship between the virtual host and the physical host on which the virtual host is running. These hosts are monitored as separate elements of the monitored service.

  The following shows an example.

  Figure 5–15: Monitoring by ITSLM of virtual hosts and physical host, which are Performance Management's monitored targets

  
  Monitored service A
Business group 1
Physical host 1 (Hyper-V server)
Virtual host 1 (Web server)
Virtual host 2 (application program server)
Virtual host 3 (database server)

  In this example, business group 1 is defined as the configuration information for monitored service A. Physical host 1 and virtual hosts 1 through 3 that are running on physical host 1 are defined for business group 1. ITSLM treats physical host 1 and virtual hosts 1 through 3 as independent elements of monitored service A without having to recognize that virtual hosts 1 through 3 are running on physical host 1.

5.3.3 Setting up the users who will be using Performance Management (PFM authentication mode)

When you link ITSLM with Performance Management, you must grant the ITSLM users the operation permissions for the JP1 resource groups corresponding to Performance Management's business groups. You can register JP1 resource groups in JP1/Base's JP1/Base Environment Settings dialog box. For details, see the section that describes setup of JP1 users in the *Job Management Partner 1/Base User's Guide*.

(1) Before you start

- Verify that Performance Management has been installed and set up. For details about how to install and set up Performance Management, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
- Verify that the PFM authentication mode has been set up as Performance Management's user authentication mode. If you are using the JP1 authentication mode, see *5.3.4 Setting up the users who will be using Performance Management (JP1 authentication mode)*.
- Verify that the ITSLM users who will be using Performance Management have been registered. For details about setup of ITSLM users, see *5.2.2 Setting up JP1 users in JP1/Base*.
- Check the correspondence between ITSLM's service groups and Performance Management's business groups, and verify the user names of ITSLM's JP1 users (service group administrators or service users) to which permissions for the business groups are to be granted.

(2) Procedure

PFM - Web Console is used to set up Performance Management users' accounts. For details, see the *Job Management Partner 1/Performance Management User's Guide*.

To set up JP1 users, use JP1/Base's JP1/Base Environment Settings dialog box or a JP1/Base command. This subsection explains the procedure that uses the JP1/Base Environment Settings dialog box. For details, see the section that describes setup of JP1 users in the *Job Management Partner 1/Base User's Guide*.

To set up the users who will be using Performance Management:

1. Log in to PFM - Web Console as a user who has a user account with administrator user permissions, and then create a performance management user account that is authorized to monitor the target business group.

   > **Tip**
   >
   > For the user name of the user account to be created, specify the name of an ITSLM service group administrator or service user.

2. Start JP1/Base as a user with Administrators permissions, and then select the JP1 user with the same name as for the user account created in step 1.

3. For the selected JP1 user, add the JP1 resource group that corresponds to the business group to be monitored.

   > **Reference note**
   >
   > The correspondence between JP1 resource group names and business groups is defined in the business group definition file that is created in *5.3.5 Defining business groups in Performance Management*.

4. For the selected JP1 user, add the `JP1_PFM_Operator` permission.

   The following table describes the types of ITSLM users, permissions to be granted to each user, and operations that can be performed on Performance Management:

No.	ITSLM user type	Permissions	Operations that can be performed on Performance Management
1	Service group administrator	• `JP1_ITSLM_Admin` • `JP1_PFM_Operator`	Starting and stopping monitoring agents and specifying conditions related to the monitoring performed by monitoring agents.

No.	ITSLM user type	Permissions	Operations that can be performed on Performance Management
1	Service group administrator	• `JP1_ITSLM_Admin` • `JP1_PFM_Operator`	Also, viewing the information collected by monitoring agents from the ITSLM windows.
2	Service user	• `JP1_ITSLM_User` • `JP1_PFM_Operator`	Viewing the information collected by monitoring agents from the ITSLM windows.

When the specified settings have been applied to JP1/Base's JP1/Base Environment Settings dialog box, the setup is complete.

(3) Supplementary information

- When Performance Management uses the PFM authentication mode, single sign-on from an ITSLM window is not supported. If an attempt is made to display Performance Management information from ITSLM's Troubleshoot window, Performance Management's login window is displayed.

(4) Next task

- *5.3.5 Defining business groups in Performance Management*

(5) Related topics

- *5.2.2 Setting up JP1 users in JP1/Base*
- *5.2.3 Specifying operation permissions for each JP1 user*

5.3.4 Setting up the users who will be using Performance Management (JP1 authentication mode)

When you link ITSLM with Performance Management, you must grant the ITSLM users the operation permissions for the JP1 resource groups corresponding to Performance Management's business groups. You can register JP1 resource groups in JP1/Base's JP1/Base Environment Settings dialog box. For details, see the section that describes setup of JP1 users in the *Job Management Partner 1/Base User's Guide*.

(1) Before you start

- Verify that Performance Management has been installed and set up. For details about how to install and set up Performance Management, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.
- Verify that the JP1 authentication mode has been set up as Performance Management's user authentication mode. If you are using the PFM authentication mode, see *5.3.3 Setting up the users who will be using Performance Management (PFM authentication mode)*.
- Verify that the ITSLM users who will be using Performance Management have been registered. For details about setup of ITSLM users, see *5.2.2 Setting up JP1 users in JP1/Base*.
- Check the correspondence between ITSLM's service groups and Performance Management's business groups, and verify the user names of ITSLM's JP1 users (service group administrators or service users) to which permissions for the business groups are to be granted.

(2) Procedure

To set up JP1 users, use JP1/Base's JP1/Base Environment Settings dialog box or a JP1/Base command. This subsection explains the procedure that uses the JP1/Base Environment Settings dialog box. For details, see the section that describes setup of JP1 users in the *Job Management Partner 1/Base User's Guide*.

To set up the users who will be using Performance Management:

1. Start JP1/Base as a user with Administrators permissions, and then select a JP1 user corresponding to an ITSLM service group administrator or service user.

2. For the selected JP1 user, add the JP1 resource group that corresponds to the business group to be monitored.

> **Reference note**
>
> The correspondence between JP1 resource group names and business groups is defined in the business group definition file that is created in *5.3.5 Defining business groups in Performance Management*.

3. For the selected JP1 user, add the `JP1_PFM_Operator` permission.

   The following table describes the types of ITSLM users, permissions to be granted to each user, and operations that can be performed on Performance Management:

No.	ITSLM user type	Permission	Operations that can be performed on Performance Management
1	Service group administrator	• `JP1_ITSLM_Admin` • `JP1_PFM_Operator`	Starting and stopping monitoring agents and specifying conditions related to the monitoring performed by monitoring agents. Also, viewing the information collected by monitoring agents from the ITSLM windows.
2	Service user	• `JP1_ITSLM_User` • `JP1_PFM_Operator`	Viewing the information collected by monitoring agents from the ITSLM windows.

If you add "JP1_PFM" to the selected JP1 user as the JP1 resource group for the business group to be monitored, add JP1_PFM_Admin or JP1_PFM_Operator permission according to the access permission required by PFM.

For details, see the description of JP1 user permission required to link with ITSLM in the "Job Management Partner 1/Performance Management User's Guide".

When the specified settings have been applied to JP1/Base's JP1/Base Environment Settings dialog box, the setup is complete.

(3) Next task

- *5.3.5 Defining business groups in Performance Management*

(4) Related topics

- *5.2.2 Setting up JP1 users in JP1/Base*
- *5.2.3 Specifying operation permissions for each JP1 user*

5.3.5 Defining business groups in Performance Management

You define business groups so that you can group managed hosts in Performance Management. You must also establish the correspondences between the defined business groups and the JP1 resource groups.

(1) Before you start

- In Performance Management, perform the setup required for using business groups. Also, see *5.3.2 Business groups* to check the concept of business group creation and determine the range of managed hosts to be included in the business groups. For details about the settings, see the description of business group setup and operations in the *Job Management Partner 1/Performance Management User's Guide*.
- Verify the names of the JP1 resource groups that were added in *5.3.3 Setting up the users who will be using Performance Management (PFM authentication mode)* or *5.3.4 Setting up the users who will be using Performance Management (JP1 authentication mode)* to establish the correspondences to the business groups.

(2) Procedure

This subsection provides an overview of the business group creation procedure. For details about the settings, see the description of business group setup and operations in the *Job Management Partner 1/Performance Management User's Guide*.

To create business groups:

1. Create a business group definition file.
   In the business group definition file, specify each business group name and the JP1 resource group and host name that correspond to each business group name.

2. Check the validity of the business group definition file, and then import it to Performance Management.

When the command terminates normally, business group creation is complete.

(3) Next task

- *5.4.1 Setting up the linkage between ITSLM and Performance Management (working with Performance Management)*

5.3.6 Example JP1 user setup in Performance Management

This example registers an ITSLM user and grants to that user the operation permissions needed for ITSLM and Performance Management monitoring. It also sets up the business groups to be monitored by Performance Management and the managed hosts to be included in the business groups.

To specify which monitoring items of Performance Management are to be monitored by ITSLM, further settings are needed in ITSLM's Settings window after the setup explained here has been completed. For details about the settings in ITSLM's Settings window, see *3. Monitoring the Services to Be Monitored and Setup Required for Monitoring*.

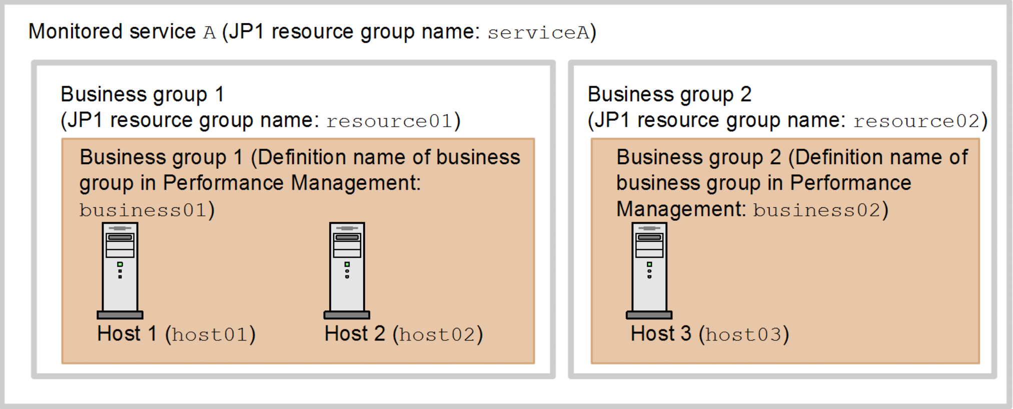
(1) Prerequisites

The prerequisites for this example of setup are as follows:

- ITSLM will be linked with a newly employed Performance Management.

- The user authentication mode in Performance Management is the JP1 authentication mode.
- user01 is set up as a new JP1 user and registered as ITSLM's service group administrator.
- The following figure shows the relationship between the monitored services and the hosts that user01 will be monitoring.

Figure 5–16: System configuration for the example of setup of a JP1 user in Performance Management


Monitored service A (JP1 resource group name: serviceA)
Business group 1
(JP1 resource group name: resource01)
Business group 1 (Definition name of business group in Performance Management: business01)
Host 1 (host01)
Host 2 (host02)
Business group 2
(JP1 resource group name: resource02)
Business group 2 (Definition name of business group in Performance Management: business02)
Host 3 (host03)

The example defines hosts 1 and 2 in business group 1 as the hosts used only by monitored service A. The example defines host 3 in business group 2, which is an independent business group, because this host might be used by other monitored services.

(2) Setting up a JP1 user who will be using ITSLM

Tasks in JP1/Base

The user with Administrators permissions for the host on which JP1/Base is installed registers user01 as a new JP1 user. This registration is performed using the procedure described below. For details about the prerequisite tasks and operations, see the description of JP1 user setup (standard user) in the *Job Management Partner 1/Base User's Guide*.

To set up a JP1 user who will be using ITSLM:

1. Start JP1/Base as a user with Administrators permissions. In the JP1/Base Environment Settings dialog box, on the **Authentication Server** tab, in **JP user**, click the **Add** button.

2. In the displayed JP1 User dialog box, register user01.

   user01 is displayed under **Users** in **JP user**.

3. In **JP user**, from **Users**, select user01.

   In **Authority level for JP1 resource group**, the group (JP1 resource group) that this user can access and that group's permission level (JP1 permission level) are displayed.

4. In **Authority level for JP1 resource group**, click the **Add** button.

   The JP1 Resource Group Details dialog box is displayed.

5. In **JP1 resource group**, enter serviceA (JP1 resource group name corresponding to service group A), and then in **Permissions**, add JP1_ITSLM_Admin.

6. Click the **OK** button.

Results of tasks

user01 has been registered as a user who will be using ITSLM and the service group administrator permissions for serviceA were granted.

(3) Adding the settings to link with Performance Management

Tasks in JP1/Base

This example adds the settings required for linking with Performance Management for registered user01. As was the case in (2), this task must be executed by a user with Administrators permissions for the host on which JP1/Base is installed.

1. In the JP1/Base Environment Settings dialog box, on the **Authentication Server** tab, from the JP1 users displayed in **JP user**, select user01.
2. In **Authority level for JP1 resource group**, click the **Add** button.
   The JP1 Resource Group Details dialog box is displayed.
3. In **JP1 resource group**, enter resource01 (JP1 resource group name corresponding to business group 1), and then in **Permissions**, add JP1_PFM_Operator.
4. Click the **OK** button.
5. While user01 is selected in **JP user** on the **Authentication Server** tab, click the **Add** button again in **Authority level for JP1 resource group**.
   The JP1 Resource Group Details dialog box is displayed.
6. In **JP1 resource group**, enter resource02 (JP1 resource group name corresponding to business group 2), and then in **Permissions**, add JP1_PFM_Operator.
7. Click the **OK** button.

Results of tasks

The permissions (JP1_PFM_Operator) needed to monitor resource01 and resource02, the JP1 resource groups corresponding to Performance Management's business groups, are now granted to user01 who will be using ITSLM.

(4) Defining business groups

This example defines business groups to group the managed hosts in Performance Management, and then establishes their correspondence to JP1 resource groups. For details about the prerequisite tasks and operations, see the description of business group setup and operation in the *Job Management Partner 1/Performance Management User's Guide*.

Tasks in PFM - Manager

To define business groups:

1. Create a business group definition file for business group 1 and then save it.
   Create the following business group definition file:
   - Specify gyoumu01 as the name for the business group.
   - Specify resource01 as the JP1 resource group name.
   - Specify host01 and host02 as the host names.

2. Create a business group definition file for business group 2 and then save it.

   Create the following business group definition file:

   - Specify `gyoumu02` as the name for the business group.
   - Specify `resource02` as the JP1 resource group name.
   - Specify `host03` as the host name.

3. Verify the validity of the business group definition files, and then import them to Performance Management.

Results of tasks

Correspondence is now established between Performance Management's business groups and `resource01` and `resource02` (JP1 resource groups monitored by `user01`), and the managed hosts are now defined.

(5) Related topics

- *5.2.2 Setting up JP1 users in JP1/Base*
- *5.2.3 Specifying operation permissions for each JP1 user*
- *5.3.4 Setting up the users who will be using Performance Management (JP1 authentication mode)*
- *5.3.5 Defining business groups in Performance Management*

5.4 Setting up a linkage between ITSLM and Performance Management

To link ITSLM with Performance Management, you must edit the system definition file in ITSLM. In Performance Management, you must use PFM - Web Console to change the Master Manager properties. For details about changing the Master Manager properties in PFM - Web Console, see the *Job Management Partner 1/Performance Management User's Guide*.

5.4.1 Setting up the linkage between ITSLM and Performance Management (working with Performance Management)

Use ITSLM's system definition file to specify the settings needed to link ITSLM with Performance Management.

(1) Before you start

- Verify that ITSLM - Manager, PFM - Manager, and PFM - Web Console have been installed and set up.
- Verify that ITSLM - Manager is terminated. For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.
- Verify that a host name, not the IP address, is specified in the `managerHost` property in the system definition file (`jp1itslm.properties`) of ITSLM - Manager. If an IP address is specified, change it to the host name.

(2) Procedure

To set up the linkage between ITSLM and Performance Management:

1. In the system definition file (`jp1itslm.properties`) of ITSLM - Manager, specify the following properties:
    - `pfmManagerHost` (PFM - Manager's host name)
    - `pfmManagerPort` (PFM - Manager's port number[#1, #2])
    - `pfmWebConsoleURL` (URL of PFM - Web Console that is to be started from ITSLM)
    - `pfmReceivePort` (Port number used by ITSLM - Manager to receive performance data[#2])

    #1: This port is used by the PFM - Manager service's **View Server**.

    #2: For details, see the description of network setup for linking with ITSLM in the *Job Management Partner 1/Performance Management User's Guide*.

    Edit the system definition file of ITSLM - Manager. The system definition file is stored at the following location:

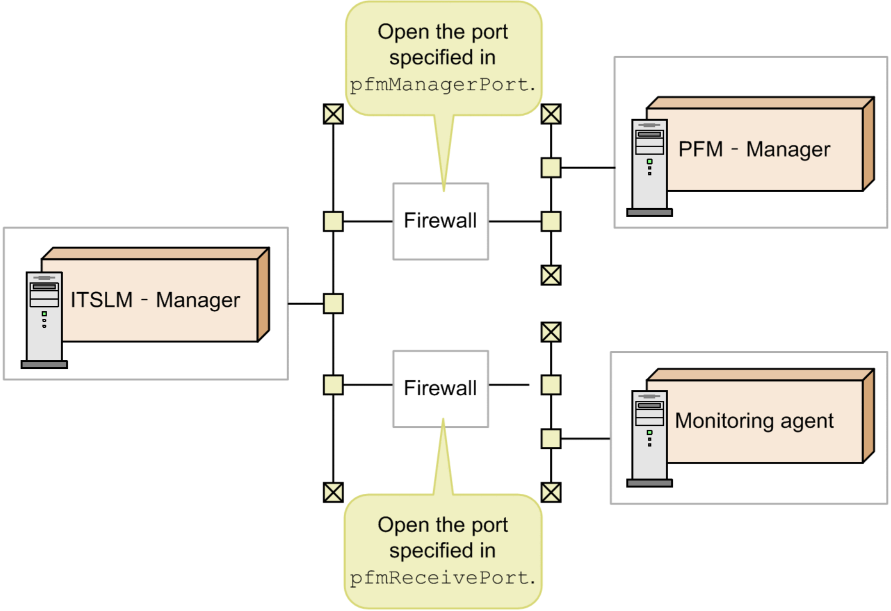
    ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`

2. If a firewall has been set up between ITSLM and Performance Management, set the firewall to open the ports that correspond to the following properties specified in step 1:
    - `pfmManagerPort`
    - `pfmReceivePort`

    Note that the port specified in the `pfmReceivePort` property is used for communications between ITSLM - Manager and monitoring agents. Therefore, configure the firewall between ITSLM - Manager and the monitoring agents so that the port specified in `pfmReceivePort` is open.

    Also check the following:

- Check if the firewall between ITSLM - Manager and PFM - Manager is configured so that the port specified for the `pfmManagerPort` property is open. If the port is not open, configure the firewall so that the port is open.
- Check if the ephemeral ports used for communication between ITSLM - Manager and PFM - Manager are open. If they are not open, configure the firewall so that the ephemeral ports are open or configure the firewall to allow communication from the following program:
  ITSLM-Manager-installation-folder`\mgr\bin\system\jslmmadaptor.exe`
  The following figure shows the correspondence between firewall locations and ports to be opened.


Open the port specified in pfmManagerPort.
PFM - Manager
Firewall
ITSLM - Manager
Firewall
Monitoring agent
Open the port specified in pfmReceivePort.

The setup needed in ITSLM to link with Performance Management is now complete.

(3) Next task

- *5.4.2 Specifying settings for saving Performance Management's performance data from ITSLM (working with Performance Management)*

5.4.2 Specifying settings for saving Performance Management's performance data from ITSLM (working with Performance Management)

When PFM - Web Console is started from ITSLM and you use it to monitor the performance data collected by Performance Management, if the performance data is not stored in Performance Management's Store database, detailed performance data cannot be checked.

You can use PFM - Web Console or ITSLM - Manager's system definition file to specify the settings needed to store performance data in the Store database.

This subsection explains the procedure for editing ITSLM - Manager's system definition file and storing performance data in the Store database.

(1) Before you start

- Verify that setup of ITSLM - Manager has been completed. For details about the setup method, see *5.1.6 Setting up ITSLM - Manager*.
- Verify that ITSLM - Manager has terminated. For details about the termination method, see *2.1.4 Terminating ITSLM - Manager*.

(2) Procedure

To specify the settings for saving Performance Management's performance data from ITSLM:

1. In ITSLM - Manager's system definition file (`jp1itslm.properties`), set the `pfmLoggingData` property to `true`.

   Edit ITSLM - Manager's system definition file. The system definition file is stored at the following location:

   ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`

The settings for storing performance data in Performance Management's Store database have now been specified.

(3) Supplementary information

- The following table shows the relationship between settings in ITSLM and Performance Management and how performance data is stored.

Table 5–5: Relationship between settings in ITSLM and Performance Management and how performance data is stored

No.	ITSLM monitoring status	pfmLoggingData property setting in ITSLM	Log property setting in PFM - Web Console#	Storage location for collected performance data
1	Monitoring has started	`true`	Yes	• Performance Management's Store database • ITSLM database
2			No	• Performance Management's Store database • ITSLM database
3		`false`	Yes	• Performance Management's Store database • ITSLM database
4			No	• ITSLM database
5	Monitoring has stopped or monitoring is not performed in ITSLM	--	Yes	• Performance Management's Store database
6			No	Performance data is not collected

Legend:

--: Not applicable (the property setting is not applicable)

#: The setting specified in PFM - Web Console is applied to each monitoring agent of Performance Management.

- ITSLM's `pfmLoggingData` property value is applied from ITSLM - Manager to each monitoring agent when ITSLM starts monitoring. The applied property value is retained by each monitoring agent until the next time ITSLM monitoring begins.

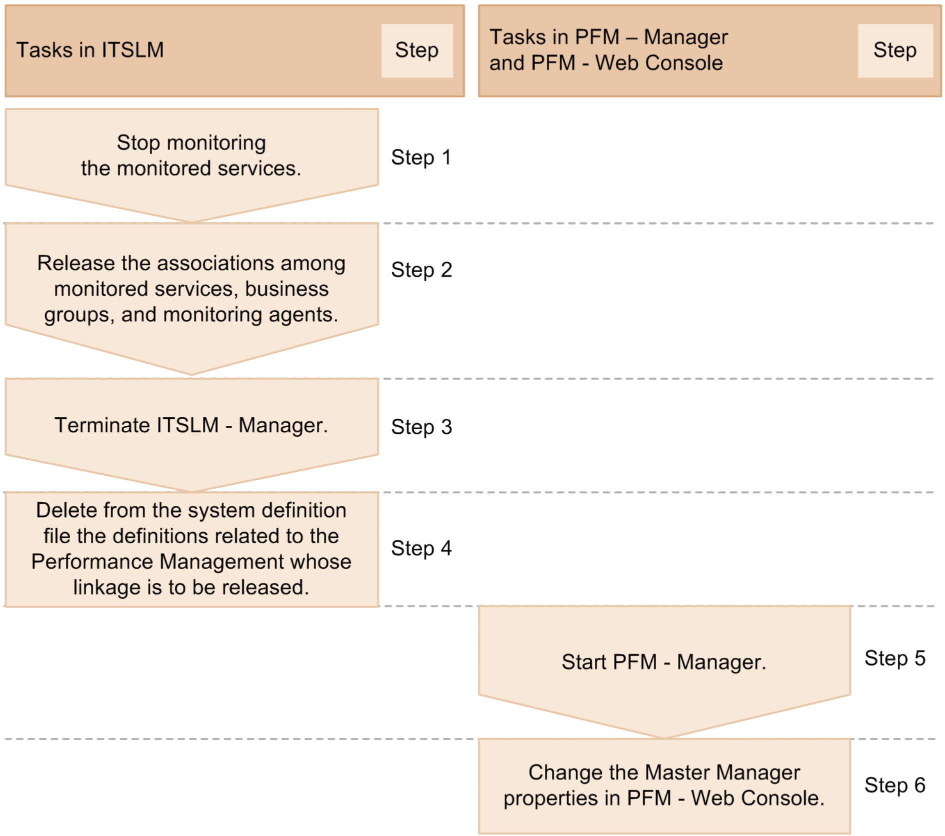
5.4.3 Releasing the linkage between ITSLM and Performance Management (working with Performance Management)

To release the linkage between ITSLM and Performance Management, you must delete the linkage information in both ITSLM and Performance Management.

In ITSLM, delete the linkage information held by ITSLM - Manager. In Performance Management, delete the linkage information held by PFM - Manager and the individual monitoring agents. For details about how to delete linkage information in Performance Management, see the *Job Management Partner 1/Performance Management User's Guide*.

The following figure shows the procedure for releasing the linkage between ITSLM and Performance Management.

Figure 5–17: Procedure for releasing the linkage between ITSLM and Performance Management


Tasks in ITSLM
Step
Tasks in PFM – Manager and PFM - Web Console
Step
Stop monitoring the monitored services.
Step 1
Release the associations among monitored services, business groups, and monitoring agents.
Step 2
Terminate ITSLM - Manager.
Step 3
Delete from the system definition file the definitions related to the Performance Management whose linkage is to be released.
Step 4
Start PFM - Manager.
Step 5
Change the Master Manager properties in PFM - Web Console.
Step 6

(1) Before you start

- Check if ITSLM is running. If ITSLM is not running, start the procedure from step 4.
- Verify that you have the service group administrator permissions. If you do not have the service group administrator permissions, request the service group administrator to perform step 1.
- Verify that monitoring of the services for which the association with Performance Management's business groups and monitoring agents is to be released is stopped.
  For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

- If monitoring of the services for which the association with Performance Management's business groups and monitoring agents is to be released is underway (not stopped), verify that PFM - Manager is running.

  For details about how to start PFM - Manager, see the description about starting and terminating Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

(2) Procedure

To release the linkage between ITSLM and Performance Management:

1. If the services for which the association with Performance Management's business groups and monitoring agents is to be released are currently being monitored, stop the monitoring.

   For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

2. In ITSLM, release all associations between monitored services and business groups and between monitored services and Performance Management's monitoring agents.

   In the **Configuration information settings** area of the Settings window, release the associations between monitored services and business groups and monitoring agents. For details about how to display the **Configuration information settings** area, see *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)*.

3. Terminate ITSLM - Manager.

   For details about the termination method, see *2.1.4 Terminating ITSLM - Manager*.

4. In ITSLM - Manager's system definition file (`jp1itslm.properties`), delete the following property values:

   - `pfmManagerHost` (PFM-Manager's host name)
   - `pfmManagerPort` (PFM-Manager's port number)
   - `pfmWebConsoleURL` (URL of PFM - Web Console that is started from ITSLM)
   - `pfmReceivePort` (Port number used by ITSLM - Manager to receive performance data)

   ITSLM - Manager's system definition file is stored at the following location:

   ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`

5. If PFM - Manager is stopped, start it.

   For details about how to start PFM - Manager, see the description about starting and terminating Performance Management in the *Job Management Partner 1/Performance Management User's Guide*.

6. In PFM - Web Console, change the Master Manager properties.

   For details about changing properties in PFM - Web Console, see the *Job Management Partner 1/Performance Management User's Guide*.

The procedure performed in ITSLM to release the linkage with Performance Management is now complete.

If you skipped step 2 and performed step 3 and the subsequent steps, perform step 1 after you have deleted and changed the ITSLM and Performance Management definitions.

(3) Related topics

- *2.1.4 Terminating ITSLM - Manager*
- *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)*

5.5 Settings for reporting monitoring results by email (working with JP1/IM)

If you link ITSLM with *JP1/IM* (JP1/IM - Manager and JP1/IM - View), you can use JP1/IM functions, including notification of monitoring results by email. This linking is optional. Evaluate whether you need to link with JP1/IM.

This section explains how to link with JP1/IM and provides details of the JP1 events that are needed to set up JP1/IM's automated actions.

For details about automated actions, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

System configuration when ITSLM is linked with Performance Management

One ITSLM - Manager can connect to one JP1/IM - Manager. One ITSLM - Manager can connect to one PFM - Manager. Therefore, if you link ITSLM with JP1/IM and Performance Management, you need one JP1/IM - Manager and one PFM - Manager for each ITSLM - Manager.

5.5.1 Linking with JP1/IM

ITSLM uses JP1/Base functions and issues JP1 events in the following cases:

- Events to be reported to monitoring persons occurred on monitored services
- Events to be reported to system operators occurred in ITSLM

The JP1 events are forwarded to JP1/IM - Manager if their forwarding settings are specified in JP1/Base's forwarding settings file. The JP1 events can then be monitored centrally from JP1/IM - View's Event Console window.

Also, if you set up automated actions in JP1/IM - Manager, you can automate notification of monitoring results by using emails and alarms to report JP1 events.

For details about the forwarding settings, see the *Job Management Partner 1/Base User's Guide*. For details about automated actions, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

This subsection explains how to link ITSLM with JP1/IM.

(1) Before you start

- Verify that setup of ITSLM - Manager has been completed.

  For details about the setup method, see *5.1.6 Setting up ITSLM - Manager*.
- Install JP1/IM.

  There is no need to install JP1/IM on the host on which ITSLM - Manager is installed. For details about how to install JP1/IM, see the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(2) Procedure

To link with JP1/IM:

1. In ITSLM - Manager's system definition file (`jp1itslm.properties`), set the `JP1Event` property to `true`.

   Edit ITSLM - Manager's system definition file. The system definition file is stored at the following location:

ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`

2. Copy ITSLM - Manager's definition file for extended event attributes to JP1/IM - Manager's folder.

   ITSLM - Manager's source file for Japanese language environment:

   ITSLM-Manager-installation-folder`\mgr\conf\event\jp1imm\ja\hitachi_jp1_itslm_attr_sys_ja.conf`

   ITSLM - Manager's source file for English language environment:

   ITSLM-Manager-installation-folder`\mgr\conf\event\jp1imm\en\hitachi_jp1_itslm_attr_sys_en.conf`

   JP1/IM - Manager's target folder:

   JP1/IM-Manager-installation-folder`\conf\console\attribute\`

   If you are using JP1/IM - Manager in a cluster environment, replace *JP1/IM-Manager-installation-folder* with *shared-folder*`\jp1cons`.

3. Restart JP1/IM - Manager.

   The definition change that has been made is not applied until JP1/IM - Manager is restarted.

The setup for linking with JP1/IM is now complete.

(3) Supplementary information

- The table below lists the JP1 events that are issued by ITSLM. For details about the attributes of the JP1 events, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Table 5–6: List of JP1 events

Event ID	Timing of event issuance	Message ID
`0x00006810`	ITSLM - Manager has started.	`KNAS02007-I`
`0x00006811`	ITSLM - Manager has terminated.	`KNAS02008-I`
`0x00006812`	ITSLM - Manager terminated abnormally.	`KNAS02009-E`
`0x00006890`#	Trend monitoring detected a trend in service performance that might lead to an overage of a threshold.	`KNAS34000-W`
`0x00006891`#	Threshold value monitoring detected that service performance has exceeded a threshold.	`KNAS34001-E`
`0x00006892`#	An out-of-range value that is significantly different from the baseline was detected during out-of-range value detection.	`KNAS34002-W`
`0x00006893`#	SLO monitoring detected a trend in system performance that might lead to an overage of an SLO threshold.	`KNAS34009-W`
`0x00006894`#	Threshold value monitoring detected that system performance has exceeded the upper-limit threshold value. Threshold value monitoring detected that system performance has dropped below the lower-limit threshold value.	`KNAS34008-E`
`0x00006895`#	A system performance value that is significantly different from the baseline was detected during predictive error detection.	`KNAS34010-W`

#: JP1 events are issued when system performance exceeds a threshold if the `JP1Event` and `JP1EventForSystem` properties are set to `true` in ITSLM - Manager's system definition file (`jp1itslm.properties`).

(4) Related topics

- *5.5.2 Details of JP1 events*
- *5.6.1 Editing the system definition files*

5.5.2 Details of JP1 events

This subsection provides the details of the JP1 events by event ID.

For details about the attributes of the JP1 events, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(1) Details of 0x00006810

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006810`

		Message	--	`KNAS02007-I`
				`The ITSLM - Manager service has started.`

Extended attribute	Common information	Severity	`SEVERITY`	`Information`
		User name	`USER_NAME`	`SYSTEM`
		Product name	`PRODUCT_NAME`	`"/HITACHI/JP1/ITSLM"`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`ITSLM`
		Root object type	`ROOT_OBJECT_TYPE`	`SERVICE`
		Root object name	`ROOT_OBJECT_NAME`	`ITSLM`
		Occurrence	`OCCURRENCE`	`START`
	Program-specific information	ITSLM - Manager host name	`ITSLM_TARGET_HOST`	Name of the ITSLM - Manager host
		ITSLM - Manager host port number	`ITSLM_PORT`	Port number of the ITSLM - Manager host

Legend:
--: Not applicable

(2) Details of event ID 0x00006811

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006811`

		Message	--	`KNAS02008-I`
				`The ITSLM - Manager service has stopped.`

Extended attribute	Common information	Severity	`SEVERITY`	`Information`
		User name	`USER_NAME`	`SYSTEM`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Product name	PRODUCT_NAME	"/HITACHI/JP1/ITSLM"
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	ITSLM
		Root object type	ROOT_OBJECT_TYPE	SERVICE
		Root object name	ROOT_OBJECT_NAME	ITSLM
		Occurrence	OCCURRENCE	END
		Start time	START_TIME	Time execution started or restarted (number of seconds from UTC 1970-01-01 00:00:00)
	Program-specific information	ITSLM - Manager host name	ITSLM_TARGET_HOST	Name of the ITSLM - Manager host
		ITSLM - Manager host port number	ITSLM_PORT	Port number of the ITSLM - Manager host

Legend:

--: Not applicable

(3) Details of event ID 0x00006812

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0x00006812
		Message	--	KNAS02009-E An ITSLM - Manager service has not started due to an error.
Extended attribute	Common information	Severity	SEVERITY	Error
		User name	USER_NAME	SYSTEM
		Product name	PRODUCT_NAME	"/HITACHI/JP1/ITSLM"
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	ITSLM
		Root object type	ROOT_OBJECT_TYPE	SERVICE
		Root object name	ROOT_OBJECT_NAME	ITSLM
		Occurrence	OCCURRENCE	• When an error occurred while starting services: • NOTSTART • When an error occurred while stopping services: • END
		Start time	START_TIME	Time execution started or restarted (number of seconds from UTC 1970-01-01 00:00:00)
	Program-specific information	ITSLM - Manager host name	ITSLM_TARGET_HOST	Name of the ITSLM - Manager host

Attribute type		Item	Attribute name	Contents
Extended attribute	Program-specific information	ITSLM - Manager host port number	`ITSLM_PORT`	Port number of the ITSLM - Manager host

Legend:

--: Not applicable

(4) Details of event ID 0x00006890

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006890`
		Message	--	`KNAS34000-W` `The SLO threshold might be exceeded. Monitor item =` *monitoring-item-name*
Extended attribute	Common information	Severity	`SEVERITY`	`Warning`
		User name	`USER_NAME`	`SYSTEM`
		Product name	`PRODUCT_NAME`	`"/HITACHI/JP1/ITSLM"`
		Object type	`OBJECT_TYPE`	`PRODUCT`
		Object name	`OBJECT_NAME`	`TREND`
		Root object type	`ROOT_OBJECT_TYPE`	`PRODUCT`
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Service group name	`SERVICE_GROUP_NAME`	Name of the service group for which a trend towards an overage of a threshold was detected
		Monitored service name	`TARGET_SERVICE_NAME`	Name of the monitored service for which a trend towards an overage of a threshold was detected
		Monitored target name	`TARGET_NAME`	• When a trend towards overage of a threshold was detected while monitoring All Web Access: `All Web Access` • When a trend towards overage of a threshold was detected while monitoring a Web transaction: *web-transaction-name*

Legend:

--: Not applicable

(5) Details of event ID 0x00006891

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006891`
		Message	--	`KNAS34001-E` `An SLO violation was detected. Monitor item =` *monitoring-item-name*

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Severity	`SEVERITY`	`Error`
		User name	`USER_NAME`	`SYSTEM`
		Product name	`PRODUCT_NAME`	`"/HITACHI/JP1/ITSLM"`
		Object type	`OBJECT_TYPE`	`PRODUCT`
		Object name	`OBJECT_NAME`	`THRESHOLD`
		Root object type	`ROOT_OBJECT_TYPE`	`PRODUCT`
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Service group name	`SERVICE_GROUP_NAME`	Name of the service group in which an overage of a threshold was detected
		Monitored service name	`TARGET_SERVICE_NAME`	Name of the monitored service in which an overage of a threshold was detected
		Monitored target name	`TARGET_NAME`	• When an overage of a threshold was detected while monitoring All Web Access: `All Web Access` • When an overage of a threshold was detected while monitoring a Web transaction: *web-transaction-name*

Legend:

--: Not applicable

(6) Details of event ID 0x00006892

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006892`
		Message	--	`KNAS34002-W` `A warning sign of performance error was detected. Monitor item =` *monitoring-item-name*
Extended attribute	Common information	Severity	`SEVERITY`	`Warning`
		User name	`USER_NAME`	`SYSTEM`
		Product name	`PRODUCT_NAME`	`"/HITACHI/JP1/ITSLM"`
		Object type	`OBJECT_TYPE`	`PRODUCT`
		Object name	`OBJECT_NAME`	`OUTLIER`
		Root object type	`ROOT_OBJECT_TYPE`	`PRODUCT`
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Service group name	`SERVICE_GROUP_NAME`	Name of the service group in which a warning sign was detected

Attribute type		Item	Attribute name	Contents
Extended attribute	Program-specific information	Monitored service name	`TARGET_SERVICE_NAME`	Name of the monitored service in which a warning sign was detected
		Monitored target name	`TARGET_NAME`	• When a warning sign was detected while monitoring All Web Access: `All Web Access` • When a warning sign was detected while monitoring a Web transaction: *web-transaction-name*

Legend:

--: Not applicable

(7) Details of event ID 0x00006893

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006893`
		Message	--	`KNAS34009-W` `An SLO threshold value might be exceeded. service group name=`*service-group-name*`, service name=`*service-name*`, host name=`*name-of-host-from-which-monitoring-item-is-to-be-obtained*`, monitored target name=`*name-of-agent-that-acquired-monitoring-item*`, monitor item name=`*name-of-monitoring-item*`, occurrence time=`*time-of-occurrence*`, details=`*details* *details* displays in the following format the time at which the threshold is expected to be exceeded: *YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss ZZZZZ* *YYYY*`/`*MM*`/`*DD*: Year, month, date *hh*`:`*mm*`:`*ss*: Hour, minute, second *ZZZZZ*: `+` or `-` followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.
Extended attribute	Common information	Severity	`SEVERITY`	`Warning`
		User name	`USER_NAME`	`SYSTEM`
		Product name	`PRODUCT_NAME`	`"/HITACHI/JP1/ITSLM"`
		Object type	`OBJECT_TYPE`	`PRODUCT`
		Object name	`OBJECT_NAME`	`TREND`
		Root object type	`ROOT_OBJECT_TYPE`	`PRODUCT`
		Occurrence	`OCCURRENCE`	`NOTICE`

Attribute type		Item	Attribute name	Contents
Extended attribute	Program-specific information	Service group name	`SERVICE_GROUP_NAME`	Name of the service group in which a trend was detected
		Monitored service name	`TARGET_SERVICE_NAME`	Name of the monitored service in which a trend was detected
		Name of the host from which the monitoring item is to be obtained	`PFM_TARGET_HOST`	Name of the host from which to obtain the monitoring item in which a trend was detected
		Monitored target name	`TARGET_NAME`	Name of the agent that acquired the monitoring item in which a trend was detected
		Monitoring item name	`METRIC_NAME`	Name of the monitoring item in which a trend was detected

Legend:

--: Not applicable

(8) Details of event ID 0x00006894

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	`0x00006894`
		Message	--	`KNAS34008-E` `An SLO violation was detected. service group name=`*service-group-name*`, service name=`*service-name*`, host name=`*name-of-host-from-which-monitoring-item-is-to-be-obtained*`, monitored target name=`*name-of-agent-that-acquired-monitoring-item*`, monitor item name=`*name-of-monitoring-item*`, occurrence time=`*time-of-occurrence*`, details=`*details* *details* displays one of the following values: `UPPER LIMIT`: The value exceeds the upper limit. `LOWER LIMIT`: The value drops below the lower limit.
Extended attribute	Common information	Severity	`SEVERITY`	`Error`
		User name	`USER_NAME`	`SYSTEM`
		Product name	`PRODUCT_NAME`	`"/HITACHI/JP1/ITSLM"`
		Object type	`OBJECT_TYPE`	`PRODUCT`
		Object name	`OBJECT_NAME`	`THRESHOLD`
		Root object type	`ROOT_OBJECT_TYPE`	`PRODUCT`
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Service group name	`SERVICE_GROUP_NAME`	Name of the service group in which a threshold overage was detected
		Monitored service name	`TARGET_SERVICE_NAME`	Name of the monitored service in which a threshold overage was detected

Attribute type		Item	Attribute name	Contents
Extended attribute	Program-specific information	Name of the host from which the monitoring item is to be obtained	PFM_TARGET_HOST	Name of the host from which to obtain the monitoring item in which an exceeded threshold was detected
		Monitored target name	TARGET_NAME	Name of the agent that acquired the monitoring item in which a threshold overage was detected
		Monitoring item name	METRIC_NAME	Name of the monitoring item in which a threshold overage was detected

Legend:

--: Not applicable

(9) Details of event ID 0x00006895

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0x00006895
		Message	--	KNAS34010-W A sign of a performance error was detected. service group name=*service-group-name*, service name=*service-name*, host name=*name-of-host-from-which-monitoring-item-is-to-be-obtained*, monitored target name=*name-of-agent-that-acquired-monitoring-item*, monitor item name=*name-of-monitoring-item*, occurrence time=*time-of-occurrence*, details=*details* *details* displays one of the following values: UPPER LIMIT: The value exceeds the upper limit from the baseline. LOWER LIMIT: The value drops below the lower limit from the baseline.
Extended attribute	Common information	Severity	SEVERITY	Warning
		User name	USER_NAME	SYSTEM
		Product name	PRODUCT_NAME	"/HITACHI/JP1/ITSLM"
		Object type	OBJECT_TYPE	PRODUCT
		Object name	OBJECT_NAME	OUTLIER
		Root object type	ROOT_OBJECT_TYPE	PRODUCT
		Occurrence	OCCURRENCE	NOTICE
	Program-specific information	Service group name	SERVICE_GROUP_NAME	Name of the service group in which a warning was detected
		Monitored service name	TARGET_SERVICE_NAME	Name of the monitored service in which a warning was detected
		Name of the host from which the monitoring item is to be obtained	PFM_TARGET_HOST	Name of the host from which to obtain the monitoring item in which a warning was detected

Attribute type		Item	Attribute name	Contents
Extended attribute	Program-specific information	Monitored target name	`TARGET_NAME`	Name of the agent that acquired the monitoring item in which a warning was detected
		Monitoring item name	`METRIC_NAME`	Name of the monitoring item in which a warning was detected

Legend:

--: Not applicable

5.6 Editing the system definition files to change settings

ITSLM enables you to change settings, including host names and port numbers, by editing ITSLM - Manager's system definition file (`jp1itslm.properties`) and ITSLM - UR's system definition file (`jp1itslmur.properties`).

This section explains how to edit the system definition files and the definitions that can be edited.

5.6.1 Editing the system definition files

This subsection explains how to edit ITSLM's system definition files (`jp1itslm.properties` and `jp1itslmur.properties`).

(1) Before you start

- Terminate the ITSLM - Manager or ITSLM - UR whose system definition file you will be editing.
  For details about the termination method, see *2.1.4 Terminating ITSLM - Manager* or *2.1.3 Terminating ITSLM - UR*.

(2) Procedure

To edit a system definition file:

1. Edit the system definition file.
   The system definition file is stored at the following location:

   For ITSLM - Manager:

   ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`

   For ITSLM - UR:

   ITSLM-UR-installation-folder`\ur\conf\jp1itslmur.properties`

   For a list of the definitions that can be edited, see *5.6.2 Editable definitions*.

   If you are editing properties that are common to both ITSLM - Manager and ITSLM - UR, make sure that you edit both system definition files.

2. Start the ITSLM - Manager or ITSLM - UR whose system definition file has been edited.
   For details about how to start ITSLM - Manager or ITSLM - UR, see *2.1.1 Starting ITSLM - Manager* or *2.1.2 Starting ITSLM - UR*.

The system definition file has been edited and the ITSLM settings have been changed.

(3) Supplementary information

- A system definition file definition is specified in the following format:

```
property=value
```

- Use ISO/IEC 646 character codes for system definition files; do not use Unicode characters. Do not include any Unicode escape sequences.
- Changes made to a system definition file are not applied until the next time ITSLM - Manager or ITSLM - UR is started (or restarted).

- If an invalid keyword that is not defined in ITSLM is specified in a system definition file, ITSLM ignores the specified keyword and continues processing.
- If an invalid value, such as an out-of-range value, is specified in a system definition file, the target ITSLM - Manager or ITSLM - UR might terminate during startup processing.

  However, for properties related to output of logs (properties beginning with `logger`), a specified invalid value, such as an out-of-range value, will be changed to the default value and ITSLM - Manager or ITSLM - UR processing will continue.
- Paths specified in a definition file cannot exceed 100 characters. The following characters can be used:
  - `A` to `Z`, `a` to `z`, `0` to `9`, space, underscore (_), period (`.`), left and right parentheses (`()`), and the path separator character (\)

    Note that two consecutive path separator characters (\\) must be specified, as indicated in the following.

    Example specification: `C:\\Program Files\\HITACHI\\JP1ITSLM\\ur\\accesslog`

  None of the following are permitted:
  - Double-byte characters
  - Characters that Windows does not allow in file or folder names (`\`, `/`, `:`, `*`, `?`, `"`, `<`, `>`, `|`)
  - NTFS stream names that contain a colon (`:`), except as a separator after the drive name
  - Reserved device names (`AUX`, `CON`, `NUL`, `PRN`, `CLOCK$`, `COM1` through `COM9`, `LPT1` through `LPT9`)
  - Folder names that start with `u`
  - Paths that include `#`
  - Paths that end with `\\`
  - Paths on a network drive
- We recommend that you make a backup after you have edited a system definition file.

  For details about how to back up system definition files, see *8.1.1 Backing up the definition files*.
- If you are running ITSLM in a cluster system and change a system definition file, make sure that you make the same changes to the system definition files in both systems to avoid inconsistent settings between the active and standby servers.

(4) Related topics

- *2.2.1 Logging in to ITSLM - Manager*
- *5.4.1 Setting up the linkage between ITSLM and Performance Management (working with Performance Management)*
- *5.4.2 Specifying settings for saving Performance Management's performance data from ITSLM (working with Performance Management)*
- *5.4.3 Releasing the linkage between ITSLM and Performance Management (working with Performance Management)*
- *8.4.1 Renaming the ITSLM - Manager host*
- *8.4.2 Renaming the ITSLM - UR host*
- *8.5.1 Changing ITSLM - Manager's RMI communication port number*
- *8.5.2 Changing ITSLM - UR's RMI communication port number*
- *8.5.3 Changing the listen port number of the ITSLM - Manager embedded database*
- *8.5.4 Changing the listen port number of the ITSLM - Manager embedded Web server*

- *8.5.5 Changing the port number of the internal communications port of the ITSLM - Manager embedded Web server*
- *8.5.6 Changing the port number of the completion-message receiving port of the ITSLM - Manager embedded Web server*
- *8.6 Changing the network interface number*

5.6.2 Editable definitions

Editing definitions is optional in ITSLM.

This subsection explains the definitions that can be edited in ITSLM.

(1) List of definitions that can be edited in ITSLM

The following table explains the definitions that can be edited when it is necessary to do so.

Table 5–7: List of definitions that can be edited in ITSLM

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
1	accessLogFilePath	U	O	Specifies the destination file path for the files in which access logs are recorded.	Absolute path of the folder, including the drive letter[#1]	None	T
2	announceRetryCount	U	O	Specifies the number of retries when a communication error occurs when start or termination is reported from ITSLM - UR to ITSLM - Manager.	Integer from 1 to 20 (count)	3	T
3	announceRetryInterval	U	O	Specifies the retry interval when a communication error occurs when start or termination is reported from ITSLM - UR to ITSLM - Manager.	Integer from 1 to 1000 (seconds)	10	T
4	announceRetryMessage	U	O	Specifies whether the retry message (KNAS03016-W) is to be output to message logs when a communication error occurs when start or termination is reported from ITSLM - UR to ITSLM - Manager.	true (output) or false (do not output)[#2]	false	T
5	communicationRetryCount	M, U	O	Specifies the number of retries when a communication error occurs between ITSLM - UR and ITSLM - Manager.	Integer from 1 to 20 (count)	3	T
6	communicationRetryInterval	M, U	O	Specifies the retry interval when a communication error occurs between ITSLM - UR and ITSLM - Manager.	Integer from 1 to 1000 (seconds)	10	T

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
7	communicationRetryMessage	M, U	O	Specifies whether the retry message (KNAS03016-W) is to be output to message logs when a communication error occurs between ITSLM - UR and ITSLM - Manager.	true (output) or false (do not output)#2	false	T
8	dashboardChartPlotInterval	M	O	Specifies in minutes the maximum interval between dots for drawing a straight line on a performance chart for system performance.	Integer from 1 to 1440	5	T
9	dashboardEventListRecentViewSize	M	O	Specifies the maximum number of events that can be displayed at the same time when events of multiple services are listed in an ITSLM window. The specified number of the most recent events are displayed.	Integer from 1 to 8192	1000	T
10	dashboardPrioritizeSystem	M	O	Changes the default display for the following windows according to the monitoring configuration: • Add template window • **Add/Delete monitor** area in the Settings window	true (default display for a system monitoring configuration) or false (default display for a service monitoring configuration)	false	T
11	dashboardPropagateSystemStatus	M	O	Specifies whether the system performance monitoring status is to be propagated to the service status.	true (propagate) or false (do not propagate)	false	T
12	jbsHostName	M	O	Specifies the local host name of JP1/Base. Specification of this property is required when JP1/Base is run with a cluster configuration.	Character string with a length of 1 to 196 bytes (permitted characters include alphanumeric characters and hyphen (-))	None	T
13	JP1Event	M	O	Specifies whether issuance of JP1 events is to be enabled. Specification of this property is required when ITSLM is linked with JP1/IM. For details about linking with JP1/IM, see *5.5.1 Linking with JP1/IM*.	true (issue) or false (do not issue)#2	false	D
14	JP1EventForSystem	M	O	Specifies whether JP1 events for system performance are to be issued when the JP1Event property is set to true and ITSLM is linked to Performance Management.	true (issue JP1 events) or false (do not issue JP1 events)	false	T

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
15	loggerCommandMessageFileCount	M	O	Specifies the maximum number of message log files for commands.	Integer from 2 to 16	3	D
16	loggerCommandMessageMaxFileSize	M	O	Specifies the maximum size of a message log file for commands.	Integer from 4096 to 16777216 (bytes)	1048576 (1 MB)	D
17	loggerDaoMessageFileCount	M	O	Specifies the maximum number of message log files that are used by the ITSLM function to access the database.	Integer from 2 to 16	3	D
18	loggerDaoMessageMaxFileSize	M	O	Specifies the maximum size of a message log file that is used by the ITSLM function to access the database.	Integer from 4096 to 2147483647 (bytes)	1048576 (1 MB)	D
19	loggerInputAdaptorCtrlMessageFileCount	M	O	Specifies the maximum number of message log files that are used by the ITSLM function to receive performance data from external programs.	Integer from 2 to 16	3	D
20	loggerInputAdaptorCtrlMessageMaxFileSize	M	O	Specifies the maximum size of a message log file that is used by the ITSLM function to receive performance data from external programs.	Integer from 4096 to 2147483647 (bytes)	1048576 (1 MB)	D
21	loggerIntegrationLogLevel	M, U	O	Specifies the log output level for integrated trace logs. A small value decreases the amount of output information, and a large value increases the amount of output information increases.	0, 10, 20, or 30	10	D
22	loggerMessageLogLevel	M, U	O	Specifies the log output level for message log files. A small value decreases the amount of output information, and a large value increases the amount of output information increases.	0, 10, 20, or 30	10	D
23	loggerPerfCollectorMessageFileCount	M	O	Specifies the maximum number of message log files for the performance analysis manager.	Integer from 2 to 16	3	D
24	loggerPerfCollectorMessageMaxFileSize	M	O	Specifies the maximum size of a message log file for the performance analysis manager.	Integer from 4096 to 2147483647 (bytes)	1048576 (1 MB)	D

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
25	`loggerProcessCtrlMessageFileCount`	M, U	O	Specifies the maximum number of message log files for process control.	Integer from `2` to `10`	`3`	D
26	`loggerProcessCtrlMessageMaxFileSize`	M, U	O	Specifies the maximum size of a message log file for process control.	Integer from `4096` to `16777216` (bytes)	`1048576` (1 MB)	D
27	`loggerRmiServerMessageFileCount`	M, U	O	Specifies the maximum number of message log files for the RMI server.	Integer from `2` to `16`	`3`	D
28	`loggerRmiServerMessageMaxFileSize`	M, U	O	Specifies the maximum size of a message log file for the RMI server.	Integer from `4096` to `2147483647` (bytes)	`1048576` (1 MB)	D
29	`loggerUserResponseMessageFileCount`	M, U	O	Specifies the maximum number of message log files for UR control.	Integer from `2` to `16`	`3`	D
30	`loggerUserResponseMessageMaxFileSize`	M, U	O	Specifies the maximum size of a message log file for UR control.	Integer from `4096` to `2147483647` (bytes)	`1048576` (1 MB)	D
31	`loggerViewMessageFileCount`	M	O	Specifies the maximum number of message log files for a servlet.	Integer from `2` to `16`	`3`	D
32	`loggerViewMessageMaxFileSize`	M	O	Specifies the maximum size of a message log file for a servlet.	Integer from `4096` to `2147483647` (bytes)	`1048576` (1 MB)	D
33	`loggerWebSystemAnalysisMessageFileCount`	U	O	Specifies the maximum number of message log files for the Web system analysis process and service detection process.	Integer from `2` to `16`	`3`	D
34	`loggerWebSystemAnalysisMessageMaxFileSize`	U	O	Specifies the maximum size of a message log file for the Web system analysis process and service detection process.	Integer from `4096` to `2147483647` (bytes)	`1048576` (1 MB)	T
35	`loginFailedLimit`	M	O	Specifies the number of retries allowed in ITSLM's login window. Once the specified number of retries have been used, the window is locked. If `0` is specified, the window will not be locked.	Integer from `0` to `30`	`3`	T
36	`managerHost`	M, U	R	Specifies the host name of ITSLM - Manager. If ITSLM is linked with Performance Management,	ASCII codes `0x20` to `0x7e` (excluding control characters) and a length of 1 to 256 bytes (permitted	None	T

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
36	managerHost	M, U	R	an IP address cannot be specified (you must specify the host name).	number of bytes depends on Windows). Characters that are not permitted in host names in Windows cannot be specified. None of the following addresses can be specified: • 0.0.0.0 • 127.0.0.1 • 255.255.255.255	None	T
37	managerStartMode	M	O	Specifies the start mode for restarting the Windows service in ITSLM - Manager.	normal (starting the Windows service with monitoring stopped) or restart (starting the Windows service with restart of the monitoring that was running before the Windows service stopped)#2	normal	T
38	monitoringItemNameMaxLength	M	O	Specifies the length of a monitoring item name. Specify the number of bytes obtained after UTF-8 conversion.	Integer from 1 to 1024 (bytes)	300	T
39	outlierRate	M	O	Specifies the percentage of performance data in the monitoring range that has to result in an out-of-range value before an event is reported during predictive error detection.	Integer from 1 to 100 (%)	10	T
40	pfmLoggingData	M	O	Specifies whether Performance Management's monitoring agents are to store performance data in the Store database.	true (store in the Store database) or false (do not store in the Store database)#2	false	T
41	pfmManagerHost	M	O	Specifies the host name of the PFM - Manager that is to be linked with ITSLM. If the specified host name is invalid, communication with Performance Management will fail.	ASCII codes 0x20 to 0x7e (excluding control characters) with a length of 1 to 256 bytes (permitted number of bytes depends on Windows). Characters that are not permitted in host names in Windows cannot be specified. None of the following addresses can be specified: • 0.0.0.0 • 127.0.0.1	None	T

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
41	`pfmManagerHost`	M	O	Specifies the host name of the PFM - Manager that is to be linked with ITSLM. If the specified host name is invalid, communication with Performance Management will fail.	• `255.255.255.255`	None	T
42	`pfmManagerPort`	M	O	Specifies the port number of PFM - Manager that is to be linked with ITSLM. If the specified port number is invalid, communication with Performance Management will fail.	`1024` to `65535`	`22286`	T
43	`pfmReceivePort`	M	O	Specifies the port number used by ITSLM - Manager to receive performance data sent from Performance Management.	`1024` to `65535`	`20905`	T
44	`pfmWebConsoleURL`	M	O	Specifies the URL of the target PFM - Web Console. Specify the URL without the URL encoding (percent encoding). The following shows an example: `http://`*host*`:`*port*`/PFMWebConsole/login.do` *host*: Host name or IP address *port*: Port number The value specified for URL must be in RFC 2396-compliant format.	Character string with a length of 0 to 1024 (characters)	None	T
45	`rdbPort`	M	O	Specifies the listen port number of the embedded database.	`5001` to `65535`	`20903`	T
46	`rmiManagerPort`	M, U	O	Specifies the RMI communication port number of ITSLM - Manager.	`5001` to `65535`	`20904`	T
47	`rmiUrPort`	U	O	Specifies the RMI communication port number of ITSLM - UR.	`5001` to `65535`	`20910`	T
48	`serviceBaselineExclusion`	M	O	Specifies whether out-of-range value detection events that are opposite to the threshold direction are to be excluded during predictive error detection for service performance.	`true` (exclude) or `false` (do not exclude)	`false`	T
49	`sloThresholdRate`	M	O	Specifies the percentage of performance data in the monitoring range that has to	Integer from `1` to `100` (%)	`10`	T

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
49	sloThresholdRate	M	O	result in an overage of a threshold before an event is reported by threshold value monitoring.	Integer from 1 to 100 (%)	10	T
50	systemBaselineExclusion	M	O	Specifies whether out-of-range value detection events that are opposite to the threshold direction are to be excluded for the threshold type that is received from Performance Management during predictive error detection for system performance. For example, if the threshold type received from Performance Management is the upper limit, this property specifies whether lower-limit events are to be excluded in out-of-range value detection.	true (exclude) or false (do not exclude)	false	T
51	urHost	U	R	Specifies the host name of ITSLM - UR.	ASCII codes 0x20 to 0x7e (excluding control characters) and a length of 1 to 256 bytes (permitted number of bytes depends on Windows). Characters that are not permitted in host names in Windows cannot be specified. None of the following addresses can be specified: • 0.0.0.0 • 127.0.0.1 • 255.255.255.255	None	T
52	urNetworkInterfaceNumber	U	R	Specifies the network interface number assigned by the capture module. If you have changed the network interface configuration on the host on which ITSLM - UR is installed, make sure that you use the jslmuripls command to check and, if necessary, revise the specified value. For details about the jslmuripls command, see *jslmuripls (displays network interface number and IP address)* in *9. Commands*.	Integer from 1 to 60. An error results if the specified network interface number does not exist in the jslmuripls command execution results.	None	

Legend:

Trgt: Target

Spec: Specification

M: ITSLM - Manager

U: ITSLM - UR

R: Specification is required

O: Specification is optional

D: If there is an error in the setting, ITSLM - Manager or ITSLM - UR assumes the default value upon startup.

T: If there is an error in the setting, ITSLM - Manager or ITSLM - UR terminates.

#1

If you want to run ITSLM - UR in a cluster configuration, make sure the path points to a shared disk so the access log will be switched over when node switching occurs.

#2

The value is not case sensitive.

(2) Supplementary information

- The system definition files to be edited (`jp1itslm.properties` or `jp1itslmur.properties`) are stored at the following locations:

  For ITSLM - Manager:

  ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`

  For ITSLM - UR:

  ITSLM-UR-installation-folder`\ur\conf\jp1itslmur.properties`

- The following shows example definitions in the system definition files:

  For ITSLM - Manager:

```
managerHost=192.168.2.109
rmiManagerPort=20904
```

  For ITSLM - UR:

```
managerHost=192.168.2.109
rmiManagerPort=20904
urHost=192.168.2.109
rmiUrPort=20910
urNetworkInterfaceNumber=1
```

- For details about the port numbers used by ITSLM, see *A. List of Port Numbers Used by ITSLM*.

5.7 ITSLM language settings

5.7.1 Browser language settings

By configuring the browser language settings in ITSLM, you can change the language displayed in the browser.

5.7.2 Host language settings

By configuring the language and service settings of a host on which ITSLM is installed, you can change the language of the log data output by ITSLM and by the installer.

(1) Language settings

The following three settings need to be configured:

- User locale
- System locale
- Locale ID of MUI (Multilingual User Interface)#

The above three settings must be set to the same language. If the set language is not the same, ITSLM will output a mix of Japanese and English, and garbled text might be displayed.

#

This setting is necessary only if you are using MUI.

(2) Service settings

For each ITSLM service, you must change the service logon account from the local system account to the user account of the currently logged-in user.

6 Preparations Before Starting (Cluster System)

This chapter explains the preparations before starting ITSLM in a cluster system, including installation, setup, and user settings. This chapter also explains optional preparations, such as linking with JP1/IM to report monitoring results by a means such as email, linking with Performance Management to monitor hosts and middleware providing services, and how to migrate to a cluster system.

The cluster systems considered in this chapter are *node switching systems* whose purpose is to achieve high availability (HA), not cluster systems whose purpose is load distribution.

6.1 Overview of cluster systems

ITSLM - Manager and ITSLM - UR can be run in cluster systems intended for achieving high availability.

A cluster system consists of multiple server systems that are linked together to run as a single system. The purpose of such a system is to ensure seamless operation in the event of a server failure by continuing business operations on another server.

By running ITSLM - Manager in a cluster system, you can continue monitoring the status of services, even when a failure occurs in ITSLM - Manager. If the service performance obtained as monitoring results is managed by using a shared disk, the service performance from before a failure can be inherited.

Running ITSLM - UR in a cluster system makes it possible to continue collecting HTTP packets when a failure occurs in ITSLM - UR.

The overview and components of a cluster system for ITSLM - Manager and ITSLM - UR are the same as for a cluster system supported by JP1/Base. For details, see the *Job Management Partner 1/Base User's Guide* as necessary

6.1.1 Prerequisites for cluster system operations

ITSLM can operate in a logical host environment in a cluster system that supports failover. The prerequisites for running ITSLM in a logical host environment are that the allocation, deletion, and operation monitoring of the shared disk and logical IP addresses must be managed routinely by the cluster software.

ITSLM supports Windows Server Failover Cluster as the cluster software.

Important note

Depending on the system configuration and environment setup, a cluster software program that is supported by ITSLM might not satisfy the prerequisites described here. Evaluate the system configuration and environment setup to make sure that all the prerequisites are satisfied.

(1) Prerequisites for the logical host environment

To run ITSLM in a logical host environment, the following prerequisites for the shared disk and logical IP addresses must be satisfied.

Table 6–1: Prerequisites for the logical host environment

Logical host component	Prerequisites
Shared disk	• A shared disk that can inherit data from the active server to the standby server is available. • The shared disk is allocated before ITSLM is started. • Allocation of the shared disk is not released while ITSLM is running. • Allocation of the shared disk is released after ITSLM has stopped. • The shared disk is controlled in such a manner that it will not be accessed improperly from multiple nodes. • Files are protected by means such as a file system with a journal function so that files are not deleted by events such as system shutdown. • File contents are guaranteed and inherited in the event of a failover. • Forced failover is supported, even while a process is using the shared disk.

Logical host component	Prerequisites
Shared disk	• If a shared disk failure is detected, a program such as cluster software will manage the recovery processing, and there will be no need for ITSLM to be aware of the recovery processing. If ITSLM needs to be started or stopped as an extension of recovery processing, the cluster software must issue the stop and start requests to ITSLM.
Logical IP addresses	• Inheritable logical IP addresses can be used for communication. • A unique logical IP address can be obtained from any logical host name. • The logical IP addresses have been allocated before ITSLM is started. • The logical IP addresses will not be deleted while ITSLM is running. • While ITSLM is running, the correspondence between logical host names and logical IP addresses will not be changed. • The logical IP addresses will be deleted after ITSLM has stopped. • If a network failure is detected, a program such as cluster software will manage the recovery processing, and there will be no need for ITSLM to be aware of the recovery processing. If ITSLM needs to be started or stopped as an extension of recovery processing, the cluster software must issues the stop and start requests to ITSLM.

(2) Prerequisites for the physical host environment

In a cluster system that runs ITSLM on a logical host, each server's physical host environment must satisfy the prerequisites described below.

Table 6–2: Prerequisites for the physical host environment

Physical host component	Prerequisites
Server	• The cluster consists of two server systems. • Sufficient CPU performance is available for the processing that will be performed (for example, if multiple logical hosts are started, there is adequate CPU performance). • Sufficient real memory capacity is available for the processing that will be performed (for example, if multiple logical hosts are started, there is adequate real memory capacity).
Disk	• Files are protected by a means such as a file system with a journal function so that files are not deleted during events such as system shutdown.
Network	• Communications can be performed using IP addresses corresponding to the physical host names (results of the `hostname` command) (a program such as the cluster software is not able to change settings that will disable communications). • While ITSLM is running, the correspondence between host names and IP addresses will not be changed (by programs such as the cluster software or the name server). • A LAN board supporting host names is given the top priority by the network bind settings (no other LAN board, such as one for heartbeat, is given the top priority).
OS and cluster software	• The cluster software and its version are supported by ITSLM. • The patches and service packs required by ITSLM and the cluster software have already been applied. • Each server's environment is set up appropriately so that the same processing can continue in the event of a failover.

(3) Scope of ITSLM support

When ITSLM is run on a logical host in a cluster system, ITSLM controls only itself. The logical host environment (including shared disk allocation and inheritance of logical IP addresses) is managed by the cluster software.

If the prerequisites for the logical host environment and the physical host environment are not satisfied or there is any problem in controlling the logical host environment, ITSLM will not respond to problems that arise from ITSLM operations. For troubleshooting, see the documentation for the cluster software and the OS that control the logical host environment.

6.1.2 ITSLM system configuration in a cluster system

To run ITSLM in a cluster system, the system configuration must satisfy the following conditions:

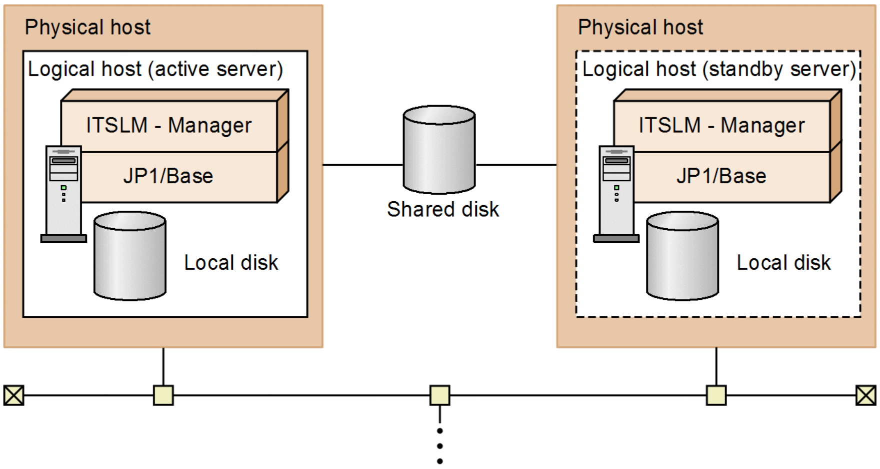
- The logical hosts require a shared disk and logical IP addresses that can be inherited from the active server to the standby server. The shared disk and logical IP addresses must satisfy the conditions described in *6.1.1 Prerequisites for cluster system operations*.
- The same OS must be used throughout the cluster system. Failover between different OSs is not supported.
- The cluster system must have an active-standby configuration.

This following subsections explain the system configuration for running ITSLM - Manager and ITSLM - UR in a cluster system.

(1) System configuration for ITSLM - Manager

This subsection explains a system configuration example for ITSLM - Manager in a cluster system. For details about the system configuration for JP1/Base in a cluster system, see the *Job Management Partner 1/Base User's Guide*. If you run JP1/Base with a cluster configuration, you must specify the logical host name of JP1/Base in the `jbsHostName` property in ITSLM - Manager's system definition file (`jp1itslm.properties`).

Figure 6–1: System configuration example for ITSLM - Manager in a cluster system



ITSLM - Manager places the information that is to be inherited from the active server to the standby server in the event of a failover in shared folders on the shared disk. The files to be placed in the shared folders are created when an environment is set up for ITSLM - Manager on the logical host. If there are no shared folders when an environment is set up for ITSLM - Manager on the logical host, the setup command creates them.

A file system area for the database is placed on the shared disk. The name that is used for the folders is shown below.

Folder name for the database file system area:

shared-folder# `\JP1ITSLM\database`

#

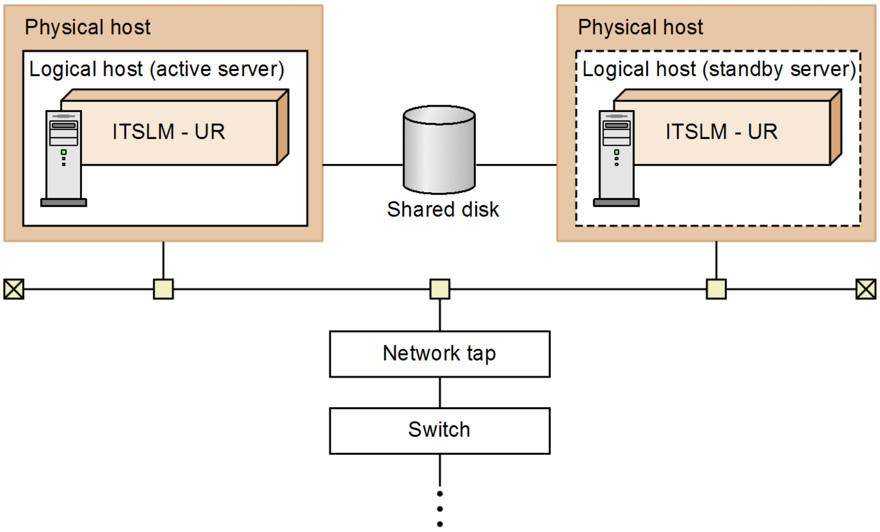
A different shared folder must be specified at setup for each logical host.

Only the ITSLM system information and performance data for monitored services are stored in the database file system area on the shared disk. The other file system areas used by ITSLM are created on local disks of the individual logical hosts.

(2) System configuration for ITSLM - UR

The following figure shows an example of a system configuration for ITSLM - UR in a cluster system.

Figure 6–2: System configuration example for ITSLM - UR in a cluster system



Note that ITSLM - UR uses the shared disk so that any access logs will be switched over to the standby server in the event of a failover. To determine whether a shared disk is required in the system configuration, check the cluster software specifications, as well as the destination path where the files than make up the access logs are to be recorded.

When ITSLM - UR is run in a cluster system, a *network tap* that copies HTTP packets passing through the switch's mirror ports is required between ITSLM - UR and the switch. The network tap copies the HTTP packets that pass the switch and sends them to the individual ITSLM - URs that make up the cluster system.

6.1.3 Failover timing

Failover occurs at the following times:

- When ITSLM detects a failure that results in failover
- When the cluster software detects a failure that results in failover

The table below describes the failures that are detected by ITSLM as resulting in failover. When ITSLM detects such a failure, it terminates the Windows services and notifies the cluster software of the failure.

Table 6–3: Failures detected by ITSLM as resulting in failover

No.	Status	Failure	Description
1	All statuses	Abnormal process termination	An ITSLM process terminated abnormally.
2		Memory shortage	A memory shortage occurred in ITSLM. This results in the same status as 1 above because the corresponding process terminates abnormally.

No.	Status	Failure	Description
3	Monitoring of services is underway	Communication error	A communication error occurred while ITSLM was monitoring services and all retry attempts failed. This results in the same status as 1 above because the source process terminates abnormally.
4		Database access error#	A database access error occurred while ITSLM was monitoring services and all retry attempts failed. This results in the same status as 1 above because the source process terminates abnormally.

#

Not applicable to ITSLM - UR.

The failures detected by the cluster software depend on cluster software specifications. For details, see the cluster software documentation.

6.1.4 Status after failover

This subsection explains the monitoring status after failover that occurred when ITSLM was monitoring or detecting monitored services.

(1) Status of monitoring of monitored services before and after failover

If failover occurs while ITSLM is monitoring monitored services, the monitoring continues.

The following table shows the status of monitoring of monitored services before and after failover.

Table 6–4: Status of monitoring of monitored services before and after failover

No.	Monitoring status before failover	Monitoring status after failover	
		Failover that occurs on ITSLM - Manager	Failover that occurs on ITSLM - UR
1	**Start**	**Start**	**Start**
2	**Stop**	**Stop**	**Stop**
3	**Starting**		**Stop**#1
4	**Stopping**	**Start**	**Start**#2

#1

If failover of ITSLM - UR is completed before a monitoring start instruction is sent from ITSLM - Manager to ITSLM - UR since the user initiated monitoring start processing, the monitoring start processing continues.

#2

If failover of ITSLM - UR is completed before a monitoring stop instruction is sent from ITSLM - Manager to ITSLM - UR since the user initiated monitoring stop processing, the monitoring stop processing continues.

If failover occurs on ITSLM - Manager, the following information is inherited to the target environment after failover:

- Service performance displayed in the Home window or Real-time Monitor window is not restored in the target environment after failover; this includes the icons indicating the status of services, response times being monitored, throughput, and error rate values. If ITSLM is linked with Performance Management, the system performance is also not restored in the target environment after failover; this includes the icons indicating the status of monitoring items, measurement values of monitoring items, and availability monitoring status. The purpose of this is minimize the amount of time required for failover processing because it takes time to load service performance into memory.

- ITSLM cannot monitor services while failover processing is underway. If failover occurs on ITSLM - Manager or ITSLM - UR while services are being monitored, service performance is not collected while the failover processing is underway, and service performance for that period will be missing.

(2) Status of detecting monitored services before and after failover

If failover occurs while ITSLM is detecting monitored services, the detection status depends on whether failover occurred on ITSLM - Manager or ITSLM - UR and the number of ITSLM - URs in the system that are detecting monitored services.

The following table shows the status of detecting monitored services before and after failover.

Table 6–5: Status of detecting monitored services before and after failover

No.	Detection status before failover	Detection status after failover	
		Failover that occurs on ITSLM - Manager	Failover that occurs on ITSLM - UR
1	**Detecting**	**Stopped**	**Detecting** or **Stopped**#
2	**Stopped**		**Stopped**

#

When failover occurs on ITSLM - UR while it is detecting monitored services, the detection processing is not restarted on the ITSLM - UR resulting in failover. If one or more ITSLM - URs are detecting monitored services in the system configuration in addition to the one resulting in failover, the status is **Detecting**.

If there are no more ITSLM - URs detecting monitored services other than the one resulting in failover, the status is **Stopped**.

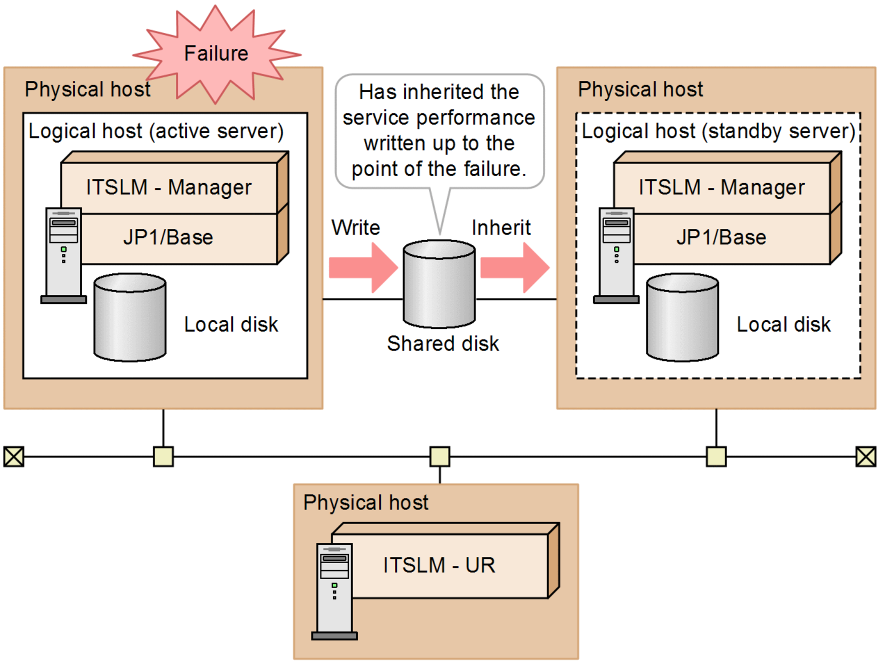
If failover occurs simultaneously on both ITSLM - Manager and ITSLM - UR, the status after failover of detecting monitored services is **Stopped**.

6.1.5 Processing performed when failover occurs on ITSLM - Manager

When failover occurs on ITSLM - Manager, the service performance information that has been written onto the shared disk by ITSLM - Manager on the active server up to that point is inherited by ITSLM - Manager on the standby server. The standby server resumes business operations on the basis of the inherited information. However, monitored-service detection processing is not resumed.

The following figure shows the processing that is performed when failover occurs on ITSLM - Manager.

Figure 6–3: Processing when failover occurs on ITSLM - Manager



When failover occurs, the service performance is inherited, but the icons indicating error and warning statuses displayed on the window are not inherited. When the service is restarted after failover processing, the service performance is re-analyzed and the appropriate icons are displayed based on the analysis results.

The following subsections explain the failover processing flows depending on the timing of the failover.

(1) While neither monitoring nor detection of monitored services is being performed

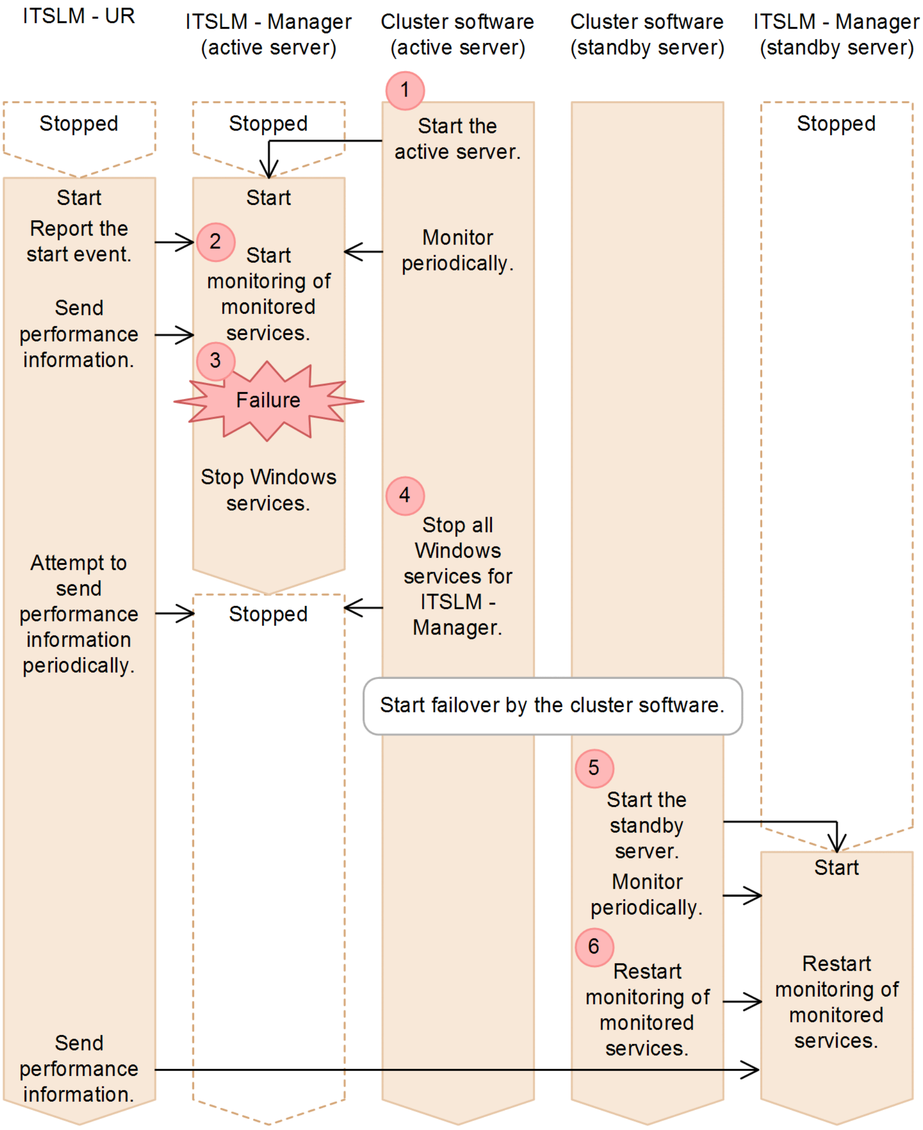
When failover occurs on ITSLM - Manager while neither monitoring nor detection of monitored services is being performed, only the connection to ITSLM - UR is restored after ITSLM - Manager is started on the standby server. Neither monitoring nor detection processing is started.

(2) While monitored services are being monitored

When failover occurs on ITSLM - Manager while monitored services are being monitored, the monitoring status is restored to what it was immediately before the failure, on the basis of the service performance information in the database on the shared disk after ITSLM - Manager has started on the standby server.

The following figure shows the processing flow when failover occurs on ITSLM - Manager while monitored services are being monitored.

Figure 6–4: Processing flow when failover occurs on ITSLM - Manager while monitored services are being monitored


ITSLM - UR
ITSLM - Manager (active server)
Cluster software (active server)
Cluster software (standby server)
ITSLM - Manager (standby server)
Stopped
Stopped
1
Start the active server.
Stopped
Start
Report the start event.
Start
2
Start monitoring of monitored services.
Monitor periodically.
Send performance information.
3
Failure
Stop Windows services.
4
Stop all Windows services for ITSLM - Manager.
Attempt to send performance information periodically.
Stopped
Start failover by the cluster software.
5
Start the standby server.
Start
Monitor periodically.
6
Restart monitoring of monitored services.
Restart monitoring of monitored services.
Send performance information.

The following explains the processing flow shown in the figure, where the numbers correspond to the numbers in the figure:

1. The cluster software (active server) starts ITSLM - Manager (active server). The cluster software (active server) also starts periodic monitoring of server status.

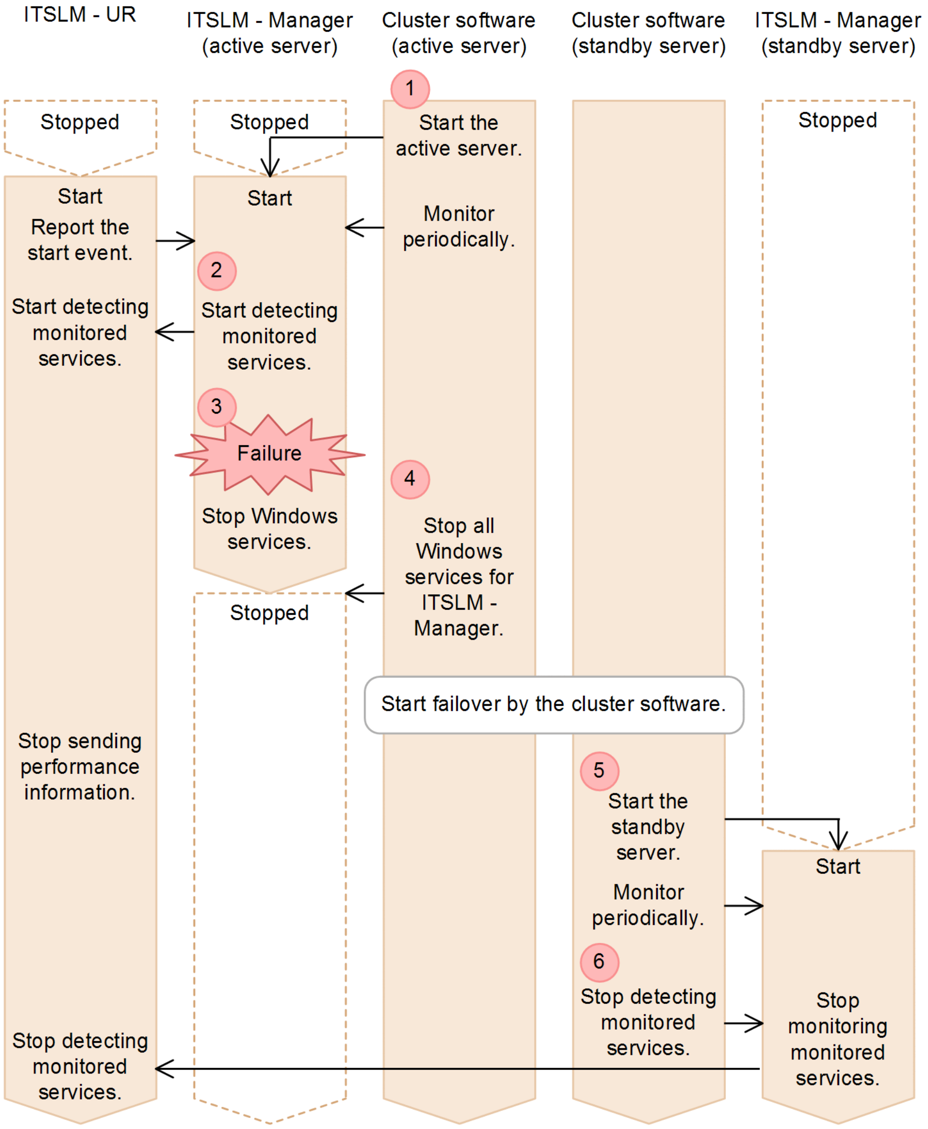
   Note that you must start ITSLM - UR manually. For details about how to start ITSLM - UR manually, see *2.1.2 Starting ITSLM - UR*.
2. ITSLM - Manager (active server) starts monitoring the monitored services.
3. Because a failure has occurred on ITSLM - Manager (active server), the Windows services stop.
4. All Windows services for ITSLM - Manager that have been registered into ITSLM - Manager (active server) are stopped by the cluster software (active server), after which failover processing starts.
5. The cluster software (standby server) starts ITSLM - Manager (standby server). The cluster software (standby server) also starts periodic monitoring of server status.
6. The cluster software (standby server) restarts monitoring of the monitored services by ITSLM - Manager (standby server). The service performance collected by ITSLM - UR is sent to ITSLM - Manager (standby server).

(3) While detection of monitored services is being performed

When failover occurs on ITSLM - Manager while detection of monitored services is being performed, the detection processing is canceled.

The following figure shows the processing flow when failover occurs on ITSLM - Manager while monitored services are being detected.

Figure 6–5: Processing flow when failover occurs on ITSLM - Manager while monitored services are being detected


ITSLM - UR
ITSLM - Manager (active server)
Cluster software (active server)
Cluster software (standby server)
ITSLM - Manager (standby server)
Stopped
Stopped
1
Start the active server.
Stopped
Start
Start
Report the start event.
Monitor periodically.
2
Start detecting monitored services.
Start detecting monitored services.
3
Failure
4
Stop Windows services.
Stop all Windows services for ITSLM - Manager.
Stopped
Start failover by the cluster software.
Stop sending performance information.
5
Start the standby server.
Start
Monitor periodically.
6
Stop detecting monitored services.
Stop monitoring monitored services.
Stop detecting monitored services.

The following explains the processing flow shown in the figure, where the numbers correspond to the numbers in the figure:

1. The cluster software (active server) starts ITSLM - Manager (active server). The cluster software (active server) also starts periodic monitoring of server status.

   Note that you must start ITSLM - UR manually. For details about how to start ITSLM - UR manually, see *2.1.2 Starting ITSLM - UR*.
2. ITSLM - Manager (active server) starts detecting monitored services.
3. Because a failure has occurred on ITSLM - Manager (active server), the Windows services stop.

4. All Windows services for ITSLM - Manager that have been registered into ITSLM - Manager (active server) are stopped by the cluster software (active server), after which failover processing starts.
5. The cluster software (standby server) starts ITSLM - Manager (standby server). The cluster software (standby server) also starts periodic monitoring of server status.
6. The cluster software (standby server) stops detection of monitored services by ITSLM - Manager (standby server). It also sends a notification to ITSLM - UR indicating that detection of monitored services is stopped.

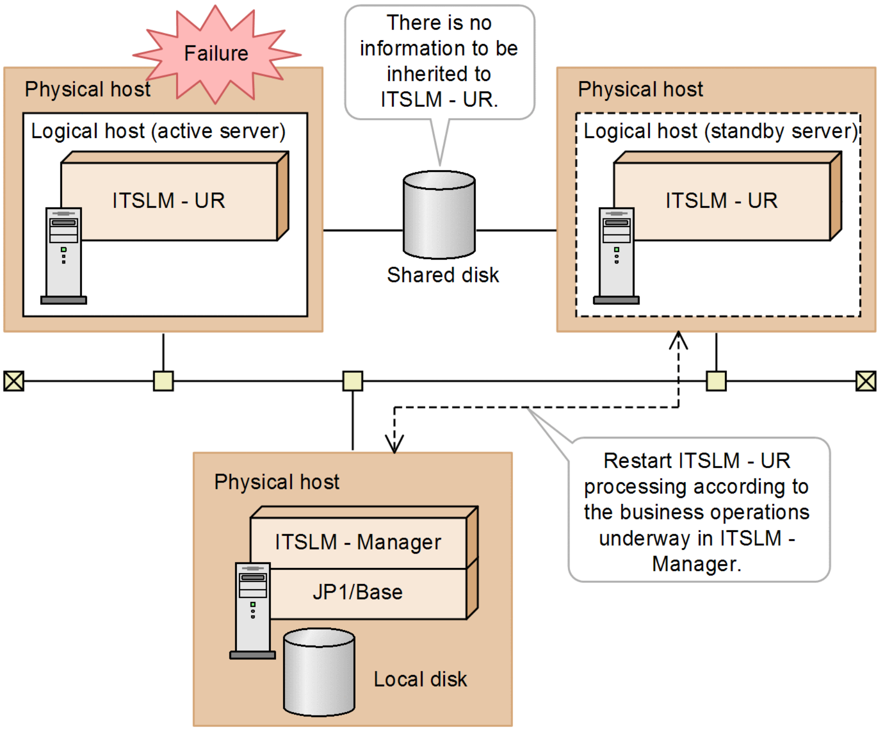
6.1.6 Processing performed when failover occurs on ITSLM - UR

When failover occurs on ITSLM - UR, ITSLM - UR on the active server is terminated and ITSLM - UR on the standby server is started. Note that the shared disk does not contain any ITSLM - UR information that is to be inherited to the standby server.

After ITSLM - UR starts on the standby server, ITSLM - UR is connected to ITSLM - Manager. After that, ITSLM - UR starts its processing according to the business operations underway in ITSLM - Manager.

The following figure shows the processing that is performed when failover occurs on ITSLM - UR.

Figure 6–6: Processing when failover occurs on ITSLM - UR


Failure
Physical host
Logical host (active server)
ITSLM - UR
There is no information to be inherited to ITSLM - UR.
Shared disk
Physical host
Logical host (standby server)
ITSLM - UR
Physical host
ITSLM - Manager
JP1/Base
Local disk
Restart ITSLM - UR processing according to the business operations underway in ITSLM - Manager.

The following subsections explain the failover processing flows depending on the timing of the failover.

(1) While neither monitoring nor detection of monitored services is being performed

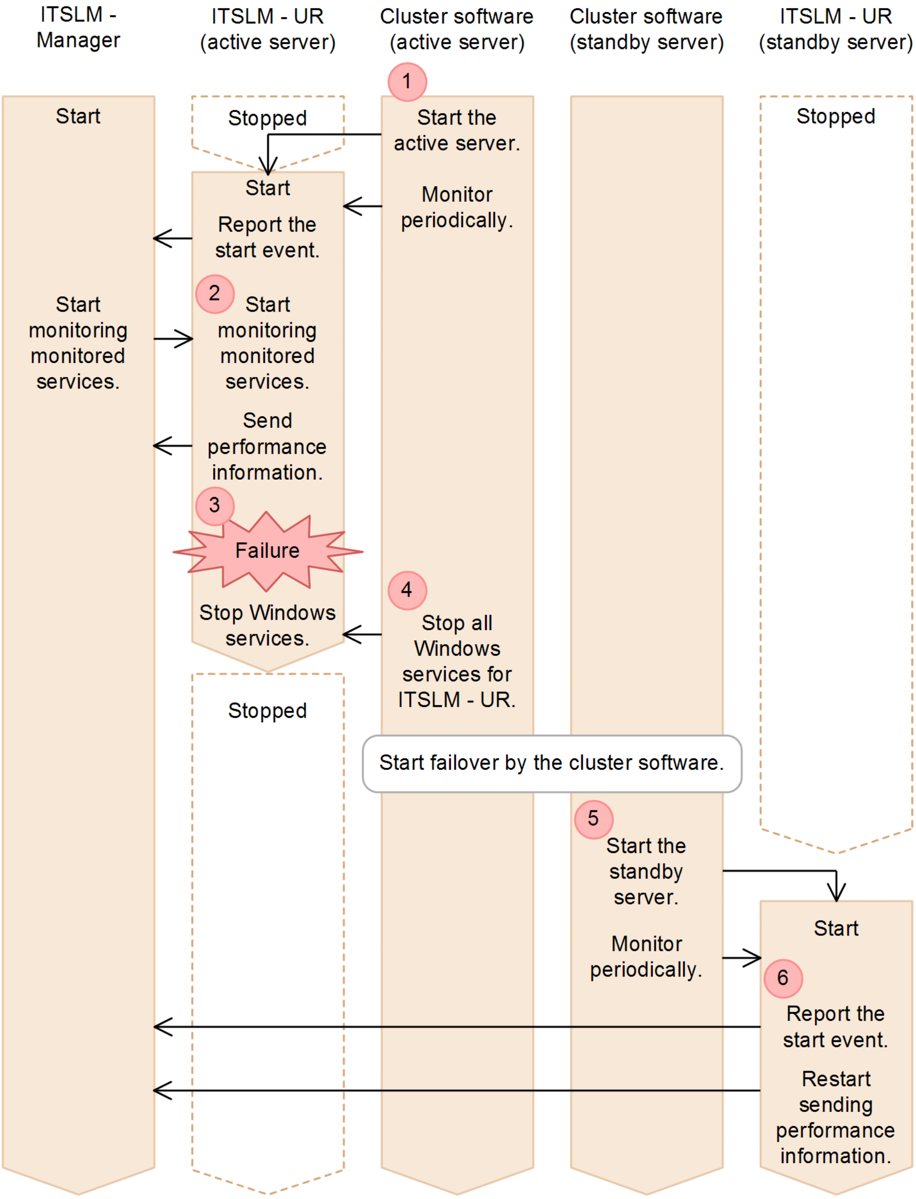
When failover occurs on ITSLM - UR while neither monitoring nor detection of monitored services is being performed, only connection to ITSLM - Manager is restored after ITSLM - UR is started on the standby server. Neither monitoring nor detection processing is started.

(2) While monitored services are being monitored

When failover occurs on ITSLM - UR while monitored services are being monitored, monitoring is restarted after ITSLM - UR has started on the standby server.

The following figure shows the processing flow when failover occurs on ITSLM - UR while monitored services are being monitored.

Figure 6–7: Processing flow when failover occurs on ITSLM - UR while monitored services are being monitored


ITSLM - Manager
ITSLM - UR (active server)
Cluster software (active server)
Cluster software (standby server)
ITSLM - UR (standby server)
1
Start
Stopped
Start the active server.
Stopped
Start
Monitor periodically.
Report the start event.
2
Start monitoring monitored services.
Start monitoring monitored services.
Send performance information.
3
Failure
4
Stop Windows services.
Stop all Windows services for ITSLM - UR.
Stopped
Start failover by the cluster software.
5
Start the standby server.
Start
Monitor periodically.
6
Report the start event.
Restart sending performance information.

The following explains the processing flow shown in the figure, where the numbers correspond to the numbers in the figure:

1. The cluster software (active server) starts ITSLM - UR (active server). The cluster software (active server) also starts periodic monitoring of server status.
2. Upon receiving a notification that ITSLM - Manager has started monitoring the monitored services, ITSLM - UR (active server) starts monitoring and sends performance information.

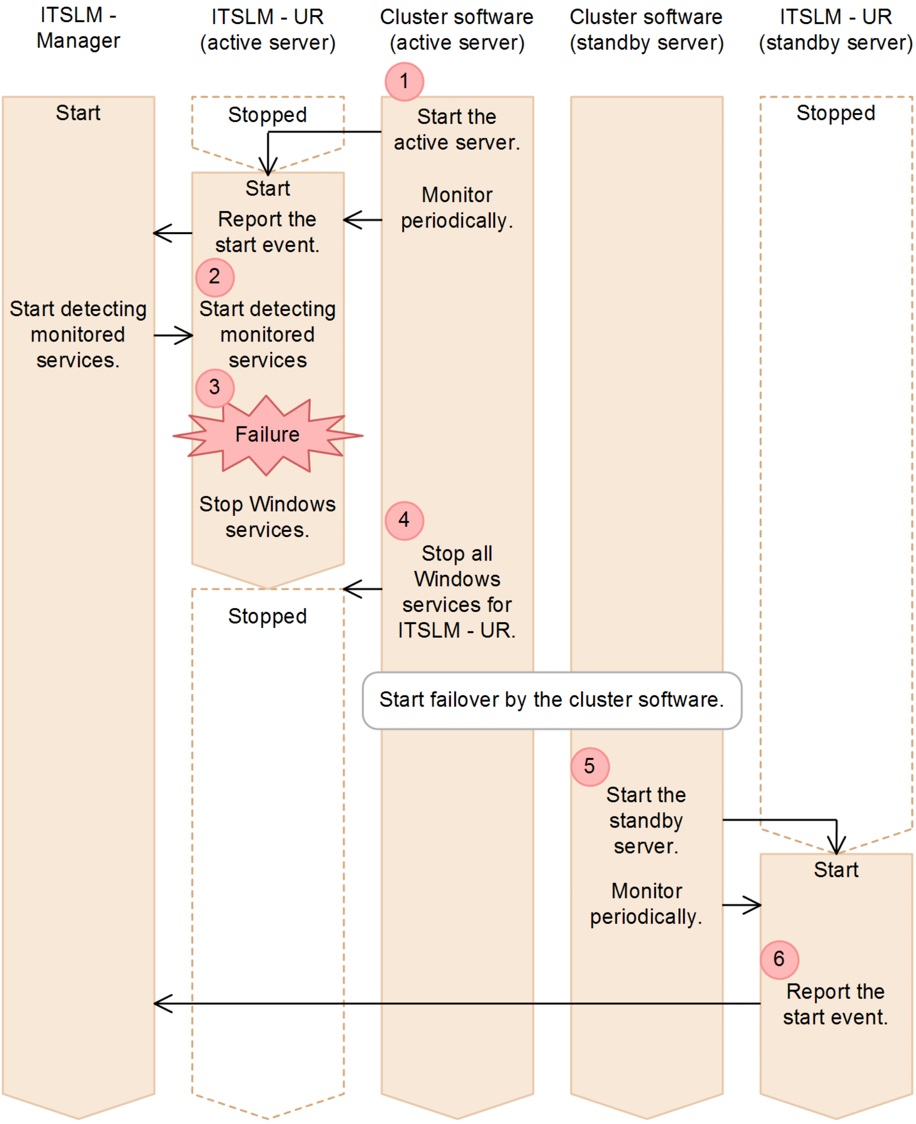
3. Because a failure has occurred on ITSLM - UR (active server), the Windows services stop.
4. All Windows services for ITSLM - UR that have been registered into ITSLM - UR (active server) are stopped by the cluster software (active server) after which failover processing starts.
5. The cluster software (standby server) starts ITSLM - UR (standby server). The cluster software (standby server) also starts periodic monitoring of server status.
6. A notification of the start event is sent from the started ITSLM - UR (standby server) to ITSLM - Manager and transmission of performance information is restarted.

(3) While detection of monitored services is being performed

When failover occurs on ITSLM - UR while detection of monitored services is being performed, the ITSLM - Manager status changes from **Detecting** to **Stopped**. Once ITSLM - UR has started on the standby server, its connection to ITSLM - Manager is restored.

The following figure shows the processing flow when failover occurs on ITSLM - UR while monitored services are being detected.

Figure 6–8: Processing flow when failover occurs on ITSLM - UR while monitored services are being detected


ITSLM - Manager
ITSLM - UR (active server)
Cluster software (active server)
Cluster software (standby server)
ITSLM - UR (standby server)
1
Start
Stopped
Start the active server.
Stopped
Start
Report the start event.
Monitor periodically.
2
Start detecting monitored services.
Start detecting monitored services
3
Failure
Stop Windows services.
4
Stop all Windows services for ITSLM - UR.
Stopped
Start failover by the cluster software.
5
Start the standby server.
Start
Monitor periodically.
6
Report the start event.

The following explains the processing flow shown in the figure, where the numbers correspond to the numbers in the figure:

1. The cluster software (active server) starts ITSLM - UR (active server). The cluster software (active server) also starts periodic monitoring of server status.
2. Upon receiving a notification that ITSLM - Manager has started detecting monitored services, ITSLM - UR (active server) starts detection processing.
3. Because a failure has occurred on ITSLM - UR (active server), the Windows services stop.
4. All Windows services for ITSLM - UR that have been registered into ITSLM - UR (active server) are stopped by the cluster software (active server), after which failover processing starts.
5. The cluster software (standby server) starts ITSLM - UR (standby server). The cluster software (standby server) also starts periodic monitoring of server status.
6. A notification indicating that ITSLM - UR (standby server) has started is sent to ITSLM - Manager and connection is restored.

6.2 Deploying ITSLM

This section explains the tasks that must be performed in order to use ITSLM in a cluster system.

You must perform the tasks described below before you configure your cluster system.

Table 6–6: Preparations for using ITSLM in a cluster system

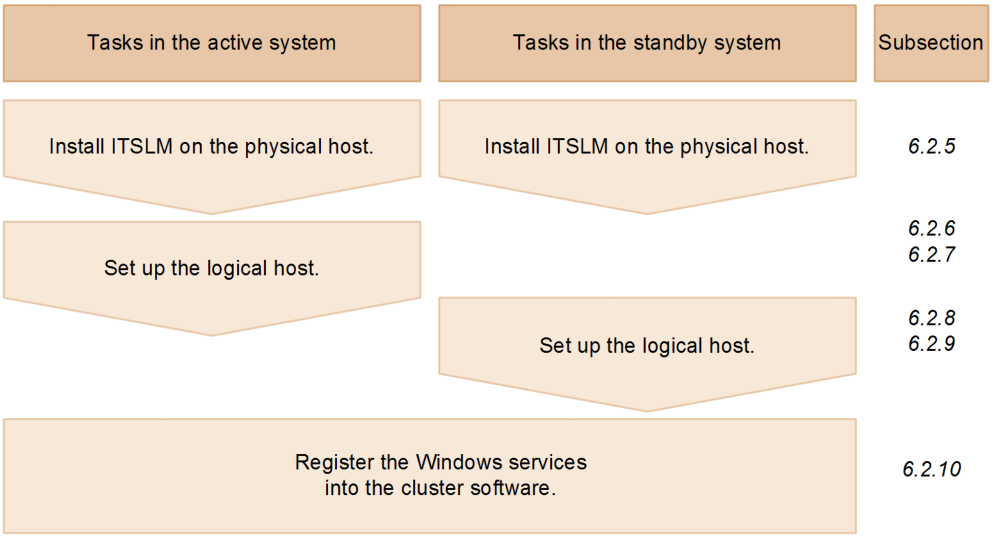
No.	Task	Description
1	Prepare a shared disk.	Prepare a shared disk for sharing service performance information when the system is switched from the active server to the standby server. Before you set up the logical host environment, set up the shared disk so that it can be accessed from both the active server and the standby server.
2	Register host names and IP addresses (if a DNS server is not used).	Register the host names and IP addresses of the following hosts into the `hosts` files on both the active system and the standby system: • Physical hosts • Logical hosts
3	Set the time on the server machines.	Set the time on the server machines so that the time on the active and standby systems is synchronized.
4	Prepare JP1/Base.	Install JP1/Base on the physical host on which ITSLM - Manager is installed and set it up for operations in the cluster system.

To run ITSLM in a cluster system, you must set up the logical hosts in the active and standby systems and register the Windows services into the cluster software after you have installed ITSLM.

6.2.1 General procedure for deploying ITSLM

The figure below shows the general procedure for deploying ITSLM. Your tasks also include setup of JP1 users in JP1/Base. The JP1 user setup procedure is the same as when ITSLM is run in a non-cluster system; for details, see *5.1.1 General procedure for deploying a new ITSLM*.

Figure 6–9: General procedure fur using ITSLM in a cluster system


Tasks in the active system
Tasks in the standby system
Subsection
Install ITSLM on the physical host.
Install ITSLM on the physical host.
6.2.5
Set up the logical host.
6.2.6
6.2.7
Set up the logical host.
6.2.8
6.2.9
Register the Windows services into the cluster software.
6.2.10

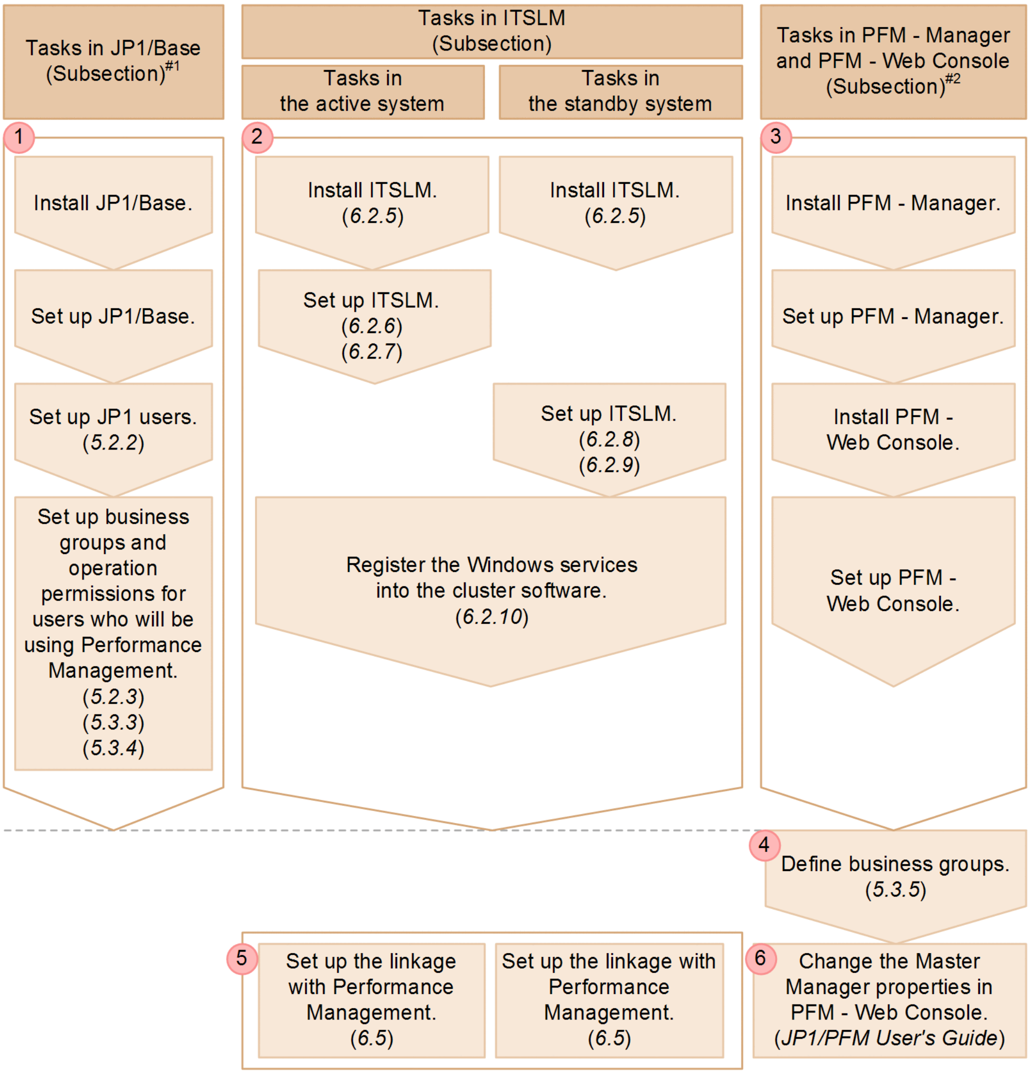
6.2.2 General procedure for upgrading ITSLM

Before you upgrade an ITSLM that has already been deployed, be sure to back up the data. You can then perform the tasks for deploying ITSLM.

6.2.3 General procedure for deploying ITSLM (when linking with a newly deployed Performance Management)

The figure below shows the general procedure for deploying ITSLM that is linked with a newly deployed Performance Management when an ITSLM linked with Performance Management is to run in a cluster configuration. Steps 1 through 3 in the figure can be performed in any order; the same applies to steps 5 and 6.

Figure 6–10: General procedure for deploying ITSLM when ITSLM is linked to a newly deployed Performance Management


Tasks in JP1/Base (Subsection)#1
Tasks in ITSLM (Subsection)
Tasks in the active system
Tasks in the standby system
Tasks in PFM - Manager and PFM - Web Console (Subsection)#2
1
Install JP1/Base.
Set up JP1/Base.
Set up JP1 users. (5.2.2)
Set up business groups and operation permissions for users who will be using Performance Management. (5.2.3) (5.3.3) (5.3.4)
2
Install ITSLM. (6.2.5)
Install ITSLM. (6.2.5)
Set up ITSLM. (6.2.6) (6.2.7)
Set up ITSLM. (6.2.8) (6.2.9)
Register the Windows services into the cluster software. (6.2.10)
3
Install PFM - Manager.
Set up PFM - Manager.
Install PFM - Web Console.
Set up PFM - Web Console.
4
Define business groups. (5.3.5)
5
Set up the linkage with Performance Management. (6.5)
Set up the linkage with Performance Management. (6.5)
6
Change the Master Manager properties in PFM - Web Console. (JP1/PFM User's Guide)

Note: In the manual name above, *Job Management Partner 1/ Performance Management* is abbreviated as *JP1/PFM*.

#1: For the tasks for which no subsection is indicated, see the *Job Management Partner 1/Base User's Guide*.

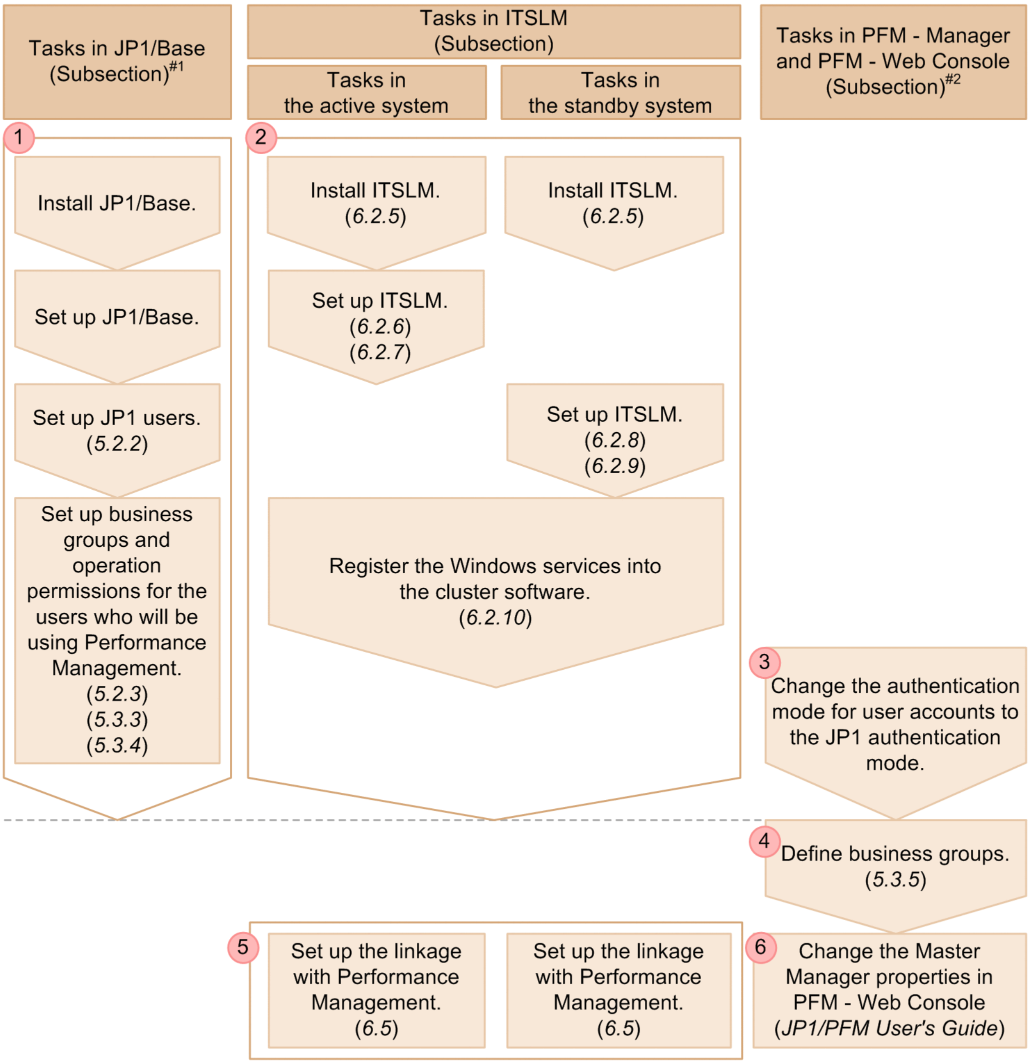
#2: For the tasks for which no subsection is indicated, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The procedure explained here is applicable to ITSLM that runs in a cluster configuration. For details about the deployment procedure when the Performance Management to be linked with ITSLM is also run in a cluster configuration, see the description of configuration and operation in a cluster system in the *Job Management Partner 1/Performance Management User's Guide*.

6.2.4 General procedure for deploying ITSLM (when linking with an existing Performance Management)

The figure below shows the general procedure for deploying ITSLM that is linked with an existing Performance Management when an ITSLM linked with Performance Management is to run in a cluster configuration. Steps 1 through 3 in the figure can be performed in any order; the same applies to steps 5 and 6.

Figure 6–11: General procedure for deploying ITSLM when ITSLM is linked to an existing Performance Management



Tasks in JP1/Base (Subsection)#1
Tasks in ITSLM (Subsection)
Tasks in the active system
Tasks in the standby system
Tasks in PFM - Manager and PFM - Web Console (Subsection)#2
1
Install JP1/Base.
Set up JP1/Base.
Set up JP1 users. (5.2.2)
Set up business groups and operation permissions for the users who will be using Performance Management. (5.2.3) (5.3.3) (5.3.4)
2
Install ITSLM. (6.2.5)
Install ITSLM. (6.2.5)
Set up ITSLM. (6.2.6) (6.2.7)
Set up ITSLM. (6.2.8) (6.2.9)
Register the Windows services into the cluster software. (6.2.10)
3
Change the authentication mode for user accounts to the JP1 authentication mode.
4
Define business groups. (5.3.5)
5
Set up the linkage with Performance Management. (6.5)
Set up the linkage with Performance Management. (6.5)
6
Change the Master Manager properties in PFM - Web Console (JP1/PFM User's Guide)

Note: In the manual name above, *Job Management Partner 1/ Performance Management* is abbreviated as *JP1/PFM*.

#1: For the tasks for which no subsection is indicated, see the *Job Management Partner 1/Base User's Guide*.
#2: For the tasks for which no subsection is indicated, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

The procedure explained here is applicable to ITSLM that is run in a cluster configuration. For details about the deployment procedure when Performance Management to be linked with ITSLM is run in a cluster configuration, see the description of configuration and operation in a cluster system in the *Job Management Partner 1/Performance Management User's Guide*.

6.2.5 Installing ITSLM

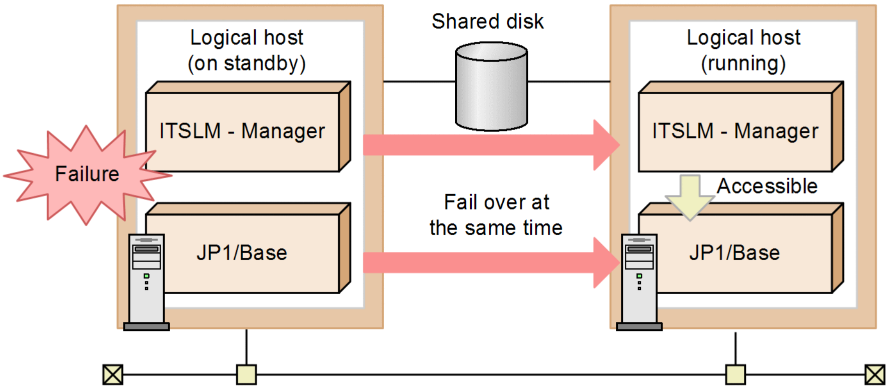
>Installation of ITSLM is the same as when ITSLM is run in a non-cluster system. For details about how to install ITSLM, see *5.1.5 Installing ITSLM*.

(1) Supplementary information

- Do not install ITSLM on the shared disk.
- Install the same version of ITSLM on the local disks of the active and standby systems.
- Install ITSLM in folders with the same names on drives with the same names in both the active and standby systems.
- During installation, specify the same settings in both the active and standby systems.
- To use ITSLM - Manager, JP1/Base is required. You must install JP1/Base on the physical machines on which ITSLM - Manager is installed in both the active and standby systems. For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.
- When the logical host of JP1/Base is set up, the event database might not be created on the local disk, depending on settings, which will result in a setting that information not be inherited.

  Set up the logical host of JP1/Base so that the event database is inherited. For details about JP1/Base setup, see the *Job Management Partner 1/Base User's Guide*.
- A JP1/Base environment must be configured on the same logical host as for ITSLM - Manager and set up to fail over when failover occurs on ITSLM - Manager. The following figure shows the configuration in which JP1/Base is configured on the same logical host.

  Figure 6–12: Configuration in which JP1/Base is configured on the same logical host



  If the JP1/Base environment is configured on a different logical host from the one used for ITSLM - Manager and failover occurs only on the JP1/Base logical host, the JP1/Base functions will no longer be accessible from JP1/Software Distribution Manager. As a result, ITSLM - Manager's login function and the JP1 event issuance function will become unavailable.

(2) Next task

- *6.2.6 Setting up the logical host in the active system (ITSLM - Manager)*

6.2.6 Setting up the logical host in the active system (ITSLM - Manager)

You set up ITSLM - Manager as the logical host in the active system.

You can set up either ITSLM - Manager first or ITSLM - UR first.

This subsection explains how to set up ITSLM - Manager.

(1) Before you start

- Before you start the setup, install the ITSLM - Manager that is to be set up.
  For details about how to install ITSLM, see *6.2.5 Installing ITSLM*.
- Verify that the following three Windows services have stopped:
  - ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`)
  - ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
  - ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

The other items to be verified are the same as when ITSLM is run in a non-cluster system; for details, see *5.1.6 Setting up ITSLM - Manager*.

(2) Procedure

To set up the logical host in the active system:

1. Create the options file required for setup.
   For details about the options file, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

2. Store the created options file in a desired folder.
   Make sure that the absolute path of the options file storage location does not exceed 255 bytes including the options file name (any name).

3. Execute the setup command.
   The following shows the setup command that is to be executed:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup -c online` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

If the command terminates normally, ITSLM - Manager has been set up to be used as the logical host in the active system.

(3) Supplementary information

The supplementary information is the same as when ITSLM is run in a non-cluster system; for details, see *5.1.6 Setting up ITSLM - Manager*.

(4) Next task

- *6.2.7 Setting up the logical host in the active system (ITSLM - UR)*

6.2.7 Setting up the logical host in the active system (ITSLM - UR)

You set up ITSLM - UR as the logical host in the active system.

You can set up either ITSLM - UR first or ITSLM - Manager first.

(1) Before you start

- Before you start the setup, install the ITSLM - UR that is to be set up.
  For details about how to install ITSLM, see *6.2.5 Installing ITSLM*.
- Verify that the following Windows service is stopped:
  - ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`)

The other items to be verified are the same as when ITSLM is run in a non-cluster system; for details, see *5.1.7 Setting up ITSLM - UR*.

(2) Procedure

To set up the logical host in the active system:

1. Execute the command for checking the network interface number and IP address of the host on which ITSLM - UR has been installed.
   Execute the following command:
   ITSLM-UR-installation-folder`\ur\bin\jslmuripls`
   For details about the command for checking the network interface number and IP address, see *jslmuripls (displays network interface number and IP address)* in *9. Commands*.

2. Create the options file required for setup based on the information checked by executing the `jslmuripls` command.
   For details about the options file, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

3. Store the created options file in a desired folder.
   Make sure that the absolute path of the options file storage location does not exceed 255 bytes including the options file name (any name).

4. Execute the setup command.
   The following shows the setup command that is to be executed:
   ITSLM-UR-installation-folder`\ur\bin\jslmursetup -c online` *absolute-path-of-options-file*
   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

If the command terminates normally, ITSLM - UR has been set up to be used as the logical host in the active system.

(3) Supplementary information

The supplementary information is the same as when ITSLM is run in a non-cluster system; for details, see *5.1.7 Setting up ITSLM - UR*.

(4) Next task

- *6.2.8 Setting up the logical host in the standby system (ITSLM - Manager)*

6.2.8 Setting up the logical host in the standby system (ITSLM - Manager)

You set up ITSLM - Manager as the logical host in the standby system.

You can set up either ITSLM - Manager first or ITSLM - UR first.

(1) Before you start

- Switch the standby system from standby server to active server to make the shared disk accessible.
- Before you start the setup, install the ITSLM - Manager that is to be set up.
  For details about the installation, see *6.2.5 Installing ITSLM*.
- Verify that the following three Windows services are stopped:
  - ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`)
  - ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
  - ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

The other items to be verified are the same as when ITSLM is run in a non-cluster system; for details, see *5.1.6 Setting up ITSLM - Manager*.

(2) Procedure

To set up the logical host in the standby system:

1. Create the options file required for setup.
   For details about the options file, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

2. Store the created options file in a desired folder.
   Make sure that the absolute path of the options file storage location does not exceed 255 bytes including the options file name (any name).

3. Execute the setup command.
   The following shows the setup command that is to be executed:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup -c standby` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

If the command terminates normally, ITSLM - Manager has been set up to be used as the logical host in the standby system.

(3) Supplementary information

- Specify the same information in the options file that is specified in the argument of the `jslmmgrsetup` command as was specified for the active system. After you have executed the `jslmmgrsetup` command, make sure that you verify that the contents of ITSLM - Manager's system definition file are the same as the contents of ITSLM - Manager's system definition file in the active system.

The other supplementary information is the same as when ITSLM is run in a non-cluster system; for details, see *5.1.6 Setting up ITSLM - Manager*.

(4) Next task

- *6.2.9 Setting up the logical host in the standby system (ITSLM - UR)*

6.2.9 Setting up the logical host in the standby system (ITSLM - UR)

You set up ITSLM - UR as the logical host in the standby system.

You can set up either ITSLM - UR first or ITSLM - Manager first.

(1) Before you start

- Switch the standby system from standby server to active server to make the shared disk accessible.
- Before you start the setup, install the ITSLM - UR that is to be set up.
  For details about the installation, see *6.2.5 Installing ITSLM*.
- Verify that the following Windows service is stopped:
  - ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`)

The other items to be verified are the same as when ITSLM is run in a non-cluster system; for details, see *5.1.7 Setting up ITSLM - UR*.

(2) Procedure

To set up the logical host in the standby system:

1. Execute the command for checking the network interface number and IP address of the host on which ITSLM - UR has been installed.
   Execute the following command:
   ITSLM-UR-installation-folder`\ur\bin\jslmuripls`
   For details about the command for checking the network interface number and IP address, see *jslmuripls (displays network interface number and IP address)* in *9. Commands*.

2. Create the options file required for setup based on the information checked by executing the `jslmuripls` command.
   For details about the options file, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

3. Store the created options file in a desired folder.
   Make sure that the absolute path of the options file storage location does not exceed 255 bytes including the options file name (any name).

4. Execute the setup command.
   The following shows the setup command that is to be executed:
   ITSLM-UR-installation-folder`\ur\bin\jslmursetup -c standby` *absolute-path-of-options-file*
   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

If the command terminates normally, ITSLM - UR has been set up to be used as the logical host in the standby system.

(3) Supplementary information

- Specify the same information in the options file that is specified in the argument of the `jslmursetup` command as was specified for the active system. After you have executed the `jslmursetup` command, make sure that you verify that the contents of ITSLM - UR's system definition file are the same as the contents of ITSLM - UR's system definition file in the active system.

The other supplementary information is the same as when ITSLM is run in a non-cluster system; for details, see *5.1.7 Setting up ITSLM - UR*.

(4) Next task

- *6.2.10 Registering the Windows services into the cluster software*

6.2.10 Registering the Windows services into the cluster software

You register the Windows services for ITSLM - Manager and ITSLM - UR into the cluster software.

(1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- If at the time you register the Windows services into the cluster software you set the order in which the Windows services are to be started, use the order shown in the table below.
    - Windows services for ITSLM - Manager

No.	Windows service		Dependency
	Displayed name	Service name	
1	**JP1/Base Event** *logical-host-name*#1	`JP1_Base_Event`*logical-host-name*#1	• Logical IP address used by JP1/Base • Shared disk used by JP1/Base
2	**JP1/Base** *logical-host-name*#1	`JP1_Base_`*logical-host-name*#1	Windows service for 1
3	**JP1/ITSLM - Manager DB Service**#2	`HiRDBEmbeddedEdition_JL0`	• Logical IP address used by ITSLM - Manager • Shared disk used by ITSLM - Manager
4	**JP1/ITSLM - Manager DB Cluster Service**#2	`HiRDBClusterService_JL0`	Windows service for 3
5	**JP1/ITSLM - Manager Service**	`JP1_ITSLM_MGR_Service`	Windows service for 4
6	**JP1/ITSLM - Manager Web Service**#3	`JP1_ITSLM_MGR_Web_Service`	Windows service for 5

#1

logical-host-name is the logical host name specified when JP1/Base is run in the cluster system.

#2

If the cluster software is set so that, before failover is performed after the Windows service has stopped, starting the Windows services is retried on the same physical host, set the cluster software to fail over without retrying starting the Windows services.

#3

After you have registered the Windows service, perform the operations listed below, based on the OS you are using.

If the OS is Windows Server 2008 R2:

Open a command prompt with Administrators permissions, and then execute the following command:

```
Cluster res "JP1/ITSLM - Manager Web Service" /priv StartupParameters=""
```

If the OS is Windows Server 2012:

Execute `PowerShell` in the command prompt, and then execute the following command:

```
Get-ClusterResource "JP1/ITSLM - Manager Web Service" | Set-ClusterParameter -Name
StartupParameters -value ""
```

After executing the command, display the Properties dialog box for **JP1/ITSLM - Manager Web Service** to verify that the startup parameter value is blank on the **General** tab.

- Windows services for ITSLM - UR

No.	Windows service		Dependency
	Displayed name	Service name	
1	**JP1/ITSLM - UR Response Service**	`JP1_ITSLM_UR_Service`	• Logical IP address used by ITSLM - UR • Shared disk used by ITSLM - UR

- If you have configured the ITSLM - Manager and ITSLM - UR environments on the same logical host, set the cluster service to start ITSLM - Manager first and then start ITSLM - UR.

(2) Procedure

For details about how to register the Windows services into the cluster software, see the applicable cluster software documentation.

6.2.11 Installing the HTML manual

Copying the HTML manual to a specified folder enables you to reference the HTML manual by clicking **Help** in the upper right corner of a window (or by clicking the **Help** button in the login window).

Installation of the HTML manual is the same as when ITSLM is run in a non-cluster system; for details, see *5.1.8 Installing the HTML manual*.

6.2.12 Installing and setting up PFM - Manager and PFM - Web Console (working with Performance Management)

You install and then set up PFM - Manager and PFM - Web Console as the products required for linking with Performance Management.

The procedures for installing and setting up PFM - Manager and PFM - Web Console are the same as when ITSLM is run in a non-cluster system; for details, see *5.1.9 Installing and setting up PFM - Manager and PFM - Web Console (working with Performance Management)*.

6.2.13 Deleting the Windows services from the cluster software

If you delete the ITSLM environment from the cluster system, you must also delete the Windows services.

(1) Before you start

- Verify that your user account belongs to the OS's Administrators group.

(2) Procedure

Delete the Windows services for ITSLM that were registered in *6.2.10 Registering the Windows services into the cluster software*.

For details about how to delete Windows services from the cluster software, see the cluster software documentation.

(3) Next task

- *6.2.15 Undoing the setup of ITSLM on the logical hosts in the active and standby systems*

6.2.14 Undoing the setup of PFM - Manager and PFM - Web Console and then uninstalling them (working with Performance Management)

When PFM - Manager and PFM - Web Console are no longer needed, you undo their setup, and then uninstall them. If you will be using Performance Management after its linkage with ITSLM has been released, there is no need to undo the setup or to uninstall Performance Management.

The procedures for undoing the setup and uninstalling PFM - Manager and PFM - Web Console are the same as when ITSLM is run in a non-cluster system; for details, see *5.1.10 Undoing the setup of and uninstalling PFM - Manager and PFM - Web Console (working with Performance Management)*.

6.2.15 Undoing the setup of ITSLM on the logical hosts in the active and standby systems

To delete the cluster system environment, you undo the setup of the logical hosts.

(1) Before you start

- Switch the logical host in the active or standby system that is subject to unsetup to the active server. If you undo the setup without switching the logical host to the active server, unneeded files might be retained.

(2) Procedure

The procedure for undoing the setup of logical hosts is the same in both the active and standby systems. This procedure is also the same as for undoing the setup of ITSLM - Manager and ITSLM - UR when ITSLM is run in a non-cluster system.

For details about how to undo the setup of ITSLM - Manager, see *5.1.11 Undoing the ITSLM - Manager setup*. For details about how to undo the setup of ITSLM - UR, see *5.1.12 Undoing the ITSLM - UR setup*.

(3) Next task

- *6.2.16 Uninstalling ITSLM*

6.2.16 Uninstalling ITSLM

Uninstallation of ITSLM is the same as when ITSLM is run in a non-cluster system. For details about the uninstallation procedure, see *5.1.13 Uninstalling ITSLM*.

6.3 Setting up the users in ITSLM

To use ITSLM, you must provide an authentication server (JP1/Base), and then use JP1/Base as the authentication server to set up the JP1 users and the operation permissions in ITSLM.

The procedure for setting up users in ITSLM is the same as when ITSLM is run in a non-cluster system; for details, see *5.2 User settings in ITSLM*.

If you run ITSLM - Manager in a cluster system, you must also run a JP1/Base that is installed on the same machine in the cluster system. However, if you have configured the JP1/Base that is used as the authentication server on a separate machine, it is optional to use the authentication server in the cluster system.

For details about the settings for running JP1/Base in a cluster system, see the *Job Management Partner 1/Base User's Guide*.

6.4 Setting up the users in Performance Management (working with Performance Management)

If you link ITSLM with Performance Management, you must set up the JP1 users in JP1/Base according to the user authentication mode used in Performance Management. Also in Performance Management, set up the business groups to be associated with the JP1 users.

The procedure for setting up users in Performance Management is the same as when ITSLM is run in a non-cluster system. See *5.3 User setup in Performance Management (working with Performance Management)*.

6.5 Setting up a linkage between ITSLM and Performance Management

If you link ITSLM with Performance Management, you must edit the system definition files in ITSLM. The items that need to be edited are the same as when ITSLM is run in a non-cluster system; for details, see *5.4 Setting up a linkage between ITSLM and Performance Management*.

If you run ITSLM in a cluster system, you must edit the system definition files in both the active and standby systems. Specify the same information in the system definition files in both the active and standby systems.

In Performance Management, the Master Manager properties must be changed in PFM - Web Console. For details about changing the Master Manager properties in PFM - Web Console, see the *Job Management Partner 1/Performance Management User's Guide*.

6.6 Settings for reporting monitoring results by email (working with Performance Management)

When it is linked with JP1/IM (JP1/IM - Manager and JP1/IM - View), ITSLM can report monitoring results by email. This linking is optional. Evaluate whether you need to link with JP1/IM.

The settings for linking with JP1/IM are the same as when ITSLM is run in a non-cluster system; for details, see *5.5 Settings for reporting monitoring results by email (working with JP1/IM)*.

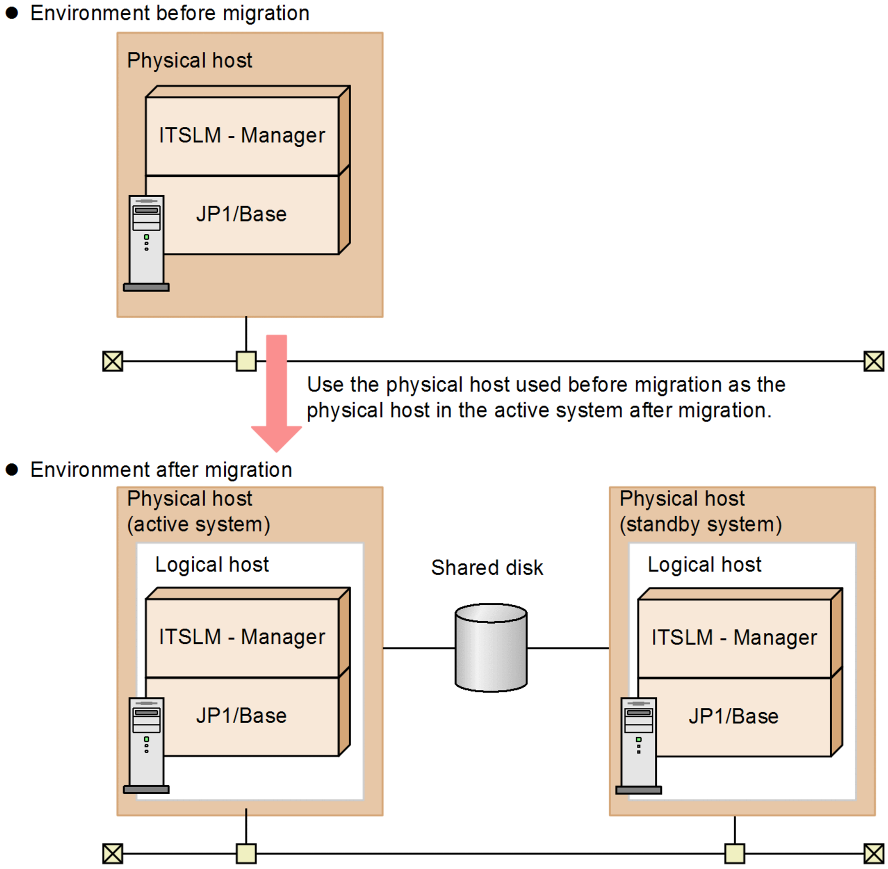
6.7 Migrating to a cluster system

This section explains the tasks involved in migrating ITSLM from a non-cluster system environment to a cluster system environment.

Before you migrate ITSLM, you must change the ITSLM version in the non-cluster environment so that it matches the ITSLM version that will be used in the cluster system environment.

The procedure explained here assumes that the physical host used in the non-cluster system is migrated to the cluster system environment and then is used as the physical host in the active system, as shown in the figure below. The figure shows the procedure for ITSLM - Manager, but the same procedure applies to ITSLM - UR.

Figure 6–13: Example of using the physical host in the non-cluster system as the physical host in the active system after migration (migrating ITSLM - Manager)


● Environment before migration
Physical host
ITSLM - Manager
JP1/Base
Use the physical host used before migration as the physical host in the active system after migration.
● Environment after migration
Physical host (active system)
Logical host
ITSLM - Manager
JP1/Base
Shared disk
Physical host (standby system)
Logical host
ITSLM - Manager
JP1/Base

6.7.1 Migrating ITSLM - Manager

This subsection explains the procedure for migrating ITSLM - Manager from a non-cluster system environment to a cluster system environment.

(1) Before you start

- First, terminate ITSLM - Manager operation, then perform the following preparations for migration:

    1. Verify that the Windows services listed below are running; if they are not running, start them:
    JP1/ITSLM - Manager DB Service

JP1/ITSLM - Manager Service

JP1/ITSLM - Manager Web Service

2. Export data from the database.

   Use the `jslmmgrexport` command to export all the data that is to be migrated to the cluster environment.

   For details about the command, see *jslmmgrexport (exports service monitor information)* in *9. Commands*.

3. Use the cluster software to stop the Windows services for ITSLM - Manager.

4. Undo the setup of ITSLM - Manager.

   Restore ITSLM - Manager to its pre-setup status. For details about undoing the setup of ITSLM - Manager, see *5.1.11 Undoing the ITSLM - Manager setup*.

(2) Procedure

To migrate ITSLM - Manager from a non-cluster system environment to a cluster system environment:

1. Set up the logical hosts in both the active and the standby systems, add the Windows services, and then set up the cluster system.

   The procedure for setting up the cluster system is the same as for setting up a new cluster system.

   For details about setting up a cluster system, see *6.2 Deploying ITSLM*.

2. Use the cluster software's functions to change the active system to the active server.

   For details about changing systems, see the cluster software documentation.

   If the active system has already been set up as the active server, skip this step.

3. Use the cluster software's functions to start ITSLM in the active system.

4. Import into the database in the active system the data that was exported from database earlier.

   Use the `jslmmgrimport` command to import all the data that is to be migrated to the cluster environment. For details about the command, see *jslmmgrimport (imports service monitor information)* in *9. Commands*.

6.7.2 Migrating ITSLM - UR

This subsection explains the procedure for migrating ITSLM - UR from a non-cluster system environment to a cluster system environment.

(1) Before you start

- First terminate ITSLM - UR, then undo the setup of ITSLM - UR in preparation for migration.

  For details about undoing the setup of ITSLM - UR, see *5.1.12 Undoing the ITSLM - UR setup*.

(2) Procedure

To migrate ITSLM - UR from a non-cluster system environment to a cluster system environment:

1. Set up the logical hosts in both the active and the standby systems, add the Windows services, and then set up the cluster system.

   The procedure for setting up the cluster system is the same as for setting up a new cluster system.

   For details about setting up a cluster system, see *6.2 Deploying ITSLM*.

2. Use the cluster software's functions to change the active system to the active server.
   For details about changing systems, see the cluster software documentation.
   If the active system has already been set up as the active server, skip this step.

3. Use the cluster software's functions to start ITSLM in the active system.

6.8 Notes about running ITSLM in a cluster system

- If you run ITSLM in a cluster system, you must specify `restart` in the `managerStartMode` property in the system definition file.

  When you set up a logical host that is run in a cluster system, `restart` is set in the `managerStartMode` property depending on the command. After you have set up the logical host, do not change this property value to `normal`. If it is changed to `normal`, the monitoring of monitored services cannot be restarted after failover.

- If ITSLM - UR starts, stops, or fails over while failover processing is underway on ITSLM - Manager, a start or termination notification from ITSLM - UR to ITSLM - Manager might timeout. To avoid such a timeout, we recommend that you adjust the values of the `announceRetryCount` and `announceRetryInterval` properties in the system definition file to satisfy the following condition:

  announceRetryCount property value × *announceRetryInterval property value* > *amount of time in seconds required from start to completion of ITSLM - Manager failover*

- Whether ITSLM is run in a physical host environment or a logical host environment is determined after ITSLM has been set up. ITSLM cannot be run in both physical and logical environments at the same time. Also, ITSLM does not support running more than one logical host at a time.

- When the cluster environment setup is undone, database-related files might remain on the shared disk. If you do not need these files, delete them manually.

- If you want to set up as a standby host a host that has already been set up as the active host, or vice versa, make sure that you first undo the setup and then perform the setup again. The unsetup process deletes the existing data. Therefore, before you undo the setup, export data that you need. Import the data after you have finished setting up the host.

- When you set up logical hosts in a cluster environment, specify the same settings in the options files in both the active and standby systems.

- If you run ITSLM in a cluster environment, do not use the JP1/Base function for controlling the order in which Windows services are started. If you want to specify the order in which the Windows services for ITSLM and JP1/Base are started and stopped, use the cluster software's function for controlling the Windows service start sequence.

7 Troubleshooting

This chapter explains how to troubleshoot problems with ITSLM.

7.1 Troubleshooting

If a problem occurs in ITSLM, a message might be output to the window, event log, integrated trace log, or message log. In the event of a problem, check the displayed message and then take the appropriate corrective action, if possible.

In the following cases, you must collect data needed for determining the cause of the problem and then contact the system administrator:

- The displayed message cannot be handled.
- The corrective action taken based on the message does not resolve the problem.
- A problem arises, but no message is output.

This section explains how to check and handle messages that are output and how to collect the data needed for determining the cause of a problem.

7.1.1 Checking and handling the output messages

The ITSLM messages are output to the window, event log, integrated trace log, or message log.

If a message has been output, check the message to determine the nature of the problem. If the problem can be handled based on the information provided in the message, take the appropriate corrective action.

(1) Before you start

- Check if a message has been output.
  For details about troubleshooting when no message is output, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

(2) Procedure

To check and handle an output message:

1. Check the message that has been output.
   Messages are output to the window, event log, integrated trace log, or message log.
   - To display the event logs, from the Windows **Start** menu, select **Administrative Tools**, **Event Viewer**, and then from the displayed Event Viewer window, select **Custom Views**, then **Administrative Events**.
   - The integrated trace logs are output to the following location:
     system-drive`:\Program Files\HITACHI\HNTRLib2\spool\hntr2`*N*#`.log`
     system-drive`:\Program Files (x86)\HITACHI\HNTRLib2\spool\hntr2`*N*#`.log`
     #: *N* is a number from `1` to `4`.
   - The message logs are output to the following location:
     For ITSLM - Manager:
     ITSLM-Manager-installation-folder`\mgr\logs\`
     For ITSLM - UR:
     ITSLM-UR-installation -folder`\ur\logs\`
2. If possible, take the appropriate corrective action based on the information provided in the message.

For details about the messages, see *11.3 Messages*.

Checking and handling an output message is now complete. However, if the message cannot be handled or the corrective action taken based on the message does not resolve the problem, you must collect data needed for determining the cause of the problem and contact the system administrator.

For details about how to collect the data needed for determining the cause, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

(3) Related topics

- *7.2.1 Event logs*
- *7.2.2 Integrated trace logs*
- *7.2.3 Message logs*
- *7.2.5 Notes about log files*

7.1.2 Examples of handling problems that might occur in ITSLM

This subsection explains examples of handling problems that might occur in ITSLM.

No.	Description
1	The ITSLM - Manager service does not start.
2	The ITSLM - UR service does not start.
3	Cannot log in (the login window cannot be displayed).
4	An attempt was made to register a monitored service, but its URI is not detected.
5	The monitor settings for a monitored service cannot be changed.
6	Monitoring results exceeded the threshold or were off the baseline, but no **Error** or **Warning** event was displayed.
7	**Error** or **Warning** is displayed in the Real-time Monitor window although the numeric values are normal.
8	**Error** or **Warning** is displayed on the **Performance chart** tab in the **Event** and **Performance chart** tabs area of the Troubleshoot window for a time period when values do not appear to be exceeding the threshold or to be off the baseline.

(1) The ITSLM - Manager service does not start

Cause:

The following are possible causes:

1. There is an error in one or more settings in the system definition file.
2. A port number is in conflict with another program.

Corrective action:

The following describes the corrective action to take for each of the possible causes.

1. Check the values of the settings in the system definition file.

   In the system definition file, check the settings required to start ITSLM - Manager. For details about the system definition file, see *5.6 Editing the system definition files to change settings*.
2. Check the port number being used by ITSLM - Manager. If you need to change a port number, see the following subsections.

Changing the port number in ITSLM - Manager

- *8.5.1 Changing ITSLM - Manager's RMI communication port number*
- *8.5.2 Changing ITSLM - UR's RMI communication port number*
- *8.5.3 Changing the listen port number of the ITSLM - Manager embedded database*
- *8.5.4 Changing the listen port number of the ITSLM - Manager embedded Web server*
- *8.5.5 Changing the port number of the internal communications port of the ITSLM - Manager embedded Web server*
- *8.5.6 Changing the port number of the completion-message receiving port of the ITSLM - Manager embedded Web server*

(2) The ITSLM - UR service does not start

Cause:

The following are possible causes:

1. ITSLM - Manager is not running.
2. There is an error in one or more settings in the system definition file.
3. A port number is in conflict with another program.

Corrective action:

The following describes the corrective action to take for each of the possible causes.

1. Check whether ITSLM - Manager has started. If ITSLM - Manager has not started, take the corrective action described in *(1) The ITSLM - Manager service does not start*.
2. Check the values of the settings in the system definition file.

   In the system definition file, check the settings required to start ITSLM - UR. For details about the system definition file, see *5.6 Editing the system definition files to change settings*.
3. Check the port number.

   If you need to change the port number, see the following subsection.

Changing the port number in ITSLM - UR

- *8.5.2 Changing ITSLM - UR's RMI communication port number*

(3) Cannot log in (the login window cannot be displayed)

Cause:

The following are possible causes:

1. The required Flash Player product has not been installed.
2. No firewall has been set up.

Corrective action:

The following describes the corrective action to take for each of the possible causes.

1. Install Flash Player.
2. Specify the port release setting in the firewall.

   For ITSLM - Manager:

Release the port numbers specified in the `psb_Listen` and `manager_port` definition items in the options file that was used during setup. If you change the settings in the options file, you must also change the firewall settings.

For details about the options file, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

For ITSLM - UR:

Release the port number specified in the `ur_port` definition item in the options file that was used during setup. If you change the setting in the options file, you must also change the firewall setting.

For details about the options file, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

(4) An attempt was made to register a monitored service, but its URI is not detected

Cause:

The following are possible causes:

1. The network interface number is not valid.
2. The browser used for the actual access is running on a different host from the host running the browser displaying the window for registering monitored services.
3. ITSLM - UR processing for detecting the monitored service to be registered has failed (the *KNAS15719-W* message is output).

Corrective action:

The following describes the corrective action to take for each of the possible causes.

1. Use the `jslmuripls` command to check the interface number of the network device and specify the network interface number used by ITSLM - UR.

   For details about the `jslmuripls` command, see *jslmuripls (displays network interface number and IP address)* in *9. Commands*.
2. On the host running the browser that is displaying the window for registering monitored services, open another tab or start another browser for the actual access.
3. Recover the status of the ITSLM - UR where the error occurred and then re-execute service detection. You can identify the ITSLM - UR where the processing error occurred from the *KNAS15719-W* message that was output around the time the service detection error occurred.

(5) The monitor settings for a monitored service cannot be changed

Cause:

Monitoring of the monitored service whose settings are to be changed has not been stopped.

Corrective action:

Stop monitoring the monitored service whose settings are to be changed. For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

(6) Monitoring results exceeded the threshold or were off the baseline, but no Error or Warning event was displayed

The **Error** and **Warning** events are not displayed for a period after monitoring begins because a certain amount of service performance must be collected before monitoring results can be obtained.

The following shows when display of events starts for each type of monitoring:

- Threshold value monitoring: 60 seconds after monitoring begins
- Out-of-range value detection: 60 seconds after monitoring begins
- Trend monitoring: When 30% of the period subject to trend monitoring specified in the **Monitor settings** area of the Settings window has elapsed (for example, if the specified value is 1 hour, display of events starts when 18 minutes have elapsed)

If monitoring is stopped and then restarted, events are not displayed until the above times have elapsed since the restart.

(7) Error or Warning is displayed in the Real-time Monitor window although the numeric values are normal

Even if the current numeric values are normal, the display of **Error** or **Warning** remains until the status resulting in the **Error** and **Warning** is released. By default, the display of **Error** or **Warning** remains until the number of error data items in the past one minute becomes less than $S \times 10 \div 100$ (rounded up), where *S* is the number of service performance items measured in 60 seconds.

(8) Error or Warning is displayed on the Performance chart tab in the Event and Performance chart tabs area of the Troubleshoot window for a time period when values do not appear to be exceeding the threshold or to be off the baseline

Cause:

> You might be looking at a graph whose display period is set to 10 minutes or more.
>
> When the display period is 10 minutes or more, a graph is plotted to show a summary of maximum values in a specific period so that the number of data items becomes 60. Therefore, the actual times of the error and warning events might appear to be shifted on the graph.

Corrective action:

> Check the timing of events by using a graph with the display period set to one minute.

7.1.3 Investigating the cause of a failover (cluster system)

You must investigate the cause of a failover that occurs when ITSLM is running in a cluster system. Failover occurs when an event that leads to failover occurs on the active server. For the types of failures that result in failover, see *6.1.3 Failover timing*.

(1) Before you start

- Check if a message has been output.

  For details about troubleshooting when no message is output, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

(2) Procedure

To investigate the cause of a failover:

1. Check the message output at the active server.

Messages are output to the cluster software's logs in addition to the ITSLM - Manager window, event log, integrated trace log, or message log.

- For details about the cluster software's logs, see the cluster software documentation.
- For details about the event log, integrated trace log, and message log output destinations, see *7.1.1 Checking and handling the output messages*.

2. If possible, take the appropriate corrective action based on the information provided in the message.

   For details about the messages see *11.3 Messages*.

Message checking and taking of corrective action are now complete. However, if the message cannot be handled or the corrective action taken based on the message does not resolve the problem, you must collect data needed for determining the cause of the problem and contact the system administrator.

For details about how to collect the data needed for determining the cause, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

(3) Related topics

- *6.1.3 Failover timing*
- *7.2.1 Event logs*
- *7.2.2 Integrated trace logs*
- *7.2.3 Message logs*
- *7.2.5 Notes about log files*

7.1.4 Handling failover errors (cluster system)

If failover from the active server to the standby server has failed, take the appropriate corrective action based on the cause of the failover error.

(1) Procedure

To handle a failover error:

1. Check the cluster software's logs to determine the cause of the failover error.

   The cause of a failover error is one of the following:

   - A Windows service start error occurred on ITSLM's standby server
   - A cluster software error occurred

   If a Windows service start error occurred on ITSLM's standby server, go to step 2; if a cluster software error occurred, go to step 3.

2. Check the message output to the standby server's event log, integrated trace log, or message log, and eliminate the cause of the Windows service start error on the standby server.

   For details about the output destinations of the event log, integrated trace log, and message log, see *7.1.1 Checking and handling the output messages*. For details about the messages, see *11.3 Messages*. After you have taken corrective action, go to step 4.

3. If failover occurred due to a cluster software error, check the cluster software's logs and eliminate the cause of the error.

4. Start the Windows services for ITSLM from the cluster software.

   For details about the Windows services to be started, see *2.1.1 Starting ITSLM - Manager* and *2.1.2 Starting ITSLM - UR*.

If the Windows services start successfully on the standby server, handling of the failover error is complete. If the Windows services still do not start successfully on the standby server after the corrective action was taken on the basis of the message, collect the data needed for determining the cause of the error and contact the system administrator. For details about how to collect the data needed for determining the cause, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

7.1.5 Handling a shortage of database capacity

If a shortage of database capacity occurs while ITSLM - Manager is running, you must undo the ITSLM - Manager setup, extend the database area, and then set up ITSLM - Manager again.

You can determine whether there is a shortage of database capacity by checking the Windows event logs. From Windows **Start** menu, select **Administrative Tools**, then **Event Viewer**, and then check the **Applications** logs for the following messages:

Table 7–1: Messages output in the event of a shortage of database capacity

No.	Type	Source	Event	Message
1	Error	`JP1_ITSLM_Manager_DB_Service`	`30001`	`KFPH22025-E`
2	Error	`JP1_ITSLM_Manager_DB_Service`	`30001`	`KFPH22026-E`

If either of these messages has been output, take the appropriate corrective action by following the procedure described below.

(1) Before you start

- Make a database backup. For details about how to back up the database, see *8.1.2 Backing up the database*.
- Estimate the size of the database area required for storing data. For details about how to estimate the size of the database area, see *How to estimate the size of the database area* in *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*. Provide as much free space as needed based on the estimation of the database area that is to be extended.

(2) Procedure

To handle a shortage of database capacity:

1. Execute the `jslmmgrexport` command to create an export file.

   For details about the `jslmmgrexport` command, see *jslmmgrexport (exports service monitor information)* in *9. Commands*.

2. Execute the unset command for ITSLM - Manager.

   For details about the unsetup command, see *jslmmgrunsetup (undoes ITSLM - Manager setup)* in *9. Commands*.

3. Create the options file (`jp1itslm_setup.opt`) needed for setting up ITSLM - Manager and specify in the `hdb_area_size` definition item the database capacity estimated in *(1) Before you start*. Also, specify in the

`hdb_area_path` definition item (the `hdb_share_area_path` definition item if ITSLM is running in a cluster system) the path of an area that provides as much free space as specified in the `hdb_area_size` definition item.

For details about the options file, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

4. Execute the setup command for ITSLM - Manager.

   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

5. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).

6. Execute the `jslmmgrimport` command to import the export file created in step 1.

   For details about the `jslmmgrimport` command, see *jslmmgrimport (imports service monitor information)* in *9. Commands*.

If the import command terminates normally, the database area has been extended.

7.1.6 Collecting the data needed for determining the cause of a problem

You must collect data needed for determining the cause of a problem and then contact the system administrator in the following cases:

- The displayed message cannot be handled.
- The corrective action taken based on the message does not resolve the problem.
- There is a problem but no message is output.

This subsection explains how to collect the data needed for determining the cause of a problem.

If an error dialog box is displayed when an error has occurred, start collecting data while the dialog box is being displayed.

(1) Procedure

To collect the data needed for determining the cause of a problem:

1. Obtain a thread dump.

   Obtain the execution results of the following command:

   For ITSLM - Manager:

   ITSLM-Manager-installation-folder`\mgr\system\psb\jdk\jre\bin\jheapprof -f -p` *process-ID*

   For ITSLM - UR:

   ITSLM-UR-installation -folder`\ur\system\psb\jdk\jre\bin\jheapprof -f -p` *process-ID*

   To specify *process-ID*, open Windows Task Manager's **Process** tab and specify the process ID of the following ITSLM process:

   For ITSLM - Manager:

   - `cjstartweb.exe`
   - `jslmmengine.exe` (all instances of `jslmmengine.exe`)
   - `jslmmpcollect.exe`
   - `jslmmRMI.exe`
   - `jslmmUR.exe`

- `jslmmadaptor.exe`
- `jslmmdao.exe`

For ITSLM - UR:

- `jslmuengine.exe`
- `jslmuRMI.exe`
- `jslmuUR.exe`

If there are multiple processes with the same name as an ITSLM process on the **Process** tab, right-click a candidate process, select **Properties** from the displayed context menu, and then check the location displayed in **Location** on the **General** tab. If the location is under the ITSLM installation folder, it is an ITSLM process.

For example, if the ITSLM - Manager installation folder is `C:\Program Files\HITACHI\JP1ITSLM`, **Location** on the **General** tab for the ITSLM - Manager process `cjstartweb.exe` shows `C:\Program Files\HITACHI\JP1ITSLM\mgr\system\psb\CC\web\bin`.

If the process ID is not displayed on the **Process** tab, select **View**, **Select Columns**, and then select **PID (Process Identifier)**.

For details about the command for collecting thread dumps, see *7.2.4 Thread dumps*.

2. Execute the data collection command.

   Execute the following data collection command:

   For ITSLM - Manager:

   ITSLM-Manager-installation-folder`\mgr\bin\jslmminfoget.bat`

   For ITSLM - UR:

   ITSLM-UR-installation -folder`\ur\bin\jslmurinfoget.bat`

   For details about the data collection command, see *jslmminfoget (collects data needed for investigating the cause of ITSLM - Manager errors)* or *jslmurinfoget (collects data needed for investigating the cause of ITSLM - UR errors)* in *9. Commands*.

3. Collect OS statistical information.

   To collect statistical information, use the Windows Performance Monitor. To display Performance Monitor, from the Windows **Start** menu, select **Administrative Tools**, and then **Performance Monitor**.

   The following table lists the parameters that need to be collected as OS statistical information.

Table 7–2: Parameters to be collected as OS statistical information

Object	Instance	Counter
`Processor`	`_Total`	`%Processor Time`
		`%Privileged Time`
		`%User Time`
`Memory`	None	`Cache Bytes`
		`Cache Faults/sec`
		`Page Faults/sec`
		`Transition Faults/sec`
`Process`	`_Total`	`Handle Count`
		`Page Faults/sec`
		`Private Bytes`

Object	Instance	Counter
`Process`	`_Total`	`Virtual Bytes`
		`Working Set`

4. Record the details of the operation that was underway when the error occurred.

   After you have collected data according to steps 1 through 3, record the details of the operation that was underway when the error occurred. You must record the following information:

   - Details of the operation that was underway immediately before the error occurred
   - Details of the error
   - The time the error occurred
   - The system configuration (OS version, host name, configuration of ITSLM - Manager and ITSLM - UR)
   - The error's reproducibility
   - Login user name

5. Collect the error information displayed in the window.

   Press the **PrintScreen** key while holding down the **Ctrl** key to obtain a screenshot of the error event. You must collect the following information:

   - Error message output by ITSLM and OS
   - Error dialog box
   - Message issued by a command

6. Collect a user dump.

   If an ITSLM process terminated due to an application error, open Windows Task Manager's **Process** tab while the error dialog box is being displayed, then right-click the terminated process. From the displayed context menu, select **Create Dump File** to collect a user dump.

   The ITSLM processes are as follows:

   For ITSLM - Manager:

   - `cjstartweb.exe`
   - `jslmmengine.exe` (all instances of `jslmmengine.exe`)
   - `jslmmpcollect.exe`
   - `jslmmprocctrl.exe`
   - `jslmmRMI.exe`
   - `jslmmUR.exe`
   - `jslmmadaptor.exe`
   - `jslmmdao.exe`

   For ITSLM - UR:

   - `jslmuengine.exe`
   - `jslmuprocctrl.exe`
   - `jslmuRMI.exe`
   - `jslmuUR.exe`

   If there are multiple processes with the same name as an ITSLM process on the **Process** tab, right-click a candidate process, select **Properties** from the displayed context menu, and then check the location displayed in **Location** on the **General** tab. If the location is under the ITSLM installation folder, it is an ITSLM process.

For example, if the ITSLM - Manager installation folder is `C:\Program Files\HITACHI\JP1ITSLM`, **Location** on the **General** tab for the ITSLM - Manager process `cjstartweb.exe` shows `C:\Program Files\HITACHI\JP1ITSLM\mgr\system\psb\CC\web\bin`.

Note:

To collect an accurate user dump, keep the error dialog box displayed while you collect the dump.

7. Collect the log file from when ITSLM was installed.

You must obtain the log file from the time when ITSLM was installed only when installation of ITSLM has failed.

If ITSLM installation failed, execute the commands shown below using a user account belonging to the OS's Administrators group to run the installer and collect the log file.

For ITSLM - Manager:

`cd` *ITSLM-Manager-installer-(MSI-file)-storage-folder*

```
msiexec.exe /i ITSLM_MGR.msi /l*vx JP1ITSLM_MGR.log
```

For ITSLM - UR:

`cd` *ITSLM-UR-installer-(MSI-file)-storage-folder*

```
msiexec.exe/iITSLM_UR.msi/l*vxJP1ITSLM_UR.log
```

Also collect the following folder (including files under the folder):

For ITSLM - Manager:

`%TEMP%`#`\Hitachi\JP1ITSLMM\hliclib`

For ITSLM - UR:

`%TEMP%`#`\Hitachi\JP1ITSLMU\hliclib`

#: `%TEMP%` is the path indicated by the `TEMP` environment variable.

Once you have collected all the necessary data, the task for collecting data needed for determining the cause of a problem is complete.

(2) Related topics

- *7.2.1 Event logs*
- *7.2.2 Integrated trace logs*
- *7.2.3 Message logs*
- *7.2.4 Thread dumps*
- *7.2.5 Notes about log files*

7.2 Log files

The following are the log files:

- Event log, integrated trace log, and message log that are output by ITSLM
- Thread dump of a thread running within ITSLM's Java process that is collected by executing the `jheapprof` command

This section explains the event log, integrated trace log, message log, and thread dumps.

7.2.1 Event logs

Event logs are log information reporting problems in the system and are intended for system administrators. They provide the minimum amount of information. ITSLM's event logs are output to Windows event logs.

To display event logs, from the Windows **Start** menu, select **Administrative Tools**, **Event Viewer**, and then from the displayed Event Viewer window, select **Custom Views**, then **Administrative Events**.

The following table describes the items displayed in the event logs.

Table 7–3: Items displayed in the event logs

No.	Displayed item	Description
1	**Log Name**	`Application` is always displayed.
2	**Source**	Product name. One of the following is displayed: • `ITSLM - Manager` • `ITSLM - UR`
3	**Date and Time**	Event log output date and time (local time) in the following format: *YYYY*/*MM*/*DD hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*)
4	**Event ID**	ID assigned to each message
5	**Task Category**	`None` is always displayed.
6	**Level**	Type of event log. One of the following is displayed: • `Information` • `Warning` • `Error`
7	**Keywords**	`Classic` is always displayed.
8	**User**	`N/A` is always displayed.
9	**Computer**	Computer name
10	**OpCode**	Nothing is displayed.
11	**More Information**	Message output by ITSLM, in the following format: `KNAS`*nnnnn*`-`*Z message* `KNAS`*nnnnn*`-`*Z*: Message ID (*nnnnn*: message serial number; *Z*: message type) *message*: Message text

7.2.2 Integrated trace logs

Integrated trace logs are provided by Hitachi Network Objectplaza Trace Library (*HNTRLib2*) as collections of trace information output by individual programs at a specific output destination. They contain messages related to start and termination of ITSLM.

The output destinations of integrated trace logs are as follows:

system-drive`:\Program Files\HITACHI\HNTRLib2\spool\hntr2`*N*#`.log`

system-drive`:\Program Files(x86)\HITACHI\HNTRLib2\spool\hntr2`*N*#`.log`

#: *N* is a number from 1 through 4.

The following tables describe the header information and the items output to the integrated trace logs.

Table 7–4: Header information output to the integrated trace logs

No.	Header	Description
1	**OS information**	Information about the OS on which HNTRLib2 is running.
2	**Host name**	Information about the host on which HNTRLib2 is running.
3	**Time zone**	OS's time zone.
4	**HNTRLib2 start time**	Time HNTRLib2 started.

Table 7–5: Items output to the integrated trace logs

No.	Output item	Description
1	*number* (4 digits)	Each trace record's sequence number. This numbering is initialized for each process that outputs logs.
2	*date* (10 bytes)	Date the trace was output, in the following format: *YYYY*/*MM*/*DD* (*year*/*month*/*date*)
3	*time* (12 bytes)	Time (local time) the trace was output, in the following format: *hh*:*mm*:*ss*.*sss* (*hour*:*minute*:*second*.*millisecond*)
4	*application-program-name* (maximum of 16 bytes)	Name that identifies the application. The following application program names are output by ITSLM: • `JP1ITSLMProcCtrl` • `JP1ITSLMView` • `JP1ITSLMUsrResp` • `JP1ITSLMWebSysAn` • `JP1ITSLMPerColct` • `JP1ITSLMRmiSrv` • `JP1ITSLMDao` • `JP1ITSLMAdaptor` • *command-identifier*#
5	*pid*	Process ID set by the OS
6	*tid*	ID identifying the thread
7	*message-ID*	Message identifier
8	*message-text*	Message text

#

If the message was output by a command, the identifier of the command is output. For the identifiers that are output, see the descriptions of functions in *9. Commands*.

The log output time that is included in the integrated trace logs is based on the time zone of the process that output the log. Therefore, if you change the value of the `TZ` environment variable and start services or execute commands, the output time might not be based on the time zone of the OS.

Output example:

The following shows an output example of integrated trace log information:

```
**** Microsoft WindowsNT6.1(Build:7600)                           host01
TZ=(local)-9:00                 2011/04/20 19:51:04.437
     yyyy/mm/dd hh:mm:ss.sss                     pid      tid      message-id
message(LANG=0x0411)
0000 2011/04/20 19:53:57.639     JP1ITSLMView     000010FC J33D2EED KNAS15300-I
Logged in. User name = super
```

7.2.3 Message logs

Message logs are the log information containing the messages that are output by each process while ITSLM is running.

By default, the message logs are output to the following folders:

For ITSLM - Manager:

ITSLM-Manager-installation-folder`\mgr\logs\`

For ITSLM - UR:

ITSLM-UR-installation -folder`\ur\logs\`

You can change the size and number of message log files in the `jp1itslm.properties` or `jp1itslmur.properties` system definition file. For details, see *5.6.1 Editing the system definition files* and *5.6.2 Editable definitions*.

The following table lists and describes the message logs that are output by ITSLM - Manager.

Table 7–6: Message logs output by ITSLM - Manager

No.	Message log	Description	Properties in related system definition file	Process that outputs the message log
1	`ProcessCtrlMessageM`*N*[#]`.log`	This log is output by ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`). This is a log of the process that controls each child process.	• `loggerMessageLogLevel` • `loggerProcessCtrlMessageFileCount` • `loggerProcessCtrlMessageMaxFileSize`	`jslmmprocctrl`
2	`RmiServerMessageM`*N*[#]`.log`	These logs are output by a child process that was started by the control process.	• `loggerMessageLogLevel` • `loggerRmiServerMessageFileCount`	`jslmRMI`

No.	Message log	Description	Properties in related system definition file	Process that outputs the message log
2	`RmiServerMessageM`*N*#`.log`	These logs are output by a child process that was started by the control process.	• `loggerRmiServerMessageMaxFileSize`	`jslmRMI`
3	`UserResponseMessageM`*N*#`.log`		• `loggerMessageLogLevel` • `loggerUserResponseMessageFileCount` • `loggerUserResponseMessageMaxFileSize`	`jslmmUR`
4	`PerfCollectorMessage`*N*#`.log`		• `loggerMessageLogLevel` • `loggerPerfCollectorMessageFileCount` • `loggerPerfCollectorMessageMaxFileSize`	`jslmmpcollect`
5	`ViewMessage`*N*#`.log`		• `loggerMessageLogLevel` • `loggerViewMessageFileCount` • `loggerViewMessageMaxFileSize`	`cjstartweb`
6	`DaoMessage[`*n*`] .log`		• `loggerDaoMessageFileCount` • `loggerDaoMessageMaxFileSize`	`jslmmdao`
7	`InputAdaptorCtrlMessage[`*n*`].log`		• `loggerInputAdaptorCtrlMessageFileCount` • `loggerInputAdaptorCtrlMessageMaxFileSize`	`jslmmadaptor`
8	`CommandMessageM`*N*#`.log`	This log is output by some ITSLM - Manager commands.	• `loggerCommandMessageFileCount` • `loggerCommandMessageMaxFileSize`	Each command process

#: *N* is a number from 1 through the specified number of files.

The following table lists and describes the message logs that are output by ITSLM - UR.

Table 7–7: Message logs output by ITSLM - UR

No.	Message log	Description	Properties in related system definition file	Process that outputs the message log
1	`ProcessCtrlMessageUR`*N*#`.log`	This log is output by ITSLM - Manager service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`). This	• `loggerMessageLogLevel`	`jslmuprocctrl`

No.	Message log	Description	Properties in related system definition file	Process that outputs the message log
1	ProcessCtrlMessageUR*N*#.log	is a log of the process that controls each child process.	• loggerProcessCtrlMessageFileCount • loggerProcessCtrlMessageMaxFileSize	jslmuprocctrl
2	RmiServerMessageUR*N*#.log	These logs are output by a child process that was started by the control process.	• loggerMessageLogLevel • loggerRmiServerMessageFileCount • loggerRmiServerMessageMaxFileSize	jslmRMI
3	UserResponseMessageUR*N*#.log		• loggerMessageLogLevel • loggerUserResponseMessageFileCount • loggerUserResponseMessageMaxFileSize	jslmuUR
4	WebSystemAnalysisMessage*N*#.log		• loggerMessageLogLevel • loggerWebSystemAnalysisMessageFileCount • loggerWebSystemAnalysisMessageMaxFileSize	jslmWebSystemAnalysis

#: *N* is a number from 1 through the specified number of files.

The header information and items that are output to the message logs are the same as for integrated trace logs. For details about the header information and output items, see *7.2.2 Integrated trace logs*.

7.2.4 Thread dumps

A thread dump is a file to which information about the threads running in a Java process is output.

This subsection explains the `jheapprof` command that is used to collect thread dumps.

`jheapprof` (outputs an extended thread dump with statistics by Hitachi class)

The following explains the function, format, and an example of the `jheapprof` command.

For the format of command explanations, see *Format of command explanations* in *9. Commands*.

Function

Outputs for Java processes extended thread dumps containing statistics by Hitachi class. From the statistics by Hitachi class, you can obtain the size of all instances under the members of the instances of each class.

Format

```
jheapprof [-i|-f] [-class class-name] [-explicit|-noexplicit] [-
fullgc|-copygc|-nogc] -p process-ID
```

Execution permission

None

Storage folder

- For ITSLM - Manager:
  ITSLM-Manager-installation-folder`\mgr\system\psb\jdk\jre\bin\`
- For ITSLM - UR:
  ITSLM-UR-installation -folder`\ur\system\psb\jdk\jre\bin\`

Arguments

- `-i`

  Specifies that the user is to be asked whether this command is to be executed on the process with the specified process ID.

  If the `-f` option is omitted, this option is assumed, even if it is omitted.

- `-f`

  Specifies that the user is not be asked whether this command is to be executed on the process with the specified process ID.

- `-class` *class-name*

  Specifies that the structure of the classes that have the class (instance) with the specified class name is to be output to the thread dump as members in list format. You must enclose the package name of the specified class in double quotation marks (`"`).

- `-explicit`

  Specifies that an explicit heap is to be included as a target of the instance statistics function. If this option is specified together with the `-noexplicit` option, the last option specified takes effect. Note that there is no need to specify this option in ITSLM.

- `-noexplicit`

  Specifies that an explicit heap is not to be included as a target of instance statistics function. If this option is specified together with the `-explicit` option, the last option specified takes effect. Note that there is no need to specify this option in ITSLM.

- `-fullgc`

  Specifies that a full garbage collection is to be performed before statistics information is output.

  If this option is specified together with the `-copygc` or `-nogc` option, the last option specified takes effect.

- `-copygc`

  Specifies that a copy garbage collection is to be performed before statistics information is output.

  If this option is specified together with the `-fullgc` or `-nogc` option, the last option specified takes effect.

- `-nogc`

  Specifies that a garbage collection is not to be performed before statistics information is output.

  If this option is specified together with the `-fullgc` or `-copygc` option, the last option specified takes effect.

- `-p` *process-ID*

  Specifies the process ID of the Java program for which statistics by Hitachi class are to be output.

Notes:

This command cannot be executed more than once on the same Java process. If you want to execute this command on the same Java process more than once, wait until the extended thread dump with statistics by Hitachi class has been output by the first execution of the `jheapprof` command before executing the command again.

When a Java process starts, it uses MailSlot to initialize communication. If initialization fails, the Java process outputs a message and cancels the processing.

This command can be executed by a user who is not the owner of the Java process whose process ID is specified in the argument.

When any of the following messages is output, an extended thread dump with statistics by Hitachi class has not been output.

No.	Error message	Description
1	`usage: jheapprof [-f|-i] [-class classname] [-explicit|-noexplicit] [-fullgc|-copygc|-nogc] [-garbage|-nogarbage] [-rootobjectinfo|-norootobjectinfo] [-rootobjectinfost size] -p process-id jheapprof`	An invalid argument was specified in the command.
2	`jheapprof: illegal option --` *option*	An invalid option was specified in the `jheapprof` command.
3	*process-ID*`: Now processing previous request, this request canceled`	The process whose process ID was specified in the argument of the `jheapprof` command is already outputting statistics by Hitachi class.
4	*process-ID*`: Not owner`	`0` is specified as the process ID in the argument of the `jheapprof` command.
5	`jheapprof: can't create work file at temporary directory , this request canceled`	An extended thread dump with statistics by Hitachi class could not be output, because the command does not have view or write permission for the temporary files folder. The request to output an extended thread dump with statistics by Hitachi class has been canceled.
6	`jheapprof: can't get temporary directory, this request canceled`	An extended thread dump with statistics by Hitachi class could not be output, because the command was not able to fetch data from the temporary files folder. The request to output extended thread dump with statistics by Hitachi class has been canceled.
7	jheapprof: please delete *name-of-file-that-could-not-be-deleted* in *full-path-of-file-that-could-not-be-deleted*	When the `jheapprof` command terminated, the internal file could not be deleted. Delete the indicated file on the indicated full path.
8	jheapprof: unexpected error occurred: <*cause-of-error*>	An unexpected error occurred during execution of the `jheapprof` command. The following information might be displayed as the cause of the error: `malloc systemcall fail (errno=Y)`: A shortage of work memory occurred. `close systemcall fail (errno=Y)`: An object close error occurred.
9	`jheapprof: can't communicate with process` <*process-ID*>	Communication failed due to an error because there was a problem in the process whose process ID was specified in the argument of the `jheapprof` command. Or, the process whose process ID was specified in the argument of the `jheapprof` command was not found.

No.	Error message	Description
10	*<process-ID>*: `Timeout occurred. Java process not responding`	The process whose process ID was specified in the argument of the `jheapprof` command did not send a response to termination of the process for output of statistics by Hitachi class within a specific amount of time.

Return value

Return value	Description
`0`	The command terminated normally.
`1`	An error occurred in the command.
`2`	There was no response to termination of the process for output of statistics by Hitachi class within a specific amount of time.

Example

This example obtains an extended thread dump with statistics by Hitachi class of a Java program whose process ID is `8662`:

```
jheapprof -p 8662
```

When this command executes, the following message is output asking whether an extended thread dump with statistics by Hitachi class is to be output:

```
Force VM to output HitachiJavaHeapProfile: ? (y/n)
```

To output an extended thread dump with statistics by Hitachi class, enter `Y` or `y`. If any other character is entered, the command terminates without outputting an extended thread dump with statistics by Hitachi class.

```
Force VM to output HitachiJavaHeapProfile: ? (y/n)y
```

When an extended thread dump with statistics by Hitachi class is output, the running Java program displays the following message:

```
Writing Java core to javacore8662.030806215140.txt... OK
```

This Java program outputs an extended thread dump with the following file name in the current folder and then continues its processing:

```
javacoreprocess-ID.date-and-time.txt
```

7.2.5 Notes about log files

- Message logs are not output until the settings of all properties related to log output (beginning with `logger`) have been read successfully from the system definition file (`jp1itslm.properties` or `jp1itslmur.properties`).

  If settings related to log output cannot be read successfully, ITSLM does not output log information to log files. When ITSLM is unable to output information to event logs, it terminates.

- If an invalid value, such as an out-of-range value, is specified in a system definition file property related to log output (beginning with `logger`), ITSLM - Manager or ITSLM - UR assumes the default value and continues operation.

- If you change the value of a system definition file property related to log output (beginning with `logger`) after the applicable properties have been read from the system definition file successfully, the change does not take effect until the process has been restarted.

- If you change the value of any of the following system definition file properties, then before ITSLM is started you must move the folders and files that were output before the change was made to provide an empty system folder inside the message log output folder:
    - `loggerCommandMessageFileCount`
    - `loggerCommandMessageMaxFileSize`
    - `loggerProcessCtrlMessageFileCount`
    - `loggerProcessCtrlMessageMaxFileSize`
    - `loggerWebSystemAnalysisMessageFileCount`
    - `loggerWebSystemAnalysisMessageMaxFileSize`
- For output of log files, ITSLM uses the default character encoding of the host on which ITSLM is running. Characters that are not supported by the default character encoding of the host on which ITSLM is running will result in garbled strings in the log files (garbled information in the log files).

8 Maintenance

This chapter explains ITSLM maintenance tasks, including backing up and restoring ITSLM definition files (system definition files and system configuration properties files), databases, and access logs, as well as migrating definition information and databases when replacing computers.

8.1 Backing up and restoring definition files, databases, and access logs

To be able to restore definition files (system definition files and system configuration properties files), databases, and access logs in the event of a problem in ITSLM, you must first have made backups.

8.1.1 Backing up the definition files

The following are the ITSLM definition files:

- System definition files: `jp1itslm.properties` and `jp1itslmur.properties`
- System configuration properties file: `system_config.properties`

You must back up these definition files manually.

This subsection explains how to back up the definition files.

We recommend that you always back up the system definition files after you have edited them.

(1) Before you start

- Verify that setup of the applicable ITSLM - Manager or ITSLM - UR has been completed.
  For details about how to set up ITSLM - Manager, see *5.1.6 Setting up ITSLM - Manager*; for details about how to set up ITSLM - UR, see *5.1.7 Setting up ITSLM - UR*.

(2) Procedure

To back up the definition files:

1. Copy the definition files to a desired location.
   Copy the following definition files:
   Definition files for ITSLM - Manager:
   - *ITSLM-Manager-installation-folder*`\ mgr\conf\jp1itslm.properties`
   - *ITSLM-Manager-installation-folder*`\ mgr\sdpengine\analysis`*N*#`\conf\system_config.properties`

     #: *N* is a number from 1 through 10.

   Definition files for ITSLM - UR:
   - *ITSLM-UR-installation-folder*`\ ur\conf\jp1itslmur.properties`
   - *ITSLM-UR-installation-folder*`\ ur\sdpengine\collector\conf\system_config.properties`
   - *ITSLM-UR-installation-folder*`\ ur\sdpengine\collector2\conf\system_config.properties`
   - *ITSLM-UR-installation-folder*`\ ur\sdpengine\recorder\conf\system_config.properties`

When you have finished copying the definition files, the task of backing up the definition files is complete.

(3) Supplementary information

- You can back up the definition files regardless of whether ITSLM - Manager or ITSLM - UR services are running.

(4) Related topics

- *8.1.4 Restoring the definition files*

8.1.2 Backing up the database

A command is used to back up a database.

This subsection explains how to back up a database.

We recommend that you back up your database periodically.

(1) Before you start

- Verify that setup of ITSLM - Manager and ITSLM - UR has been completed.
  For details about how to set up ITSLM - Manager, see *5.1.6 Setting up ITSLM - Manager*; for details about how to set up ITSLM - UR, see *5.1.7 Setting up ITSLM - UR*.

(2) Procedure

To back up the database:

1. Terminate all ITSLM - URs that are connect to the ITSLM - Manager whose database is to be backed up.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. On the host on which the ITSLM - Manager whose database is to be backed up is installed, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

3. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) of the ITSLM - Manager whose database is to be backed up.

4. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) of the ITSLM - Manager whose database is to be backed up.

5. Execute the database backup command.
   Execute the following backup command:
   `jslmdbcopy` *absolute-path-of-backup-file*
   For details about the backup command, see *jslmdbcopy (backs up database)* in *9. Commands*.

6. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** that was stopped in step 4.

7. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** that was stopped in step 3.

8. Start all ITSLM - URs that were terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

If the database backup command terminates normally and ITSLM - Manager and the ITSLM - URs start, the task of backing up the database is complete.

(3) Related topics

- *8.1.5 Restoring the database*

8.1.3 Backing up the access logs

Access logs are backed up by executing the standard OS commands for copying files and folders.

This subsection explains how to back up the access logs.

(1) Before you start

- Verify that the setup of ITSLM - Manager and ITSLM - UR has been completed.
  For details about how to set up ITSLM - Manager, see *5.1.6 Setting up ITSLM - Manager*; for details about how to set up ITSLM - UR, see *5.1.7 Setting up ITSLM - UR*.

(2) Procedure

1. Stop the service monitoring that is to be backed up and terminate ITSLM - UR.
2. Using the standard OS commands for copying files and folders, make a backup copy of the `http` folder that is in the folder specified for `accessLogFilePath` in *ITSLM-UR-installation-folder*`\ur\conf\jp1itslmur.properties`.
3. Restart ITSLM - UR.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

Once ITSLM - UR starts, the task of backing up the access logs is complete.

(3) Related topics

- *8.1.7 Restoring the access logs*

8.1.4 Restoring the definition files

If you have a backup of the definition files (system definition files and system configuration properties file) and a problem occurs in ITSLM itself, you can restore the environment to its status before the problem occurred.

You must restore definition files manually.

This subsection explains how to restore the definition files.

(1) Before you start

- Verify that you have backed up the ITSLM - Manager or ITSLM - UR system definition files that are to be restored.

(2) Procedure

To restore the definition files:

1. Terminate the ITSLM - Manager or ITSLM - URs whose definition files are to be restored.
    - If the definition files to be restored belong to ITSLM - Manager, terminate all ITSLM - URs connected to ITSLM - Manager and then terminate ITSLM - Manager.

      For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*; for details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.
    - If the definition files to be restored belong to an ITSLM - UR, terminate only that ITSLM - UR.

      For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.
2. Copy the backup of the definition files to the correct folders to overwrite the existing data.

   The copy destinations are as follows:

   If the definition files to be restored belong to ITSLM - Manager:
    - *ITSLM-Manager-installation-folder*`\ mgr\conf\jp1itslm.properties`
    - *ITSLM-Manager-installation-folder*`\ mgr\sdpengine\analysis`*N*#`\conf \system_config.properties`

      #: *N* is a number from 1 through 10.

   If the definition files to be restored belongs to an ITSLM - UR:
    - *ITSLM-UR-installation-folder*`\ ur\conf\jp1itslmur.properties`
    - *ITSLM-UR-installation-folder*`\ur\ sdpengine\collector\conf \system_config.properties`
    - *ITSLM-UR-installation-folder*`\ur\ sdpengine\collector2\conf \system_config.properties`
    - *ITSLM-UR-installation-folder*`\ur\sdpengine\recorder\conf\system_config.properties`
3. Start the ITSLM - Manager and ITSLM - URs whose definition files were restored.
    - If the restored definition files belong to ITSLM - Manager, start ITSLM - Manager that was terminated in step 1 and then start the ITSLM - URs that were also terminated in step 1.

      For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*; for details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.
    - If the restored definition files belong to an ITSLM - UR, start only that ITSLM - UR.

      For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

If ITSLM - Manager and ITSLM - URs with restored definition files start, the task of restoring the definition files is complete.

(3) Related topics

- *8.3.1 Migrating the ITSLM - Manager definition information*
- *8.3.2 Migrating the ITSLM - UR definition information*

8.1.5 Restoring the database

If you have a backup of the database and a problem occurs in ITSLM itself, you can restore the environment to its status before the problem occurred.

A command is used to restore a database.

This subsection explains how to restore a database.

(1) Before you start

- Verify that you have backed up the database.

(2) Procedure

To restore the database:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager whose database is to be restored.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. On the host on which the ITSLM - Manager whose database is to be restored is installed, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

3. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) of the ITSLM - Manager whose database is to be restored.

4. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) of the ITSLM - Manager whose database is to be restored.

5. Execute the database restore command.
   Execute the following restore command:
   `jslmdbrstr` *absolute-path-of-backup-file*
   For details about the restore command, see *jslmdbrstr (restores database)* in *9. Commands*.

6. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** that was stopped in step 4.

7. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** that was stopped in step 3.

8. Start all ITSLM - URs that were terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

If the database restore command terminates normally and ITSLM - Manager and ITSLM - URs start, the task of restoring the database is complete

(3) Related topics

- *8.3.3 Migrating the database*

8.1.6 Synchronizing the environment setup for a restored database (working with Performance Management)

If ITSLM is linked with Performance Management, when you have restored the ITSLM database or the Performance Management database, you must ensure that these databases are synchronized.

This subsection explains the task that must be performed when the ITSLM database or the Performance Management database has been restored.

(1) Before you start

- Verify that you have backed up the ITSLM database.

(2) Procedure

The procedure for when the ITSLM database has been restored is not the same as the procedure for when the Performance Management database has been restored. If you have restored the Performance Management database, skip step 5.

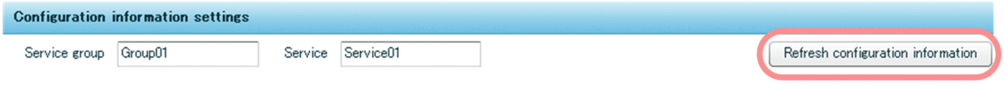
To synchronize the environment setup for a restored database:

1. If PFM - Manager is not running, start it.
   For details about how to start PFM - Manager, see the *Job Management Partner 1/Performance Management User's Guide*.

2. If ITSLM - Manager is not running, start it.
   For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

3. Log in to ITSLM - Manager.
   For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.

4. In the Settings window, display the **Configuration information settings** area, and then click the **Refresh configuration information** button.
   The configuration information for ITSLM - Manager and PFM - Manager are synchronized.


Configuration information settings
Refresh configuration information

Service group Group01 Service Service01

5. If you have restored the ITSLM database, display the **Monitor settings** area and check the settings to see if the database has been restored correctly. If any settings are not correct, correct them.
   Check the following:
   - Whether the items to be monitored are selected correctly and whether the check boxes for the items that are not to be monitored are cleared
   - Whether the threshold and predictive error detection settings are correct for the items that are to be monitored

   If any settings are not correct, correct them, and then click the **Save** button.

6. In the **Start/Stop monitor** area, synchronize the monitoring status (started or stopped) between ITSLM and Performance Management.
   Check all the monitored services whose monitoring is your responsibilities and determine which need monitoring and which do not, then synchronize their monitoring statuses. Perform the following tasks:
   - Monitored services that need to be monitored

In the **Start/Stop monitor** area, click the **Start** button to start monitoring. If monitoring has already started, click the **Stop** button to stop monitoring, and then click the **Start** button to start monitoring. This will cause Performance Management's monitoring settings to become synchronized with ITSLM's most recent monitoring settings.

- Monitored services that do not need to be monitored

  In the **Start/Stop monitor** area, click the **Stop** button to stop monitoring. If the monitoring is already stopped, click the **Start** button to start monitoring, and then click the **Stop** button to stop monitoring. As a result, monitoring stops in both ITSLM and Performance Management.

The task of synchronizing the environment setup for ITSLM and Performance Management databases is complete.

8.1.7 Restoring the access logs

Access logs are restored by executing the standard OS commands for copying files and folders.

This subsection explains how to restore the access logs.

(1) Before you start

- Verify that you have backed up the access logs.

(2) Procedure

1. Stop the service monitoring that was backed up and terminate ITSLM - UR.

2. Using the standard OS commands for copying files and folders, copy the `http` folder that was backed up into the folder specified for `accessLogFilePath` in *ITSLM-UR-installation-folder*`\ur\conf\jp1itslmur.properties`.

   For details about backing up the access logs, see *8.1.3 Backing up the access logs*.

3. Restart ITSLM - UR.

   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

Once ITSLM - UR starts, the task of restoring the access logs is complete.

8.2 Cleaning up the database

If a lot of registration and deletion of monitored services has occurred in ITSLM or errors have occurred during database processing, unneeded data might remain in the database. If a space shortage occurs in the database, you might need to secure more free space by deleting this unneeded data (cleaning up the database).

This section explains how to clean up the database.

8.2.1 Before you start

- Verify that setup of ITSLM - Manager has been completed.
  For details about how to set up ITSLM - Manager, see *5.1.6 Setting up ITSLM - Manager*.
- Verify that ITSLM - Manager is running or the following services are running:
  - Service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`)
  - Service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

  For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

8.2.2 Procedure

To clean up the database:

1. On the host on which the ITSLM - Manager whose database is to be cleaned up is installed, execute the database cleanup command.
   Execute the following cleanup command:
   `jslmmgrdbcleanup`
   For details about the cleanup command, see *jslmmgrdbcleanup (cleans up database)* in *9. Commands*.

If the cleanup command terminates normally, the task of cleaning up the database is complete.

8.3 Migrating definition information and databases

You can migrate definition information and databases to a different host than the one on which ITSLM is installed.

This section explains how to migrate ITSLM definition information and databases using the backup and restore processing that was explained in *8.1 Backing up and restoring definition files, databases, and access logs*.

8.3.1 Migrating the ITSLM - Manager definition information

This subsection explains how to migrate the ITSLM - Manager definition information from the host on which ITSLM - Manager is installed to another host.

(1) Before you start

- Verify that you have backed up the definition files (system definition files and system configuration properties file) for the ITSLM - Manager whose definition files are to be migrated.

  For details about how to back up the definition files, see *8.1.1 Backing up the definition files*.
- On the target host, install and set up ITSLM - Manager.

  For details about how to install and set up ITSLM - Manager, see *5.1.5 Installing ITSLM* and *5.1.6 Setting up ITSLM - Manager*.

(2) Procedure

To migrate the ITSLM - Manager definition information:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager on the host to which the definition information is to be migrated.

   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. On the target host to which the definition information is to be migrated, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

3. On the target host to which the definition information is to be migrated, stop the ITSLM - Manager service **JP1/ ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).

4. On the target host to which the definition information is to be migrated, stop the ITSLM - Manager service **JP1/ ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).

5. Copy the backup of the definition files to the correct folders on the target host.

   Copy the backup to the following locations:

   - *ITSLM-Manager-installation-folder*`\mgr\conf\jp1itslm.properties`
   - *ITSLM-Manager-installation-folder*`\ mgr\sdpengine\analysis`*N*#`\conf\system_config.properties`

   #: *N* is a number from 1 through 10.

6. Of the restored definition files, edit the `jp1itslm.properties` system definition file.

   In the `jp1itslm.properties` system definition file, edit the `managerHost` and `rmiManagerPort` properties as appropriate for the migration target.

   For details about how to edit the system definition file, see *5.6.1 Editing the system definition files*.

7. Terminate the ITSLM - URs that are connected to the source ITSLM - Manager from which definition information was migrated.

   For details about the termination method, see *2.1.3 Terminating ITSLM - UR*.

8. Edit the `jp1itslmur.properties` system definition files for the ITSLM - URs that were terminated in step 1.

   In these system definition files, edit the `managerHost` and `rmiManagerPort` properties as appropriate for the migration target of ITSLM - Manager.

   For details about how to edit the system definition files, see *5.6.1 Editing the system definition files*.

9. Terminate the source ITSLM - Manager from which definition information was migrated.

   For details about the termination method, see *2.1.4 Terminating ITSLM - Manager*.

10. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) that was stopped in step 4.

11. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) that was stopped in step 3.

12. Start all ITSLM - URs that were terminated in step 1.

    For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

If ITSLM - Manager and the ITSLM - URs start, the task of migrating the ITSLM - Manager definition information is complete.

(3) Next task

- *8.3.3 Migrating the database*

(4) Related topics

- *8.3.2 Migrating the ITSLM - UR definition information*
- *8.5.1 Changing ITSLM - Manager's RMI communication port number*
- *8.5.3 Changing the listen port number of the ITSLM - Manager embedded database*
- *8.5.4 Changing the listen port number of the ITSLM - Manager embedded Web server*
- *8.5.5 Changing the port number of the internal communications port of the ITSLM - Manager embedded Web server*
- *8.5.6 Changing the port number of the completion-message receiving port of the ITSLM - Manager embedded Web server*

8.3.2 Migrating the ITSLM - UR definition information

This subsection explains how to migrate the ITSLM - UR definition information from the host on which ITSLM - UR is installed to another host.

(1) Before you start

- Verify that you have backed up the definition files (system definition files and system configuration properties file) for the ITSLM - UR whose definition files are to be migrated.

  For details about how to back up the definition files, see *8.1.1 Backing up the definition files*.

- On the target host, install and set up ITSLM - UR.
  For details about how to install and set up ITSLM - UR, see *5.1.5 Installing ITSLM* and *5.1.7 Setting up ITSLM - UR*.

(2) Procedure

To migrate the ITSLM - UR definition information:

1. Terminate ITSLM - UR on the target host to which the definition information is to be migrated.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. Copy the backup of the definition files to the correct folders on the target host.
   Copy the backup to the following locations:
   - *ITSLM-UR-installation-folder*`\ur\conf\jp1itslmur.properties`
   - *ITSLM-UR-installation-folder*`\ ur\sdpengine\collector\conf\system_config.properties`
   - *ITSLM-UR-installation-folder*`\ ur\sdpengine\collector2\conf\system_config.properties`
   - *ITSLM-UR-installation-folder*`\ ur\sdpengine\recorder\conf\system_config.properties`

3. Of the restored definition files, edit the `jp1itslmur.properties` system definition file.
   In the `jp1itslmur.properties` system definition file, edit the following properties as appropriate for the migration target:
   - `managerHost`
   - `rmiManagerPort`
   - `urHost`
   - `rmiUrPort`
   - `urNetworkInterfaceNumber`

   For details about how to edit the system definition file, see *5.6.1 Editing the system definition files*.

4. Terminate the ITSLM - UR on the source host from which the definition information was migrated.
   For details about the termination method, see *2.1.3 Terminating ITSLM - UR*.

5. Start ITSLM - UR on the target host to which the definition information was migrated.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

If ITSLM - UR starts, the task of migrating the ITSLM - UR definition information is complete.

(3) Related topics

- *8.3.1 Migrating the ITSLM - Manager definition information*
- *8.5.2 Changing ITSLM - UR's RMI communication port number*

8.3.3 Migrating the database

This subsection explains how to migrate the database from a host on which ITSLM is installed to another host.

(1) Before you start

- Verify that you have backed up the database.

For details about how to back up the database, see *8.1.2 Backing up the database*.

- Copy the database backup files to a desired location on the target host.
- Install and set up ITSLM - Manager on the target host.
  For details about how to install and set up ITSLM - Manager, see *5.1.5 Installing ITSLM* and *5.1.6 Setting up ITSLM - Manager*.

(2) Procedure

To migrate the database:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager on the host to which the database is to be migrated.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.
2. On the target host to which the database is to be migrated, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
3. On the target host to which the database is to be migrated, stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).
4. On the target host to which the database is to be migrated, stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).
5. On the target host to which the database is to be migrated, execute the database restore command.
   Execute the following restore command:
   `jslmdbrstr` *absolute-path-of-backup-file*
   For details about the restore command, see *jslmdbrstr (restores database)* in *9. Commands*.
6. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** that was stopped in step 4.
7. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** that was stopped in step 3.
8. Start all ITSLM - URs that were terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

8.3.4 Migrating the service monitor information in the database

The database on the host on which ITSLM - Manager is installed contains various data needed for monitoring monitored services.

If you migrate your system from a test environment to an actual operating environment or if you replace your machine due to a change in the system configuration, you must migrate the *service monitor information* (*monitored service management information and service performance*) that is stored in the database.

The management information for each monitored service that is included in the service monitor information is as follows:

- Name of the monitored service
- Name of the service group to which the monitored service belongs
- Host name and IP address of the Web server that provides the monitored service
- Relative URI of the monitored service

- IP address of the ITSLM - UR that acquires service performance
- Monitoring item settings for the monitored service (including Web transactions)
- Business group definition information (business group definition information for ITSLM - Manager that is associated with the monitored service; this information is applicable when ITSLM is linked with Performance Management)
- Availability monitoring information (availability monitoring information collected by PFM - Agent for Service Response that is associated with the monitored service; this information is applicable when ITSLM is linked with Performance Management)
- Report template information

This subsection explains how to migrate the service monitor information in the database from the host on which ITSLM - Manager is installed to another host.

(1) Before you start

- Verify that ITSLM - Manager is running or the following services are running on the target host:
  - Service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`)
  - Service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

  For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.
- On the target host, install and set up ITSLM - Manager.
  For details about how to install and set up ITSLM - Manager, see *5.1.5 Installing ITSLM* and *5.1.6 Setting up ITSLM - Manager*.

(2) Procedure

To migrate the service monitor information in the database:

1. On the source host, execute the service monitor information export command to create an export file.
   Execute the following export command:
   `jslmmgrexport [ -g` *service-group-name* `-s` *service-name* `]`
   `-t {` *export-period* `| all | none }`
   `-o` *output-file-name*
   `[ -f ]`
   For details about the export command, see *jslmmgrexport (exports service monitor information)* in *9. Commands*.

2. Copy the export file to the target host.
   Copy the export file to a desired location (using any method of copying).

3. On the target host, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

4. Start the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

5. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).

6. On the target host, execute the service monitor information import command to import the export file copied in step 2 (*import-data-file-name*).
   Execute the following import command:

```
jslmmgrimport -i import-data-file-name
[ -g service-group-name -s service-name ]
[ -m [ IP-address-of-Web-server IP-address-of-ITSLM - UR ] ]
[ -p ]
```

For details about the import command, see *jslmmgrimport (imports service monitor information)* in *9. Commands*.

If the import command terminates normally, the task of migrating the service monitor information in the database is complete.

(3) Supplementary information

- For the information listed below that is used when ITSLM is linked with Performance Management, the `jslmmgrimport` command processing depends on whether the migration target already contains the data to be imported.

Table 8–1: jslmmgrimport command processing

No.	Information to be imported	Processing	
		The migration target contains the data to be imported	The migration target does not contain the data to be imported
1	Business group definition information	Updates the business group definition information with the imported data. The check box settings for business groups are updated only if the check boxes are cleared in the existing data (if check boxes are selected in the exiting data, those check box settings are not updated).	Imports the data as is.
2	Availability monitoring information	Updates the contents of measurement condition labels while maintaining the selection status of the availability monitoring information.	Imports the data as is and keeps the availability monitoring information unselected.
3	Report template information	Updates the report template information with the imported data regardless of the default template or user-created templates.	Imports the data as is.

- If performance data is migrated from ITSLM version 09-51 or earlier, the monitoring item names are displayed as shown below.

Table 8–2: Monitoring item names when performance data is migrated

No.	ITSLM version	
	Monitoring item name in version 09-51	Monitoring item name in version 10-00
1	**Measured**	**Measured (max)**
2	**SLO threshold value**	**Threshold**
3	**Baseline**	**Baseline**

8.4 Renaming hosts

This section explains how to rename the hosts on which ITSLM - Manager and ITSLM - UR are installed.

8.4.1 Renaming the ITSLM - Manager host

This subsection explains how to rename the ITSLM - Manager host.

Note that step 1 is required when ITSLM is linked with Performance Management. If your ITSLM is not linked with Performance Management, start with step 2.

(1) Before you start

- If the host on which PFM - Manager is installed differs from the host on which ITSLM - Manager is installed, specify the new host name for ITSLM - Manager in the PFM - Manager definition beforehand, and start PFM - Manager. If PFM - Manager and ITSLM - Manager are installed on the same host, there is no need to specify the new host name in the PFM - Manager definition beforehand, because the new host name is specified in the procedure described below.

  To specify the PFM - Manager definition, use PFM - Web Console's Master Manager properties. See the description of the configuration method for linking with ITSLM in the *Job Management Partner 1/Performance Management User's Guide*.

(2) Procedure

To rename the ITSLM - Manager host:

1. If PFM - Manager and ITSLM - Manager are installed on the same host, terminate the PFM - Manager that is linked with the ITSLM - Manager whose host is to be renamed.

   For details about how to terminate PFM - Manager, see the *Job Management Partner 1/Performance Management User's Guide*.

2. Terminate all ITSLM - URs connected to the ITSLM - Manager on the host that is to be renamed.

   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

3. Terminate the ITSLM - Manager whose host is to be renamed.

   For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.

4. Rename the host.

5. Specify the new host name in the `managerHost` property in the `jp1itslm.properties` system definition file for the ITSLM - Manager.

6. Specify the new host name in the `managerHost` property in the `jp1itslmur.properties` system definition file for each ITSLM - UR.

7. Start the ITSLM - Manager that was terminated in step 3.

   For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

8. Start all ITSLM - URs that were terminated in step 2.

   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

If the host on which PFM - Manager is installed differs from the host on which ITSLM - Manager is installed, the task of renaming the host is complete. If PFM - Manager and ITSLM - Manager are installed on the same host, go to step 9.

9. When PFM - Manager and ITSLM - Manager are installed on the same host, start the PFM - Manager that was terminated in step 1.

   For details about how to start PFM - Manager, see the *Job Management Partner 1/Performance Management User's Guide*.

10. When PFM - Manager and ITSLM - Manager are installed on the same host, specify the new host name for ITSLM - Manager in the PFM - Manager definitions.

    To specify the PFM - Manager definition, use PFM - Web Console's Master Manager properties. See the description of the configuration method for linking with ITSLM in the *Job Management Partner 1/Performance Management User's Guide*.

8.4.2 Renaming the ITSLM - UR host

This subsection explains how to rename the ITSLM - UR host.

(1) Procedure

To rename the ITSLM - UR host:

1. Terminate the ITSLM - UR whose host is to be renamed.

   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. Rename the host.

3. Create the `jp1itslm_setup.opt` options file needed for setting up ITSLM - UR and specify the new host name in the `ur_host` definition item.

   The absolute path for the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.

4. Execute the ITSLM - UR setup command.

   Execute the following setup command:

   ITSLM-UR-installation-folder`\ur\bin\jslmursetup` *absolute-path-of-options-file*

   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

5. Start the ITSLM - UR that was terminated in step 1.

   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

8.4.3 Renaming the PFM - Manager host specified in ITSLM (working with Performance Management)

This subsection explains how to change settings in ITSLM when the host on which PFM - Manager is installed is renamed.

(1) Procedure

To rename the PFM - Manager host specified in ITSLM:

1. Stop all monitored services.

   For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

2. Rename the PFM - Manager host.

   For details about how to rename the PFM - Manager host, see the description of how to rename the PFM - Manager host in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

   > **Important note**
   >
   > When you rename the PFM - Manager host, the following are also involved:
   >
   > - PFM - Manager host
   > - PFM - Web Console host
   > - Monitoring agent's host
   > - Monitoring console

3. Stop the following ITSLM - Manager services:

   - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)
   - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

   Stop **JP1/ITSLM - Manager Web Service** first and then stop **JP1/ITSLM - Manager Service**. There is no need to stop **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

   For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.

4. Specify the new PFM - Manager host name in the `pfmManagerHost` property of the `jp1itslm.properties` system definition file for ITSLM - Manager.

5. Start the following ITSLM - Manager services that were stopped in step 3:

   - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
   - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

   Start **JP1/ITSLM - Manager Service** first and then start **JP1/ITSLM - Manager Web Service**.

   For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

6. Start monitoring the monitored services that were stopped in step 1.

8.5 Changing port numbers

This section explains how to change port numbers used in ITSLM.

8.5.1 Changing ITSLM - Manager's RMI communication port number

This subsection explains how to change ITSLM - Manager's RMI communication port number.

(1) Procedure

To change ITSLM - Manager's RMI communication port number:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager whose RMI communication port number is to be changed.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.
2. Terminate the ITSLM - Manager on the host whose RMI communication port number is to be changed.
   For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.
3. Create the `jp1itslm_setup.opt` options file needed for setting up ITSLM - Manager and specify the new RMI communication port number for the ITSLM - Manager in the `manager_port` definition item.
   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.
4. Create the `jp1itslm_setup.opt` options file needed for setting up ITSLM - UR and specify the new RMI communication port number for the ITSLM - Manager in the `manager_port` definition item.
   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes. If you create this options file on the same host as for ITSLM - Manager, store it at a different location from the file created in step 3.
5. Execute the ITSLM - Manager setup command.
   Execute the following setup command:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.
6. Execute the ITSLM - UR setup command.
   Execute the following setup command:
   ITSLM-UR-installation-folder`\ur\bin\jslmursetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.
7. On the host whose RMI communication port number has been changed, change the port number release setting in the firewall.
8. Start the ITSLM - Manager that was terminated in step 2.
   For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.
9. Start all ITSLM - URs that were terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

(2) Related topics

- *A. List of Port Numbers Used by ITSLM*

8.5.2 Changing ITSLM - UR's RMI communication port number

This subsection explains how to change ITSLM - UR's RMI communication port number.

(1) Procedure

To change ITSLM - UR's RMI communication port number:

1. Terminate the ITSLM - UR whose RMI communication port number is to be changed.

   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. Create the `jp1itslm_setup.opt` options file needed for setting up ITSLM - UR and specify the new RMI communication port number for the ITSLM - UR in the `ur_port` definition item.

   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.

3. Execute the ITSLM - UR setup command.

   Execute the following setup command:

   ITSLM-UR-installation-folder`\ur\bin\jslmursetup` *absolute-path-of-options-file*

   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

4. On the host whose RMI communication port number has been changed, change the port number release setting in the firewall.

5. Start the ITSLM - UR that was terminated in step 1.

   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

(2) Related topics

- *A. List of Port Numbers Used by ITSLM*

8.5.3 Changing the listen port number of the ITSLM - Manager embedded database

This subsection explains how to change the listen port number of the ITSLM - Manager embedded database.

(1) Procedure

To change the listen port number of the ITSLM - Manager embedded database:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager whose embedded database listen port number is to be changed.

   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. Terminate the ITSLM - Manager on the host whose embedded database listen port number is to be changed.

For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.

3. Create the `jp1itslm_setup.opt` options file needed for setting up ITSLM - Manager and specify the new embedded database listen port number in the `hdb_port` definition item.

   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.

4. Execute the ITSLM - Manager setup command.
   Execute the following setup command:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

5. Start the ITSLM - Manager that was terminated in step 2.
   For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

6. Start all ITSLM - URs that were terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

(2) Related topics

- *A. List of Port Numbers Used by ITSLM*

8.5.4 Changing the listen port number of the ITSLM - Manager embedded Web server

This subsection explains how to change the listen port number of the ITSLM - Manager embedded Web server.

(1) Procedure

To change the listen port number of the ITSLM - Manager embedded Web server:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

2. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).

3. Create the `jp1itslm_setup.opt` options file needed for setting up ITSLM - Manager and specify the new embedded Web server listen port number in the `psb_Listen` definition item.

   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.

4. Execute the ITSLM - Manager setup command.
   Execute the following setup command:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

5. On the host on which the embedded Web server port number was changed, change the port number release setting in the firewall.

6. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** that was stopped in step 2.

(2) Related topics

- *A. List of Port Numbers Used by ITSLM*

8.5.5 Changing the port number of the internal communications port of the ITSLM - Manager embedded Web server

This subsection explains how to change the port number of the internal communications port of the ITSLM - Manager embedded Web server.

(1) Procedure

To change the internal communications port number of the ITSLM - Manager embedded Web server:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager whose embedded Web server listen port number is to be changed.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

3. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).

4. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).

5. Create the `jp1itslm_setup.opt` options file needed for setting up the ITSLM - Manager and specify the new embedded Web server internal communications port number in the `psb_ connector_port` definition item.
   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.

6. Execute the ITSLM - Manager setup command.
   Execute the following setup command:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.

7. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** that was stopped in step 4.

8. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** that was stopped in step 3.

9. Start the ITSLM - UR that was terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

(2) Related topics

- *A. List of Port Numbers Used by ITSLM*

8.5.6 Changing the port number of the completion-message receiving port of the ITSLM - Manager embedded Web server

This subsection explains how to change the port number of the completion-message receiving port of the ITSLM - Manager embedded Web server.

(1) Procedure

To change the completion-message receiving port number of the ITSLM - Manager embedded Web server:

1. Terminate all ITSLM - URs connected to the ITSLM - Manager whose embedded Web server completion-message receiving port number is to be changed.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.
2. From Windows **Start** menu, select **Administrative Tools**, and then **Services**.
3. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`).
4. Stop the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).
5. Create the `jp1itslm_setup.opt` options file needed for setting up the ITSLM - Manager and specify the new embedded Web server completion-message receiving port number in the `psb_shutdown_port` definition item.
   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.
6. Execute the ITSLM - Manager setup command.
   Execute the following setup command:
   ITSLM-Manager-installation-folder`\mgr\bin\jslmmgrsetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmmgrsetup (sets up ITSLM - Manager)* in *9. Commands*.
7. Start the ITSLM - Manager service **JP1/ITSLM - Manager Service** that was stopped in step 4.
8. Start the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** that was stopped in step 3.
9. Start the ITSLM - UR that was terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

(2) Related topics

- *A. List of Port Numbers Used by ITSLM*

8.5.7 Changing the port number set in ITSLM for the PFM performance data receiving port (working with Performance Management)

This subsection explains the setting that must be changed in ITSLM when the port number for receiving performance data from Performance Management has been changed.

For details about how to change port numbers in Performance Management, see the *Job Management Partner 1/ Performance Management Planning and Configuration Guide*.

(1) Before you start

- Verify that the port number used to send data has been changed in Performance Management and obtain the new port number. For details about how to change port numbers in Performance Management, see the description of installation and setup in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

(2) Procedure

To change the port number set in ITSLM for the PFM performance data receiving port:

1. Stop all monitored services.

   For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

2. On the host on which the port number for the PFM performance data receiving port is to be changed, stop the following ITSLM - Manager services:

   - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)
   - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

   Stop **JP1/ITSLM - Manager Web Service** first and then stop **JP1/ITSLM - Manager Service**. There is no need to stop **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

   For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.

3. Specify the new port number for the PFM performance data receiving port in the `pfmReceivePort` property in ITSLM - Manager's `jp1itslm.properties` system definition file.

4. Start the following ITSLM - Manager services that were stopped in step 2:

   - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
   - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

   Start **JP1/ITSLM - Manager Service** first and then start **JP1/ITSLM - Manager Web Service**.

   For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

5. Start monitoring the monitored services that were stopped in step 1.

8.5.8 Changing the port number set in ITSLM for PFM - Manager's communication port (working with Performance Management)

This subsection explains the setting that must be changed in ITSLM when the Performance Management communication port number used to communicate with ITSLM has been changed.

(1) Procedure

To change the port number set in ITSLM for the PFM - Manager communication port:

1. Stop all monitored services.

   For details about how to stop monitoring, see *4.2.2 Stopping monitoring*.

2. In PFM - Manager, change the port number used to communicate with ITSLM.

For details about how to change communication port numbers in PFM - Manager, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

3. On the host on which the Performance Management communication port number is to be changed, stop the following ITSLM - Manager services:
    - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)
    - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

    Stop **JP1/ITSLM - Manager Web Service** first and then stop **JP1/ITSLM - Manager Service**. There is no need to stop **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

    For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.

4. Specify the new Performance Management communication port number in the `pfmManagerPort` property in ITSLM - Manager's `jp1itslm.properties` system definition file.

5. Start the following ITSLM - Manager services that were stopped in step 3:
    - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
    - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

    Start **JP1/ITSLM - Manager Service** first and then start **JP1/ITSLM - Manager Web Service**.

    For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

6. Start monitoring the monitored services that were stopped in step 1.

8.6 Changing the network interface number

If you have performed any of the following tasks in ITSLM - UR, you must check and, if necessary, revise the network interface number that was specified when ITSLM - UR was set up:

- Added or deleted network interface cards
- Changed network interface settings

This section explains how to change the network interface number in ITSLM - UR.

8.6.1 Before you start

After you have performed any of the tasks listed below, execute the `jslmuripls` command to check the network interface number and IP address:

- Added or deleted network interface cards
- Changed network interface settings

When you obtain the network interface number, check its value against the `urNetworkInterfaceNumber` property value in ITSLM - UR's `jp1itslmur.properties` system definition file to determine if the property value matches the network interface number of the network device that you want to monitor.

Note:

If the `urNetworkInterfaceNumber` property value matches the network interface number of the network device to be monitored, there is no need to change the network interface number.

8.6.2 Procedure

To change the network interface number:

1. Terminate the ITSLM - UR whose network interface number is to be changed.
   For details about how to terminate ITSLM - UR, see *2.1.3 Terminating ITSLM - UR*.

2. Create the options file needed for the setup and specify in the `ur_ni_number` definition item the network interface number that you want to monitor.
   For details about the options file, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.
   The absolute path of the storage of the created options file, including the options file name (any name) at the storage, must not exceed 255 bytes.

3. Execute the ITSLM - UR setup command.
   Execute the following setup command:
   ITSLM-UR-installation-folder`\ur\bin\jslmursetup` *absolute-path-of-options-file*
   For details about the setup command, see *jslmursetup (sets up ITSLM - UR)* in *9. Commands*.

4. Start the ITSLM - UR that was terminated in step 1.
   For details about how to start ITSLM - UR, see *2.1.2 Starting ITSLM - UR*.

Related topics

5.6.2 Editable definitions

8.7 Settings needed when PFM - Agent or PFM - RM is upgraded (working with Performance Management)

If PFM - Agent or PFM - RM has been upgraded and the version of the data model has changed, you must obtain the configuration information in ITSLM - Manager and set up the monitoring items again.

For details about how to obtain the configuration information in ITSLM - Manager, see *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)*.

8.8 Applying changes made to definitions in Performance Management to ITSLM (working with Performance Management)

If definitions have been changed in Performance Management, you must apply the changes to ITSLM.

8.8.1 Applying changes to Performance Management configuration information to ITSLM

If any of the following tasks have been performed in Performance Management, you must apply the changes to the configuration information in ITSLM:

- Added or deleted business groups
- Added or deleted managed hosts
- Added or deleted monitoring agents or PFM - Agents for Service Response
- Added or deleted monitoring items

If the units of the metrics for a monitoring item are changed in Performance Management, you can also use the procedure explained here to apply the changes to ITSLM. However, the names of monitoring items that have already been registered cannot be changed with this procedure.

(1) Before you start

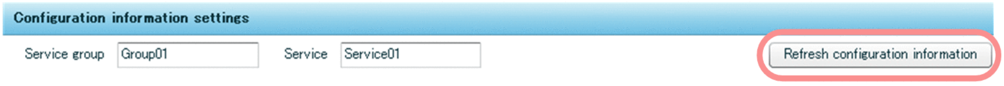
- Verify that you have the service group administrator permissions.
- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.

(2) Procedure

This subsection provides an overview of the flow of the steps in the procedure. For details about each step, see *3.2.5 Setting up the monitoring items for system performance as configuration information (working with Performance Management)*.

To apply to ITSLM changes that have been made to Performance Management configuration information:

1. In the ITSLM window, click the **Settings** button.
2. In the **Setting menu** area, select the **Configuration information settings**.
3. From the **Services** list area, select a monitored service.
4. Click the **Refresh configuration information** button.



Configuration information settings

Service group: Group01 Service: Service01

5. If business groups have been added or deleted in Performance Management, check and specify the associations between monitored services and business groups in **Business groups**.

8.8.2 Applying changes to PFM - Agent for Service Response definitions to ITSLM

If service measurement definitions for availability monitoring have been changed in PFM - Agents for Service Response, you must apply the changes to the configuration information to ITSLM.

This subsection explains the tasks that must be performed in ITSLM when service measurement definitions for availability monitoring have been changed.

(1) Before you start

- Verify that you have the service group administrator permissions.
- Log in to ITSLM - Manager.
  For details about how to log in, see *2.2.1 Logging in to ITSLM - Manager*.

(2) Procedure

This subsection provides an overview of the flow of the steps in the procedure. For details about each step, see *3.2.6 Setting up the monitoring items for availability monitoring as configuration information (working with Performance Management)*.

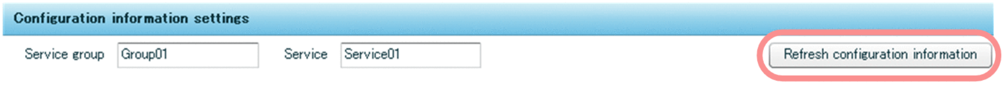
To apply to ITSLM changes that have been made to definitions of PFM - Agents for Service Response:

1. In the ITSLM window, click the **Settings** button.

2. In the **Setting menu** area, select the **Configuration information settings**.

3. From the **Services** list area, select a monitored service.

4. Click the **Refresh configuration information** button.



Configuration information settings

Service group: Group01 Service: Service01

5. Click the **Availability monitor** tab and check and specify the associations between monitored services and business groups in **Measurement conditions**.

8.8.3 Changing the URL of PFM - Web Console

If URL of PFM - Web Console has been changed, you must change the application definition in ITSLM.

(1) Procedure

To change the URL of PFM - Web Console:

1. Change the URL of PFM - Web Console.
   For details about how to change the information constituting the URL of PFM - Web Console, such as host name and IP address, see the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

2. Stop the following ITSLM - Manager services:
   - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

- **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

Stop **JP1/ITSLM - Manager Web Service** first and then stop **JP1/ITSLM - Manager Service**. There is no need to stop **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).

For details about how to terminate ITSLM - Manager, see *2.1.4 Terminating ITSLM - Manager*.

3. Specify the new URL of PFM - Web Console in the `pfmWebConsoleURL` property in ITSLM - Manager's `jp1itslm.properties` system definition file.

4. Start the following ITSLM - Manager services that were stopped in step 2:

- **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
- **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)

Start **JP1/ITSLM - Manager Service** first and then start **JP1/ITSLM - Manager Web Service**.

For details about how to start ITSLM - Manager, see *2.1.1 Starting ITSLM - Manager*.

9 Commands

This chapter explains the syntax of the ITSLM commands.

Format of command explanations

The following describes the items used to explain each command. Note that not all the items are used for some commands.

Function

Explains the function of the command.

Format

Shows the specification format of the command.

Execution permission

Explains the user permissions required to execute the command.

Storage folder

Shows the location at which the command is stored.

Arguments

Explains the command's arguments.

Arguments are case-sensitive (path specifications, however, are not case-sensitive).

Notes

Provides notes about the command.

For the notes common to all commands, see *Notes about command execution*.

Return value

Explains the command's return values.

For details about messages displayed during command execution, see *11.3 Messages*.

Example

Shows an example of specifying the command.

Example output

Shows an example of the command's output.

List of commands

The following table lists and provides an overview of the commands supported by ITSLM.

Table 9–1: List of commands supported by ITSLM

No.	Command name	Target	Overview of function
1	`jslmdbcopy`	Mgr	Backs up the database used in ITSLM.
2	`jslmdbrstr`	Mgr	Restores the database used in ITSLM.
3	`jslmmgrdbcleanup`	Mgr	Deletes unneeded data, including data that remained when monitored services were deleted and data that was created when database errors occurred.
4	`jslmmgrexport`	Mgr	Exports service monitor information needed for data migration.
5	`jslmmgrimport`	Mgr	Imports service monitor information that was exported by the `jslmmgrexport` command.
6	`jslmmgrsetup`	Mgr	Creates an execution environment for ITSLM - Manager.
7	`jslmmgrunsetup`	Mgr	Discards the execution environment for ITSLM - Manager. This command is used when the settings specified during setup are to be changed without uninstalling ITSLM - Manager.
8	`jslmminfoget`	Mgr	Collects error information for ITSLM - Manager and information needed for error analysis.
9	`jslmreport`	Mgr	Outputs report data stored in the database to a CSV file.
10	`jslmurinfoget`	UR	Collects error information for ITSLM - UR and information needed for error analysis.
11	`jslmuripls`	UR	Displays in the command prompt window the network interface number and IP address of the host on which ITSLM - UR is installed. The information displayed by this command is needed for setting up ITSLM - UR.
12	`jslmursetup`	UR	Creates an execution environment for ITSLM - UR.
13	`jslmurunsetup`	UR	Discards the execution environment for ITSLM - UR. This command is used when the settings specified during setup are to be changed without uninstalling ITSLM - UR.

Legend:

Mgr: ITSLM - Manager
UR: ITSLM - UR

Notes about command execution

This section provides notes that apply to all commands.

Important note

For the notes specific to the individual commands (including those that differ from the notes common to all commands), see *Notes* in the explanation of each command.

- If you specify a path in a command argument, you must specify an absolute path. The length of an absolute path must not exceed 255 characters. The following table shows the permitted characters and symbols.

Table 9–2: Characters and symbols permitted for paths in command arguments

No.	Characters and symbols	Remarks
1	Alphanumeric characters	--
2	Space	• If a path contains a space, enclose the entire path in double quotation marks ("). • Folder names cannot begin or end with a space.
3	_ (underscore)	--
4	. (period)	--
5	- (hyphen)	--
6	: (colon)	Can be used only as the drive delimiter.
7	# (hash mark)	--
8	@ (at mark)	--
9	\ (backslash)	Can be used only as the folder delimiter.
10	() (parentheses)	--

Legend:

--: No remarks

Note also that a path cannot contain a folder name or file name that includes a Windows reserved device name (such as AUX, CON, NUL, PRN, CLOCK$, COM1 through COM9, LPT1 through LPT9).

- The commands listed below output messages to message logs as troubleshooting information during their execution. In the event of a problem, check the messages that have been output and take the appropriate corrective action.

  For details about the message logs, see *7.2.3 Message logs*.

  - jslmmgrdbcleanup
  - jslmmgrexport
  - jslmmgrimport
- Do not specify the same file when simultaneously executing multiple commands that perform file input or output.

jslmdbcopy (backs up database)

Function

This command backs up the database used in ITSLM.

The database is configured on the host on which ITSLM - Manager is installed. To be prepared for problems that might occur on the host on which ITSLM - Manager is installed, we recommend that you execute this command periodically to back up the database.

Execute this command under the following conditions:

- The following ITSLM - Manager services are stopped:
  - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
  - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)
- The ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running.

In the case of a cluster system, in addition to the above services, the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`) must also be running. In a cluster system, execute this command on the active server (if the command is executed on the standby server, an error will result).

The command's execution results are output to the following file:

```
ITSLM-Manager-installation-folder\mgr\logs\jslmdbcopy.log
```

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmdbcopy absolute-path-of-backup-file
```

Execution permission

OS's `Administrator` account

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Arguments

absolute-path-of-backup-file

Specifies, enclosed in double quotation marks (`"`), the absolute path for the file to which the backup file is to be output.

Note that this absolute path must begin with a drive name (one character from `A` to `Z` or `a` to `z` or a colon (:)) and must consist of the characters `A` to `Z`, `a` to `z`, `0` to `9`, underscore (_), period (`.`), parentheses (`()`), backslash (`\`), and space. None of the following specifications is permitted:

- Specification in UNC representation

- Specification containing a network drive
- Specification of a drive name only
- Specification containing any of the following Windows and MS-DOS reserved words in folder and file names: `CON`, `PRN`, `AUX`, `CLOCK$`, `NUL`, `COM0`, `COM1`, `COM2`, `COM3`, `COM4`, `COM5`, `COM6`, `COM7`, `COM8`, `COM9`, `LPT0`, `LPT1`, `LPT2`, `LPT3`, `LPT4`, `LPT5`, `LPT6`, `LPT7`, `LPT8`, `LPT9`

If the backup file destination folder specified as the absolute path does not exist, create the folder before you execute the command.

Make sure that the specification does not include any special characters.

Notes

- If a file already exists at the location specified in the argument when this command is executed, that file will be overwritten by the backup file output by the command.
- Do not execute another command, including this command, while this command is executing.
- If execution of this command is canceled by pressing **Ctrl+C**, an incomplete backup file might be created under the folder specified in the argument. If this occurs, delete the corresponding file, stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`), and then restart the service. To stop and start the service, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
- If this command terminates with an error, stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`), and then restart the service. To stop and start the service, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
- If the specified backup file name contains any special character that requires enclosure in quotation marks at the command prompt, a command prompt syntax error message will be displayed and the command might terminate. In such a case, the return value will not necessarily be `1`. The following are the applicable special characters: `&`, `( )`, `[ ]`, `{ }`, `^`, `=`, `;`, `!`, `'`, `+`, `,`, `` ` ``, `~`, `< >`, `@`, and `|`.
- The backup file name must differ from any folder name under the output destination folder specified in *absolute-path-of-backup-file*.
- Do not execute this command when ITSLM - Manager has not been set up.
- If a backup file obtained in an ITSLM - Manager environment is to be restored in another ITSLM - Manager environment, the absolute path of the source RD area folder from which the backup file was obtained must match the absolute path of the target RD area folder to which the backup file is to be restored.
- This command does not apply to access logs. Access logs are backed up using the standard OS commands for copying files and folders. For details about how to make backups, see *8.1.3 Backing up the access logs*.

Return value

Return value	Description
0	Database backup processing terminated normally.
1	Database backup processing failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmdbcopy "C:\Users\Administrator
\Desktop\db\ITSLMBK01"
```

jslmdbrstr (restores database)

Function

This command restores the database used in ITSLM.

In the event of a problem on the host on which ITSLM - Manager is installed, you can restore the environment in effect just before the problem occurred by executing this command.

Execute this command under the following conditions:

- The following ITSLM - Manager services are stopped:
  - **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)
  - **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`)
- The ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running.

In the case of a cluster system, in addition to the above services, the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`) must also be running. In a cluster system, execute this command on the active server (if the command is executed on the standby server, an error will result).

The command's execution results are output to the following file:

```
ITSLM-Manager-installation-folder\mgr\logs\jslmdbrstr.log
```

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmdbrstr absolute-path-of-backup-file
```

Execution permission

OS's `Administrator` account

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Arguments

absolute-path-of-backup-file

Specifies, enclosed in double quotation marks (`"`), the absolute path for the backup file that is to be restored.

Note that this absolute path must begin with a drive name (one character from `A` to `Z` or `a` to `z` or a colon (:)) and must consist of the characters `A` to `Z`, `a` to `z`, `0` to `9`, underscore (_), period (`.`), parentheses (`()`), backslash (\), and space. None of the following specifications is permitted:

- Specification in UNC representation
- Specification containing a network drive

- Specification of a drive name only
- Specification containing any of the following Windows and MS-DOS reserved words in folder and file names:
  `CON`, `PRN`, `AUX`, `CLOCK$`, `NUL`, `COM0`, `COM1`, `COM2`, `COM3`, `COM4`, `COM5`, `COM6`, `COM7`, `COM8`, `COM9`, `LPT0`, `LPT1`, `LPT2`, `LPT3`, `LPT4`, `LPT5`, `LPT6`, `LPT7`, `LPT8`, `LPT9`

Make sure that the specification does not include any special characters.

Notes

- After this command has executed, the target database contains only the restored data.
- Do not execute another command, including this command, while this command is executing.
- Do not cancel execution of this command by pressing **Ctrl**+**C**. If execution of the command is canceled by pressing **Ctrl**+**C**, the database area might become corrupted. If this command is canceled for some reason while its execution is underway, stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`), and then restart the service. To stop and start the service, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.

  If the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** cannot be restarted successfully or ITSLM - Manager does not function normally, the database area might have become corrupted. In such a case, set up ITSLM - Manager again, and then re-execute this command to restore the database.
- If this command terminates with an error, stop the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`), and then restart the service. To stop and start the service, from the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
- If the specified backup file name contains any special character that requires enclosure in quotation marks at the command prompt, a command prompt syntax error message will be displayed and the command might terminate. In such a case, the return value will not necessarily be `1`. The following are the applicable special characters: `&`, `( )`, `[ ]`, `{ }`, `^`, `=`, `;`, `!`, `'`, `+`, `,`, `` ` ``, `~`, `< >`, `@`, and `|`.
- Do not execute this command when ITSLM - Manager has not been set up.
- If a backup file obtained in an ITSLM - Manager environment is to be restored in another ITSLM - Manager environment, the absolute path of the source RD area folder from which the backup file was obtained must match the absolute path of the target RD area folder to which the backup file is to be restored.

Return value

Return value	Description
`0`	Database restore processing terminated normally.
`1`	Database restore processing failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmdbrstr "C:\Users\Administrator
\Desktop\db\ITSLMBK01"
```

jslmmgrdbcleanup (cleans up database)

Function

This command deletes unneeded data, including the data that remained when monitored services were deleted and data that was created when database errors occurred. By deleting unneeded data, you can obtain free space for the database.

To use the database area efficiently, we recommend as a guideline that you execute this command every two months.

Execute this command while the following ITSLM - Manager services are running:

- **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`)
- **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

In a cluster system, execute this command on the active server (if the command is executed on the standby server, an error will result).

`jslmmgrdbcleanup` is set as the identifier in the messages that this command outputs to the message logs.

For details about the message logs, see *7.2.3 Message logs*.

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmmgrdbcleanup
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Notes

- Do not execute another command while this command is executing, except for the `jslmminfoget` command.
- This command does not apply to access logs. Access logs are deleted using the standard OS commands for deleting files and folders.

Return value

Return value	Description
0	Database cleanup processing terminated normally.
1	Database cleanup processing failed.
130	The import processing was canceled because **Ctrl**+**C** was pressed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrdbcleanup
```

jslmmgrexport (exports service monitor information)

Function

This command exports service monitor information needed for data migration. This export processing can be performed for a single monitored service or for all monitored services.

Execute this command while the following ITSLM - Manager services are running:

- **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`)
- **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

In a cluster system, execute this command on the active server (if the command is executed on the standby server, an error will result).

`jslmmgrexport` is set as the identifier in the messages this command outputs to the message logs.

For details about the message logs, see *7.2.3 Message logs*.

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmmgrexport [ -g service-group-name -s service-name ]
                -t { export-period | all | none }
                -o output-file-name
                [ -f ]
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Arguments

`-g` *service-group-name*

Specifies the name of the service group to which the monitored service to be exported belongs. If a nonexistent service group name is specified, an error results. A name beginning with a hyphen (`-`) cannot be specified.

When you specify this option, you must also specify the `-s` option.

To export service monitor information for all monitored services, omit both this option and the `-s` option. However, if no monitored services have been registered in ITSLM, executing this command with this option and the `-s` option both omitted results in an error.

`-s` *service-name*

Specifies the name of the monitored service whose service monitor information is to be exported. If a nonexistent service name is specified, an error results. A name beginning with a hyphen (`-`) cannot be specified.

When you specify this option, you must also specify the `-g` option.

To export service monitor information for all monitored services, omit both this option and the `-g` option. However, if no monitored services have been registered in ITSLM, executing this command with this option and the `-g` option both omitted results in an error.

`-t`

Specifies the period for which service performance data is to be exported. The following explains the specification method.

- *export-period*

  Specifies the number of days whose service performance data is to be exported.

  The permitted value is from `1` through `60` (numeric characters). If the specified value is not within this range, an error results.

  The command exports as many days' worth of past service performance data as specified here, using the time the date value changes as the reference. The data at the reference time is excluded. The time is based on the local time of the computer used to execute the command.

  The following table shows the relationship between when the command is executed and the period subject to export processing.

Table 9–3: Relationship between when the command is executed and the period subject to export processing

No.	Example specification	Command execution date and time	Reference date and time	Period subject to export processing
1	`1`	2011/11/15 00:00:00	2011/11/15 00:00:00	2011/11/14 00:00:00 through 2011/11/14 23:59:59
2	`7`	2011/11/15 12:34:56	2011/11/15 00:00:00	2011/11/08 00:00:00 through 2011/11/14 23:59:59
3	`30`	2011/11/15 23:59:59	2011/11/15 00:00:00	2011/10/16 00:00:00 through 2011/11/14 23:59:59

- `all`

  Specifies that all service performance data that has been accumulated in the database is to be exported.

- `none`

  Specifies that no service performance data is to be exported.

`-o` *output-file-name*

Specifies as an absolute path the name of the output file to which the data is to be exported. Specification in UNC representation is not supported.

The command collects the data to be exported and then outputs it in binary format to the specified file.

The service performance information subject to export processing consists of real-time information and past information. After a period of a specific amount of time, service performance information is compressed and then retained as past information. Any information whose age is less than the specific amount of time is retained as real-time information without being compressed. Therefore, the size of the output file changes even when the service monitor information is the same because the amount of real-time data varies depending on when the command is executed.

`-f`

Specifies that if the output file specified in the `-o` option already exists, that file is to be overwritten with the export data.

If this option is omitted and the specified output file already exists, the command results in an error.

Notes

- This command's processing and the following operations are mutually exclusive:
  - Registering and deleting monitored services
  - Registering and deleting Web transactions
  - Editing Web transactions (including changing their order)
  - Adding, editing, copying, and deleting report templates
  - Updating configuration information
  - Saving monitoring item settings for system performance
  - Setting up service performance monitoring
  - Setting up system performance monitoring
  - Setting up availability monitoring

  If this command is executed while any mutually exclusive processing is underway, the command results in an error and its processing is canceled. Similarly, if any mutually exclusive processing is launched while this command is executing, that processing results in an error and is canceled.
- Do not change the exported data. If the exported data is changed, it can no longer be used for import processing.
- Do not execute another command while this command is executing, except for the `jslmminfoget` command.
- Do not cancel execution of this command by closing the command prompt that is executing this command or by pressing **Ctrl**+**C** on the keyboard.
- If this command was canceled while its execution was underway, do not use the `jslmmgrimport` command to import the export data file that was partially created by this command.
- This command cannot be used to export access logs.

Return value

Return value	Description
`0`	Export processing terminated normally.
`1`	Export processing failed.
`130`	The import processing was canceled because **Ctrl**+**C** was pressed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrexport -g GroupA -s
ServiceA -t 1 -o D:\data\itslm_export
```

jslmmgrimport (imports service monitor information)

Function

This command imports service monitor information that was exported by the `jslmmgrexport` command.

You can import the data that was exported for a monitored service by the `jslmmgrexport` command as is or by specifying the name of a monitored service and the name of the service group to which the monitored service is to belong. If data was exported for all monitored services, you import that data without specifying a monitored service name or service group name.

For both import methods, the command processing depends on whether the name of an exported monitored service or the name of an exported service group to which the monitored service belongs that is contained in the data to be imported already exists at the import destination.

The following table describes the processing when service monitor information is imported.

Table 9–4: Processing when service monitor information is imported

No.	Data to be imported	Whether the name of a monitored service or the name of the service group to which the monitored service belongs that is contained in the data to be imported already exists at the import destination	
		Exists#	Does not exist
1	Monitored service management information	Data is imported according to the specified `-m` option.	Target data is imported as is.
2	Performance data and list of events	Data is imported according to the specified `-p` option.	

#

If the import target already contains a monitored service with the same name as one that is in the data to be imported, monitoring of that monitored service must be stopped.

A monitored service added by import processing is applied to the windows at the time of login.

If you need to change definition information for a monitored service because the IP address of the Web server that provides the monitored service or the IP address of ITSLM - UR has changed, you can edit the definition information in the imported data. However, if the imported data was created by exporting information for all monitored services, the definition information cannot be edited.

Execute this command while the following ITSLM - Manager services are running:

- **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`)
- **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`)

In a cluster system, execute this command on the active server (if the command is executed on the standby server, an error will result).

`jslmmgrimport` is set as the identifier in the messages this command outputs to the message logs.

For details about the message logs, see *7.2.3 Message logs*.

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmmgrimport -i import-data-file-name
             [ -g service-group-name -s service-name ]
             [ -m [ IP-address-of-Web-server IP-address-of-ITSLM-UR ] ]
             [ -p ]
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Arguments

`-i` *import-data-file-name*

Specifies as an absolute path the name of the file from which data is to be imported. Specification in UNC is not supported.

If the specified file does not exist, is not accessible, or does not contain valid data exported by the `jslmmgrexport` command, an error results.

`-g` *service-group-name*

Specifies the name of the service group to which the target monitored service belongs.

If both this option and the `-s` option are omitted, the command uses the appropriate value from the data that is to be imported as is.

If the data to be imported is for all monitored services, do not specify either the `-s` option or the `-g` option. If these options are specified in such a case, an error results.

You can specify for the name of the service group a name that differs from the one used for the export processing. However, the specified name must be a string of characters that does not include the characters `"`, `/`, `[`, `]`, `;`, `:`, `|`, `=`, `,`, `+`, `?`, `<`, `>`, space, tab, machine-dependent characters, and control characters. If the specified name does not observe this limitation, an error results. Also, a name beginning with a hyphen (`-`) cannot be specified.

`-s` *service-name*

Specifies the name of the target monitored service.

This option can be omitted together with the `-g` option. If this option is omitted, the command uses the value from the data that is to be imported as is.

If the data to be imported is for all monitored services, do not specify either the `-s` option or the `-g` option. If these options are specified in such a case, an error results.

You can specify for the name of the monitored service a name that differs from the one used for the export processing. However, the specified name must be a string of no more than 64 characters that does not include the characters `"`, `,`, `'`, `\`, space, tab, machine-dependent characters, and control characters. If the specified name does not observe this limitation, an error occurs. Also, a name beginning with a hyphen (`-`) cannot be specified.

`-m`

Specifies that if the import target already contains a monitored service with the same name as in the data to be imported, the imported data is to overwrite the management information for that monitored service.

If the import target contains a Web transaction with the same name as in the data to be imported, the display order in effect at the import target remains in effect. If the import target does not contain a Web transaction with the same name, the imported data is added following the Web transactions already registered at the import target.

If this option is omitted and the import target already contains both the name of the service group to which the monitored service specified in the `-g` option belongs and the name of the monitored service specified in the `-s` option, the command results in an error.

An error also occurs if import processing will result in the number of Web transactions for a service exceeding 10 (which is the maximum value).

This option is also used to change in the monitored service management information the IP address of the Web server that provides the monitored service and the IP address of ITSLM - UR. The following shows the specification method.

- IP address of Web server

  Specify the new IP address of the Web server that will be providing the monitored service. The specification format is as follows:

  `XXX.XXX.XXX.XXX`

  Legend:

  XXX: A number from `0` through `255`

  If the value is specified in any other format, an error results.

- IP address of ITSLM - UR

  Specify the new IP address of ITSLM - UR. The specification format is as follows:

  `XXX.XXX.XXX.XXX`

  Legend:

  XXX: A number from `0` through `255`

  If the value is specified in any other format, an error results.

When data exported for multiple monitored services is to be imported or the number of Web transactions per monitored service exceeds 10 as a result of import processing, specifying this option results in an error.

A service in a system monitoring configuration cannot be imported as a service in a service monitoring configuration by specifying the IP address of the Web server and the IP address of ITSLM - UR. Similarly, a service in a service monitoring configuration cannot be imported as a service in a system monitoring configuration.

`-p`

Specifies that service performance is to be imported.

When this option is specified and the import target contains a monitored service whose name is the same as a name in the data to be imported, this option overwrites with the imported data the performance of the existing monitored service within the range of the service performance information contained in the imported data. When overwrite import processing is performed, only the data that is within the retention period is imported based on the data with the most recent time, and any data whose retention period has expired is not imported.

The command does not import service performance when this option is omitted, in which case the command imports only management information for monitored services.

Notes

- The definition information that is edited by this command is the information contained in the imported data. The file from which the data was exported is not edited.
- This command's processing and the following operations are mutually exclusive:
  - Registering and deleting monitored services
  - Registering and deleting Web transactions
  - Editing Web transactions (including changing their order)
  - Starting monitoring of a monitored service that is subject to overwrite import processing because the `-m` option is specified
  - Adding, editing, copying, and deleting report templates
  - Updating configuration information
  - Saving monitoring item settings for system performance
  - Setting up service performance monitoring
  - Setting up system performance monitoring
  - Setting up availability monitoring

  If this command is executed while any mutually exclusive processing is underway, the command results in an error and its processing is canceled. Similarly, if any mutually exclusive processing is launched while this command is executing, that processing results in an error and is canceled.
- This command can import data that was exported by ITSLM - Manager version 09-51 or later.
- Do not execute another command while this command is executing, except for the `jslmminfoget` command.
- Do not cancel execution of this command by closing the command prompt that is executing this command or by pressing **Ctrl**+**C** on the keyboard.
- If this command is canceled while it is executing, partially processed data might remain in the database. If you canceled this command while its execution was underway, clean up the database to delete any unneeded data.

  For details about cleaning up the database, see *jslmmgrdbcleanup (cleans up database)*.

  When this command has been canceled, rollback processing is performed on the database. Therefore, if this command, any mutually exclusive command, or a window operation is performed while rollback processing is underway, a database error will occur. If a database error occurs during command execution or during a window operation after this command has been canceled, wait a while, then re-execute the command or operation.
- This command does not check whether a service group with the name specified in the `-g` option already exists. For this reason, import processing can be performed even though a nonexistent service group name is specified. To manipulate such a monitored service, use JP1/Base to register its service group (JP1 resource group) name.

Return value

Return value	Description
`0`	Import processing terminated normally.
`1`	Import processing failed.
`130`	The import processing was canceled because **Ctrl**+**C** was pressed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrimport -i D:\data
\itslm_export -g GroupA -s ServiceA -m 10.150.100.10 10.150.200.20 -p
```

jslmmgrsetup (sets up ITSLM - Manager)

Function

This command creates an execution environment for ITSLM - Manager. It can also be used to reconfigure the execution environment for an existing ITSLM - Manager.

You execute this command after you have installed ITSLM - Manager.

The command execution results are output to the standard output and displayed in the console window. For details about the messages displayed during command execution, see *11.3 Messages*.

The command performs one of the following processes, depending on the status of the execution environment at the time of command execution:

Creates an execution environment (when there is no existing execution environment):

> This command creates an execution environment when it is executed immediately after ITSLM - Manager has been newly installed or after the execution environment for ITSLM - Manager was discarded by unsetup processing.

Reconfigures the existing execution environment (when an execution environment already exists):

> If this command is executed when the execution environment for a configured ITSLM - Manager already exists, the command reconfigures the existing execution environment for ITSLM - Manager.
>
> You reconfigure the execution environment in the following cases:
>
> - The host name, IP address, or port number settings in the execution environment for a configured ITSLM - Manager are to be changed
> - The embedded Web server environment in the execution environment for a configured ITSLM - Manager is to be reconfigured
> - The execution environment for a configured ITSLM - Manager is to be reconfigured after an upgrade installation was performed
>
> Note that an RD area for the embedded database is not created when the ITSLM - Manager execution environment is reconfigured.

Format

```
jslmmgrsetup [ -c { online | standby } ] absolute-path-of-options-file
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Arguments

-c

Specifies that the execution environment used in a cluster system is to be configured. The specification method is as follows:

- `online`

Specifies that the execution environment for the active system is to be configured or reconfigured.

When a new execution environment is configured for the active system, an RD area for the embedded database is created.

- standby

  Specifies that the execution environment for the standby system is to be configured or reconfigured.

  When a new execution environment is configured for the standby system, an RD area for the embedded database is not created.

absolute-path-of-options-file

Specifies the absolute path for an options file that is to be created in text format. This file can be stored at any desired location. The absolute path of the options file storage location must be a maximum of 255 bytes of characters, including the file name (any name).

An options file template is stored at the following location:

```
ITSLM-Manager-installation-folder\mgr\template\mgr\conf\jp1itslm_setup.opt
```

The following shows the definitions in the options file:

```
manager_host=host-name-or-IP-address-of-ITSLM-Manager
manager_port=port-number-of-ITSLM-Manager
psb_Listen=listen-port-number-of-embedded-Web-server
psb_ServerName=host-name-or-IP-address-of-embedded-Web-server
psb_connector_port=port-number-of-internal-communications-port-of-embedded-
Web-server
psb_shutdown_port=port-number-of-completion-message-receiving-port-of-
embedded-Web-server
hdb_port=listen-port-number-of-embedded-database
hdb_area_path=RD-area-folder-name-of-embedded-database
hdb_share_area_path=path-of-shared-folder-for-creating-RD-area-for-embedded-
database-when-running-in-cluster-system
hdb_area_size=capacity-of-embedded-database-area
```

The following table provides the details of the definition items.

Table 9–5: Details of definition items in options file for ITSLM - Manager

No.	Definition item	Specification	Description	Default value
1	manager_host	R	Specifies the host name or IP address of the host on which ITSLM - Manager is installed, as the information for identifying ITSLM - Manager's execution environment. If ITSLM is running in a cluster system, specify the logical host name or logical IP address.	--
2	manager_port	O	Specifies the port number used by ITSLM - Manager, as a number in the range from 1 through 65535.#1	20904
3	psb_Listen	O	Specifies the listen port number used by the embedded Web server, as a number in the range from 1 through 65535.#2	20900
4	psb_ServerName	R	Specifies the host name or IP address of the embedded Web server.	localhost

No.	Definition item	Specification	Description	Default value
5	psb_connector_port	O	Specifies the port number of the internal communications port of the embedded Web server, as a number in the range from 1 through 65535.[#1]	20901
6	psb_shutdown_port	O	Specifies the port number of the completion-message receiving port of the embedded Web server, as a number in the range from 1 through 65535.[#1]	20902
7	hdb_port	O	Specifies the listen port number used by the embedded database, as a number in the range from 5001 through 65535. An error results if any of the following numbers is specified: • Number outside the permitted range • Port number that is already specified in the services file • Port number that is already in use Note that if an ephemeral port number (port number that can be used freely temporarily) is specified, that port number might correspond to a port number already in use.	20903
8	hdb_area_path[#3]	R	Specifies the absolute path of the folder storing the RD area for the embedded database. Specify a folder on the local disk as 1 to 130 characters. This value must begin with a drive name (one character from A to Z or a to z or a colon (:)) and consist of the characters A to Z, a to z, 0 to 9, underscore (_), period (.), parentheses (()), backslash (\), and space. None of the following is permitted: • Specification in UNC representation • Specification containing a network drive • Specification of a drive name only • Specification containing the ITSLM - Manager installation folder • Specification containing an ITSLM - UR installation folder	--
9	hdb_share_area_path[#3]	CR	Specifies the path of the shared folder in which an RD area for the embedded database is to be created when running in a cluster system. The same absolute path must be specified for both the active and standby systems. If ITSLM is running in a non-cluster system, specification of this definition item is ignored. The path must be expressed as a maximum of 110 characters. This value must begin with a drive name (one character from A to Z or a to z or a colon (:)) and consist of the characters A to Z, a to z, 0 to 9, underscore (_), period (.), parentheses (()), backslash (\), and space. None of the following is permitted: • Specification in UNC representation • Specification containing a network drive • Specification of a drive name only	--

No.	Definition item	Specification	Description	Default value
9	`hdb_share_area_path`#3	CR	• Specification containing the ITSLM - Manager installation folder • Specification containing an ITSLM - UR installation folder	--
10	`hdb_area_size`#3	O	Specifies the size of the embedded database area for storing the data handled by ITSLM - Manager. Specify an integer in the range from `5000` through `1048575` (MB). If the specified value is not within this range, an error results. Specify for this definition a value that is equal to or greater than the value estimated in *How to estimate the size of the database area* below. If a large value is specified, database initialization processing will require more time at setup. This definition is ignored when the execution environment is being reconfigured.	`39000`

Legend:

R: Specification is required.

O: Specification is optional.

CR: Specification is required when running in a cluster system.

--: Not applicable

#1

If the specified value is not within the permitted range, setup is completed, but an error occurs when the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) starts.

#2

If the specified value is not within the permitted range, setup is completed, but an error occurs when the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) starts.

#3

If you are reconfiguring the execution environment for a configured ITSLM - Manager, do not change the existing value.

Notes

- If an error occurs during setup, eliminate the cause of the error and re-execute the command. If configuration of a new execution environment has failed and command arguments are to be changed from those used during the previous execution, first undo the setup, and then re-execute the command.
- The options file used during setup is renamed `jp1itslm_setup.opt` after command execution and stored at the following location:

```
ITSLM-Manager-installation-folder\mgr\conf\jp1itslm_setup.opt
```

- Do not execute another command, including this command, while this command is executing.
- If the folder shown below contains a system definition file, the command renames that system definition file by adding `.bk`, saves it in the same folder, and then creates a new system definition file:

```
ITSLM-Manager-installation-folder\mgr\conf\
```

  If a file with the same name already exists when the system definition file is saved, the existing file is overwritten. If the file save processing fails, setup fails. The values of definition items contained in the saved system definition file are inherited to the new system definition file. However, for the definition items that were specified in the system definition file when the command was executed, the specified values are set. Comments are not inherited.

- Do not terminate setup processing by pressing **Ctrl**+**C** or closing the window. Also, in the event of an error, wait until setup is completed before proceeding.
- Before you start the setup processing, terminate all other resident software programs, including other installers and applications (other applications include the `jslmursetup` and `jslmurunsetup` commands).
- If setup is performed with the `-c` option specified in the command and any of a set of specific errors occurs during operation, the Windows services are closed by ITSLM - Manager. For details about the errors that result in a stoppage of the Windows services, see *6.1.3 Failover timing*.
- If a definition item is omitted, its default value is used.
- If you are reconfiguring the execution environment of a configured ITSLM - Manager, make sure that you use any setup option that was used during the previous configuration.
- If you are restoring or migrating the database, specify for the `hdb_area_size` definition item in the options file that is used for setting up the restored environment or target environment for migration a value that is equal to or greater than the value in the backed up environment or source environment for migration.
- For the size of the current database area, see the following file that is created when the `jslmmgrsetup` command is executed:

  ```
  ITSLM-Manager-installation-folder\mgr\conf\jp1itslm_setup.opt
  ```

  Note that this file is updated if setup is performed again (so, if an attempt is made to change the database capacity using an erroneous method, it will no longer be possible to determine the current size).

  Determine the current size from the size of the following folder that was specified in the setup file:

  folder-specified-in-hdb_area_path`\ITSLMSYS04`

Return value

Return value	Description
0	Setup processing terminated normally.
1	Setup processing failed.

Example

When ITSLM is running in a non-cluster system:

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrsetup
C:\Users\Administrator\Desktop\jp1itslm_setup.opt
```

When ITSLM is running in a cluster system:

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrsetup -c online
C:\Users\Administrator\Desktop\jp1itslm_setup.opt
```

How to estimate the size of the database area

Specify in the `hdb_area_size` definition item in the options file a value that is equal to or greater than the value obtained from the formula shown in the figure below.

Figure 9–1: Formula for estimating the size of the database area

Size of database area (MB)

$$= \sum_{i=1}^{n} S_i + 3250$$

Legend:
n: Total number of monitored services in ITSLM - Manager
S_i: Total size for a monitored service

S_i size for a monitored service (MB)

$$= (T + 1) \times 1750 + \uparrow I \div 10 \uparrow \times 1500$$

Legend:
T: Number of Web transactions registered for the monitored service
I: Number of monitoring items for monitoring system performance that are registered for the monitored service

Note:
↑ ↑ means that the calculation result is to be rounded up.
For example, $\uparrow 11 \div 10 \uparrow$ results in a value of 2.

jslmmgrunsetup (undoes ITSLM - Manager setup)

Function

This command discards the execution environment for ITSLM - Manager.

This command is used when the settings specified during setup are to be changed without uninstalling ITSLM - Manager.

The command execution results are output to the standard output and displayed in the console window. For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmmgrunsetup
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Notes

- When this command is executed, the RD area for the embedded database is deleted. If you want to inherit previously accumulated data, such as during re-setup, you must migrate the database.

  For details about migrating the database, see *8.3.3 Migrating the database*.
- If an error occurs during unsetup processing, eliminate the cause of the error and re-execute the command.
- Do not execute another command, including this command, while this command is executing.
- Do not terminate unsetup processing by pressing **Ctrl**+**C** on the keyboard or closing the window. In the event of an error, wait until the unsetup processing is completed before proceeding.
- Before you start unsetup processing, terminate all other resident software programs, including other installers and applications (other applications include the `jslmursetup` and `jslmurunsetup` commands).

Return value

Return value	Description
0	Unsetup processing terminated normally.
1	Unsetup processing failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrunsetup
```

jslmminfoget (collects data needed for investigating the cause of ITSLM - Manager errors)

Function

This command collects error information for ITSLM - Manager and information needed for error analysis.

This command can be executed when ITSLM - Manager setup has been completed.

Use the information collected by executing this command as data when an error has occurred in ITSLM - Manager and you need to contact the system administrator.

The command execution results are output to the following file:

```
current-command-execution-folder\jslmminfoget.zip
```

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmminfoget
```

Execution permission

OS's `Administrator` account

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Notes

- Do not execute this command in a current folder whose absolute path contains any special character that requires enclosure in quotation marks at the command prompt (the following are the applicable special characters: `&`, `( )`, `[ ]`, `{ }`, `^`, `=`, `;`, `!`, `'`, `+`, `,`, `` ` ``, `~`, and `@`). If the command is executed in this manner, collection of the data needed for error analysis will fail (and the return value will not necessarily be `1`).

  If this command is executed in a current folder that contains a special character in the absolute path, the temporary folder (`jslmminfoget_work`) might be created under a non-current folder and that temporary folder might remain after the command has terminated. In such a case, the `jslmminfoget_work` folder will have been created in a folder with a similar name to that of the current folder used for command execution in the same hierarchy as the current folder. Use Windows Explorer to locate this folder and delete it.
- While this command is executing, do not execute the `jslmdbcopy`, `jslmdbrstr`, `jslmmgrsetup`, or `jslmmgrunsetup` command.
- Do not cancel execution of this command by pressing **Ctrl**+**C** on the keyboard. If command execution is canceled by this method, the following folder or files might remain:
  - `jslmminfoget_work` folder (work folder used by the `jslmminfoget` command)
  - `jslmminfoget.zip`
  - `tmp`*about-20-numeric-characters*`.tmp` (intermediate file of `jslmminfoget.zip`)

  If you canceled execution of this command, use Windows Explorer to locate these files and delete them.

- If the command fails to store the collected file in `jslmminfoget.zip`, the following file might remain after command execution:
    - `tmp`*about-20-numeric-characters*`.tmp` (intermediate file of `jslmminfoget.zip`)

  If the command failed to store the collected file in `jslmminfoget.zip`, use Windows Explorer to locate the `tmp`*about-20-numeric-characters*`.tmp` file and delete it.

Return value

Return value	Description
0	Collection of ITSLM - Manager error information terminated normally.
1	Collection of ITSLM - Manager error information failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmminfoget
```

jslmreport (outputs report data to a CSV file)

Function

This command outputs report data, stored in the database, in CSV file format.

Execute this command under the following conditions:

- ITSLM - Manager version 10-10, or a version of ITSLM - Manager that uses the same data format as version 10-10, has been set up.
- ITSLM - Manager databases of version 10-00 or earlier have been restored using the overwrite setup.
- The ITSLM - Manager services **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) and **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) are running.

If you are in a cluster environment, execute this command on the active server. You cannot execute it on a standby server.

For details about messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmreport -t { service | system | info | overview | graph }
           -g service-group-name
           -s service-name
           -d report-start-date
           -i { 1day | 1week | 1month | 3months }
           -o output-file-name
          [  -f ]
```

Execution permission

A user account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-Manager-installation-folder\mgr\bin\
```

Arguments

-t

Specifies the category of report data to output as a CSV file. One of the following categories can be specified:

- `service`

Specify this to output service performance. Note that `service` cannot be specified if a service that is not subject to service performance monitoring is specified in the `-s` option.

- `system`

Specify this to output system performance.

- `info`

Specify this to output availability information.

- `overview`

Specify this to output a service availability overview.

- `graph`

Specify this to output a performance chart.

`-g` *service-group-name*

Specifies the name of the service group to which the target monitored service belongs.

`-s` *service-name*

Specifies the name of the target monitored service.

`-d` *report-start-date*

Specifies the date from which the report on the target monitored service is to begin. It is specified as follows.

Table 9–6: How to specify the report start date

Format	Details
`-d` *YYYYMMDD*	*YYYY* Specifies the year as a four-digit number. *MM* Specifies the month as a two-digit number. *DD* Specifies the day as a two-digit number.

- The start date uses the same time zone as ITSLM - Manager.
- The validity of the start date (whether the date exists on the calendar) is not checked.

`-i`

Specifies the report interval for the target monitored service. It is specified as follows:

- `1day`

Specify this to output a one-day report.

- `1week`

Specify this to output a one-week report.

- `1month`

Specify this to output a one-month report.

- `3months`

Specify this to output a three-month report.

-o *output-file-name*

Specifies the name of the output file, as an absolute path, for the report data.

Output format

The first line displays header information, and the second and subsequent lines display data.

The following describes the output format for each data type.

- Service performance

  The service performance output format is as follows.

Table 9–7: Service performance output format

No.	Header information	Data beginning on line 2	Data details
1	`Service_Performance_Start_Date`	Start date of the report interval	*YYYY*/*MM*/*DD* (year/month/day)
2	`Service_Performance_End_Date`	End date of the report interval	*YYYY*/*MM*/*DD* (year/month/day)
3	`Service_Performance_Monitored_Target`	Monitored target	Name of the selected monitored target
4	`Service_Performance_Monitor_Item`	Monitor item (unit)	• Average response time (milliseconds) • Throughput (count/second) • Error rate (%)
5	`Service_Performance_Average`	Average[#1]	• For average response time: *Total average response time during the report interval* ÷ *number of requests during the report interval* (milliseconds) • For throughput: *Number of requests during the report interval (excluding requests whose responses timed out before ITSLM - UR could receive them)* ÷ *operation time during the report interval* (count/second) • For error rate: (*Number of times HTTP status returned an error response during the report interval* + *number of requests whose responses timed out before ITSLM - UR could receive them*) ÷ *number of requests during the report interval* (%)
6	`Service_Performance_SLO_Compliance_Ratio`	SLO compliance rate[#1]	(1.0 - *duration of overages of a threshold* ÷ *operation time for one month*) × 100 (%)
7	`Service_Performance_VS_Previous_Term`	Comparison to a previous period (as a percentage)[#2, #3]	(*Average response time during report interval* ÷ *average response time during comparison period for the report interval* - 1.0) × 100 (%)

#1

The value is rounded to the first decimal place.

#2

The value is rounded to the second decimal place.

#3

When comparing to a previous period, the percentage is calculated for the monitored service's service performance, and the table header and the period used for comparison depend on the report interval setting.

The following table shows the relationship between the report interval and the previous period to which the percentage applies.

Table 9–8: Relationship between report interval and previous period to which percentage applies

No.	Report interval	Table header	Period used for comparison
1	1 day	Compared to previous day	Day immediately preceding the start date
2	1 week	Compared to previous week	Seven days immediately preceding the start date
3	1 month	Compared to previous month	From the same date in the previous month to the preceding day
4	3 months	Compared to previous quarter	From the same date three months ago to the preceding day

- System performance

  The system performance output format is as follows.

Table 9–9: System performance output format

No.	Header information	Data beginning on line 2	Data details
1	`System_Performance_Start_Date`	Start date of the report interval	*YYYY*/*MM*/*DD* (year/month/day)
2	`System_Performance_End_Date`	End date of the report interval	*YYYY*/*MM*/*DD* (year/month/day)
3	`System_Performance_Host`	Host	Host name of the selected monitored service
4	`System_Performance_Monitored_Target`	Monitored target	Name of the monitoring agent contained in the host
5	`System_Performance_Monitor_Item`	Monitor item (unit)	Name of a monitoring item contained in the monitoring agent
6	`System_Performance_Average`	Average#1	Average value for the monitoring item
7	`System_Performance_SLO_Compliance_Ratio`	SLO compliance rate#1	(1.0 - *duration of overages of a threshold* ÷ *operation time for one month*) × 100 (%)
8	`System_Performance_VS_Previous_Term`	Comparison to a previous period (as a percentage)#2, #3	(*Average response time during report interval* ÷ *average response time during comparison period for the report interval* - 1.0) ÷ 100 (%)

#1

The value is rounded to the first decimal place.

#2

The value is rounded to the second decimal place.

#3

When comparing to a previous period, the percentage is calculated for the monitored service's system performance, and the table header and the period used for comparison depend on the report interval setting.

For the relationship between the report interval and the previous period to which the percentage applies, see *Table 9-8 Relationship between report interval and previous period to which percentage applies*.

- Availability information

  The availability information output format is as follows.

Table 9–10: Availability information output format

No.	Header information	Data beginning on line 2	Data details
1	`Availability_Info_Start_Date`	Start date of the report interval	*YYYY*/*MM*/*DD* (year/month/day)
2	`Availability_Info_End_Date`	End date of the report interval	*YYYY*/*MM*/*DD* (year/month/day)
3	`Availability_Info_Service_Availability`	Service availability %#1	(*Sum of all operation periods during report interval* ÷ (*sum of all operation periods during report interval* + *sum of all error periods during report interval*) × 100) (%)
4	`Availability_Info_MTTR`	MTTR#2	*Sum of all error periods during report interval* ÷ *number of error periods during report interval* (minutes)
5	`Availability_Info_MTBF`	MTBF#2	*Sum of all operation periods during report interval* ÷ *number of error periods during report interval* (minutes)

#1

The value is rounded to the second decimal place.

#2

The value is rounded to the first decimal place.

- Service availability overview

The service availability overview output format is as follows.

Table 9–11: Service availability overview output format

No.	Header information	Data beginning on line 2	Data details
1	`Service_Availability_Overview_Date_And_Time`	Date and time#	Date and time an event related to availability monitoring occurred during the report interval
2	`Service_Availability_Overview_Event`	Event	One of the following events related to availability monitoring that occurred during the report interval: • Service recovery • Start of service monitoring • Stop of service monitoring • Service stop

#

Displayed in the format *YYYY*/*MM*/*DD hh*:*mm*, using the ITSLM - Manager's time zone.

- Performance chart information output to CSV file

The performance chart information output to the CSV file is as follows.

Table 9–12: Performance chart information output to CSV file

No.	Header information	Data beginning on line 2	Data details
1	Date	Date and time	Date and time data acquired from ITSLM. Displayed in the format *YYYY*/*MM*/*DD hh*:*mm*, based on the ITSLM - Manager's time zone
2	Monitoring item average	Monitoring item average value	Average value for the monitoring item
3	Monitoring item max	Monitoring item maximum value	Maximum value for the monitoring item
4	Monitoring item min	Monitoring item minimum value	Minimum value for the monitoring item

No.	Header information	Data beginning on line 2	Data details
. . .			
6	Monitoring item average	Monitoring item average value	Average value for the monitoring item
7	Monitoring item max	Monitoring item maximum value	Maximum value for the monitoring item
8	Monitoring item min	Monitoring item minimum value	Minimum value for the monitoring item

Note:

Monitoring items are defined by the following BNF notation:

monitoring-item `::=` *name-of-monitored-target* `"/"` *name-of-monitored-target-within-monitored-service* `"/"`

name-of-monitored-target-within-monitored-service `::=` `"All Web Access"` | *Web-transaction-name* | *host-name* `"/"` *agent-name*

Output character encoding

UTF-8 character encoding is used.

`-f`

Specifies that the output file specified in the `-o` option is to be overwritten if it already exists.

If this option is omitted and the output file already exists, the command results in an error.

Notes

- This command's processing and the following operations are mutually exclusive:
  - Registering and deleting monitored services
  - Registering and deleting Web transactions
  - Editing Web transactions (including changing their order)
  - Adding, editing, copying, and deleting report templates
  - Updating configuration information
  - Saving monitoring item settings for system performance
  - Setting up service performance monitoring
  - Setting up system performance monitoring
  - Setting up availability monitoring

  If this command is executed while any mutually exclusive processing is underway, the command results in an error and its processing is canceled. Similarly, if an attempt is made to start any mutually exclusive processing while this command is executing, that processing will result in an error and be canceled.
- Do not execute another command while this command is executing, except for the `jslmmgrexport` command or the `jslmminfoget` command.
- The service group name and service name must not begin with a hyphen (`-`).
- Nonexistent dates in the report interval are not subject to aggregation in the CSV file. For example, if the report start date is May 31, and the report interval is set to 1 month, the relevant period is from May 31 to June 30, excluding June 31. As a result, the last day of the report interval will be June 29, which is the day preceding June 30, and the report interval will cover May 31 through June 29. The calculations for comparisons to previous periods are handled in the same way.
- ITSLM retains report data for five years.

- If the name of a monitoring item includes a comma (,) or a double quotation mark ("), that character is replaced with an underscore (_) in the CSV file.
- Do not cancel execution of this command by closing the command prompt that is executing this command or by pressing **Ctrl**+**C** on the keyboard.

Return value

Return value	Description
0	The CSV file was output successfully.
1	Output of the report to a CSV file failed.
130	Processing was canceled because **Ctrl**+**C** was pressed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmreport -t service -g Group1 -
s Service1 -d 20130128 -i 1month -o c:\report.csv -f
```

jslmurinfoget (collects data needed for investigating the cause of ITSLM - UR errors)

Function

This command collects error information for ITSLM - UR and information needed for error analysis.

This command can be executed if the ITSLM - UR setup has been completed.

Use the information collected by executing this command as data when an error has occurred in ITSLM - UR and you need to contact the system administrator.

The command execution results are output to the following file:

```
current-command-execution-folder\jslmurinfoget.zip
```

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmurinfoget
```

Execution permission

OS's `Administrator` account

Storage folder

```
ITSLM-UR-installation-folder\ur\bin\
```

Notes

- Do not execute this command in the current folder whose absolute path contains any special character that requires enclosure in quotation marks at the command prompt (the following are the applicable special characters: `&`, `( )`, `[ ]`, `{ }`, `^`, `=`, `;`, `!`, `'`, `+`, `,`, `` ` ``, `~`, and `@`). If the command is executed in this manner, collection of the data needed for error analysis will fail (and the return value will not necessarily be `1`).

  If this command is executed in a current folder that contains a special character in the absolute path, the temporary folder (`jslmurinfoget_work`) might be created under a non-current folder and that temporary folder might remain after the command has terminated. In such a case, the `jslmurinfoget_work` folder will have been created in a folder with a similar name to that of the current folder used for command execution in the same hierarchy as the current folder. Use Windows Explorer to locate this folder and delete it.

- While this command is executing, do not execute the `jslmursetup` or `jslmurunsetup` command.

- Do not cancel execution of this command by pressing **Ctrl**+**C** on the keyboard. If command execution is canceled by this method, the following folder or files might remain:

  - `jslmurinfoget_work` folder (work folder used by the `jslmurinfoget` command
  - `jslmurinfoget.zip`
  - `tmp`*about-20-numeric-characters*`.tmp` (intermediate file of `jslmurinfoget.zip`)

  If you canceled execution of this command, use Windows Explorer to locate these files and delete them.

- If the command fails to store the collected file in `jslmurinfoget.zip`, the following file might remain after command execution:
    - `tmp`*about-20-numeric-characters*`.tmp` (intermediate file of `jslmurinfoget.zip`)

  If the command failed to store the collected file in `jslmurinfoget.zip`, use Windows Explorer to locate the `tmp`*about-20-numeric-characters*`.tmp` file and delete it.

Return value

Return value	Description
0	Collection of ITSLM - UR error information terminated normally.
1	Collection of ITSLM - UR error information failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\ur\bin\jslmurinfoget
```

jslmuripls (displays network interface number and IP address)

Function

This command displays in the command prompt window the network interface number and IP address of the host on which ITSLM - UR is installed.

The information displayed by executing this command will be needed for setting up ITSLM - UR or for changing the network interface number by editing the system definition file for ITSLM - UR.

For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmuripls
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-UR-installation-folder\ur\bin\
```

Notes

If the `jslmuripls` command is executed with any argument specified, it terminates with an error.

Return value

Return value	Description
0	The display processing terminated normally.
1	The display processing failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\ur\bin\jslmuripls
```

Example output

```
KNAS99000-I network-interface-number----IP-address
```

jslmursetup (sets up ITSLM - UR)

Function

This command creates an execution environment for ITSLM - UR. It can also be used to reconfigure the execution environment for an existing ITSLM - UR.

Before you execute this command, install ITSLM - UR, and then execute the `jslmuripls` command to check the network interface number and IP address of the host on which ITSLM - UR has been installed.

The command execution results are output to the standard output and displayed in the console window. For details about the messages displayed during command execution, see *11.3 Messages*.

The command performs one of the following processes, depending on the status of the execution environment at the time of command execution:

Creates an execution environment (when there is no existing execution environment):

> This command creates an execution environment when it is executed immediately after ITSLM - UR has been newly installed or after the execution environment for ITSLM - UR was discarded by unsetup processing.

Reconfigures the existing execution environment (when an execution environment already exists):

> If this command is executed when the execution environment for a configured ITSLM - UR already exists, the command reconfigures the existing execution environment for ITSLM - UR.
>
> You reconfigure the execution environment in the following cases:
>
> - The host name, IP address, or port number settings in the execution environment for a configured ITSLM - UR are to be changed.
> - The execution environment for a configured ITSLM - UR is to be reconfigured after an upgrade installation was performed.

Format

```
jslmursetup [ -c { online | standby } ] absolute-path-of-options-file
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-UR-installation-folder\ur\bin\
```

Arguments

-c

Specifies that the execution environment used in a cluster system is to be configured. The specification method is as follows:

- `online`

  Specifies that the execution environment for the active system is to be configured or reconfigured.

- `standby`

  Specifies that the execution environment for the standby system is to be configured or reconfigured.

absolute-path-of-options-file

Specifies the absolute path for an options file that is to be created in text format. This file can be stored at any desired location. The absolute path of the options file storage location must be a maximum of 255 bytes of characters, including the file name (any name).

An options file template is stored at the following location:

```
ITSLM-UR-installation-folder\ur\template\ur\conf\jp1itslm_setup.opt
```

The following shows the definitions in the options file:

```
manager_host=host-name-or-IP-address-of-ITSLM-Manager
manager_port=port-number-of-ITSLM-Manager
ur_host=host-name-or-IP-address-of-ITSLM-UR
ur_port=port-number-of-ITSLM-UR
ur_ni_number=network-interface-number
```

The following table provides the details of definition items.

Table 9–13: Details of definition items in options file for ITSLM - UR

No.	Definition item	Specification	Description	Default value
1	`manager_host`	R	Specifies the host name or IP address of the host on which ITSLM - Manager is installed, as the information for identifying ITSLM - Manager's execution environment. If ITSLM is running in a cluster system, specify the logical host name or logical IP address.	--
2	`manager_port`	O	Specifies the port number used by ITSLM - Manager, as a number in the range from `1` through `65535`.#	`20904`
3	`ur_host`	R	Specifies the host name or IP address of the host on which ITSLM - UR is installed, as the information for identifying ITSLM - UR's execution environment. If ITSLM is running in a cluster system, specify the logical host name or logical IP address.	--
4	`ur_port`	O	Specifies the port number used by ITSLM - Manager, as a number in the range from `1` through `65535`.#	`20910`
5	`ur_ni_number`	R	Specifies the network interface number used for connection by ITSLM - UR, as a number in the range from `1` through `60`.# You can use the `jslmuripls` command to check the connected network device. For details about the `jslmuripls` command, see *jslmuripls (displays network interface number and IP address)* in *9. Commands*.	--

Legend:

R: Specification is required

O: Specification is optional

--: Not applicable

#

If the specified value is not within the permitted range, setup is completed, but an error occurs when the ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`) starts.

Notes

- If an error occurs during setup, eliminate the cause of the error and re-execute the command.
- The options file used during setup is renamed `jp1itslm_setup.opt` after command execution and stored at the following location:

  ```
  ITSLM-UR-installation-folder\ur\conf\jp1itslm_setup.opt
  ```

- Do not execute another command while this command is executing, except for the `jslmuripls` command.
- If the folder shown below contains the options file, the command renames that options file by adding `.bk`, saves it in the same folder, and then creates a new options file:

  ```
  ITSLM-Manager-installation-folder\ur\conf\
  ```

  If a file with the same name already exists when the options file is saved, the existing file is overwritten. If the file save processing fails, setup fails. The values of definition items contained in the saved options file are inherited to the new options file. However, for the definition items that were specified in the options file when the command was executed, the specified values are set. Comments are not inherited.
- Do not terminate setup processing by pressing **Ctrl**+**C** or closing the window. Also, in the event of an error, wait until setup is completed before proceeding.
- Before you start the setup processing, terminate all other resident software programs, including other installers and applications (other applications include the `jslmursetup` and `jslmurunsetup` commands).
- If setup is performed with the `-c` option specified in the command and any of a set of specific errors occurs during operation, the Windows services are closed by ITSLM - Manager. For details about the errors that result in a stoppage of the Windows services, see *6.1.3 Failover timing*.

Return value

Return value	Description
0	Setup processing terminated normally.
1	Setup processing failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\ur\bin\jslmursetup C:\Users\Administrator
\Desktop\jp1itslm_setup.opt
```

jslmurunsetup (undoes the ITSLM - UR setup)

Function

This command discards the execution environment for ITSLM - UR.

This command is used when the settings specified during the setup are to be changed without uninstalling ITSLM - UR.

The command execution results are output to the standard output and displayed in the console window. For details about the messages displayed during command execution, see *11.3 Messages*.

Format

```
jslmurunsetup
```

Execution permission

User account that belongs to the OS's Administrators group

Storage folder

```
ITSLM-UR-installation-folder\ur\bin\
```

Notes

- If an error occurs during unsetup processing, eliminate the cause of the error and re-execute the command.
- Do not execute another command while this command is executing, except for the `jslmuripls` command.
- Do not terminate unsetup processing by pressing **Ctrl**+**C** on the keyboard or closing the window. In the event of an error, wait until the unsetup processing is completed before proceeding.
- Before you start unsetup processing, terminate all other resident software programs, including other installers and applications (other applications include the `jslmursetup` and `jslmurunsetup` commands).

Return value

Return value	Description
0	Unsetup processing terminated normally.
1	Unsetup processing failed.

Example

```
C:\Program Files\HITACHI\JP1ITSLM\ur\bin\jslmurunsetup
```

10 ITSLM Windows

This chapter describes the ITSLM windows.

10.1 Overview of the windows

10.1.1 What the windows are used for

There are five types of windows in ITSLM.

The following table summarizes the intended use of each type of window and provides a reference to the section in which you will find detailed information about that window.

Table 10–1: ITSLM windows

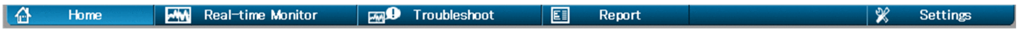
No.	Window	When it is used	What it is used for	For details about this window
1	Home window	For monitoring the status of monitored services	This window is used in monitoring the status of monitored services. It keeps track in a single location of the errors and warnings that occur in all the monitored services you are responsible for monitoring, and lets you check on monitored services that require attention.	10.2
2	Real-time Monitor window	• For monitoring the status of monitored services • For confirming recovery	This window is used in monitoring the status of monitored services. When it becomes clear that monitored services require attention, you can specify a monitored service and get the details immediately. After you have dealt with the problem, you can confirm that the monitored service has recovered.	10.3
3	Troubleshoot window	For investigating the causes of problems	When an error or warning occurs, this window lets you check past service performance and determine when the event that caused the problem occurred.	10.4
4	Report window	For creating reports	This window is used to output files and to display information for creating reports for regular reporting of monitoring results.	10.5
5	Settings window	• For adding and deleting monitored services • For setting monitoring items • For starting and stopping monitoring	This window is used to add and delete monitored services, to set monitoring items, and to start and stop monitoring.	10.6

10.1.2 Common items on all windows

(1) Buttons for switching windows

After you have logged in, you display ITSLM windows by clicking buttons located at the top of the windows. The buttons are shown in the figure below. Note that if you click the button to display the window that is already being displayed, the window is not updated.

Figure 10–1: Buttons for switching windows



The Troubleshoot window can be displayed from the list of errors and warnings displayed in the Home window, as well as from the performance charts displayed in the Real-time Monitor window. In this case, you display the Troubleshoot window after you have selected a monitored service in the Home window or Real-time Monitor window. For details about how to do this, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.

Note that for windows other than the Settings window, when you redisplay the original window after a window transition, the pre-transition window information is displayed. However, for windows whose contents are updated regularly, the displayed contents might be different, because the update process that was interrupted by the window transition is resumed when the original window is refreshed. In the case of the Settings window, when you redisplay the original window after a window transition, the pre-transition window information is not displayed.

(2) Icons displayed in windows

The Home window, Real-time Monitor window, and Troubleshoot window display lists of events that describe changes in the status of monitored services when errors and warnings have occurred. For each event, an icon is displayed indicating the status of the monitored service. By checking the icons, you can identify which monitored services require attention.

The table below shows the icons and the monitored service status that each icon represents. The table also shows the type of monitoring (detection) associated with each icon and its applicable monitoring items.

Table 10–2: Monitored service status indicated by icons

No.	Icon	Type	Monitored service status	Type of monitoring (detection)	Monitoring items
1	✖	Error	Service performance or system performance has exceeded the threshold. Immediate corrective action is required.	Threshold monitoring	• Average response time • Throughput • Error rate • System performance monitoring[#1]
			The monitored service has stopped. Immediate corrective action is required.	Availability monitoring[#1]	--
2	!	Warning	A trend has been detected indicating that service performance or system performance is likely to exceed the threshold. Take corrective action as necessary.	Trend monitoring	• Average response time • Throughput • System performance monitoring[#1]
			Service performance or system performance has veered sharply from the usual average value. Take corrective action as necessary.	Out-of-range value detection	• Average response time • Throughput • Error rate[#2] • System performance monitoring[#1, #2]
3	✓	Normal	Normal.	--	--
4	⏸	Monitoring stopped	Monitoring of the monitored service is not being performed.		

Legend:

--: Not applicable.

#1

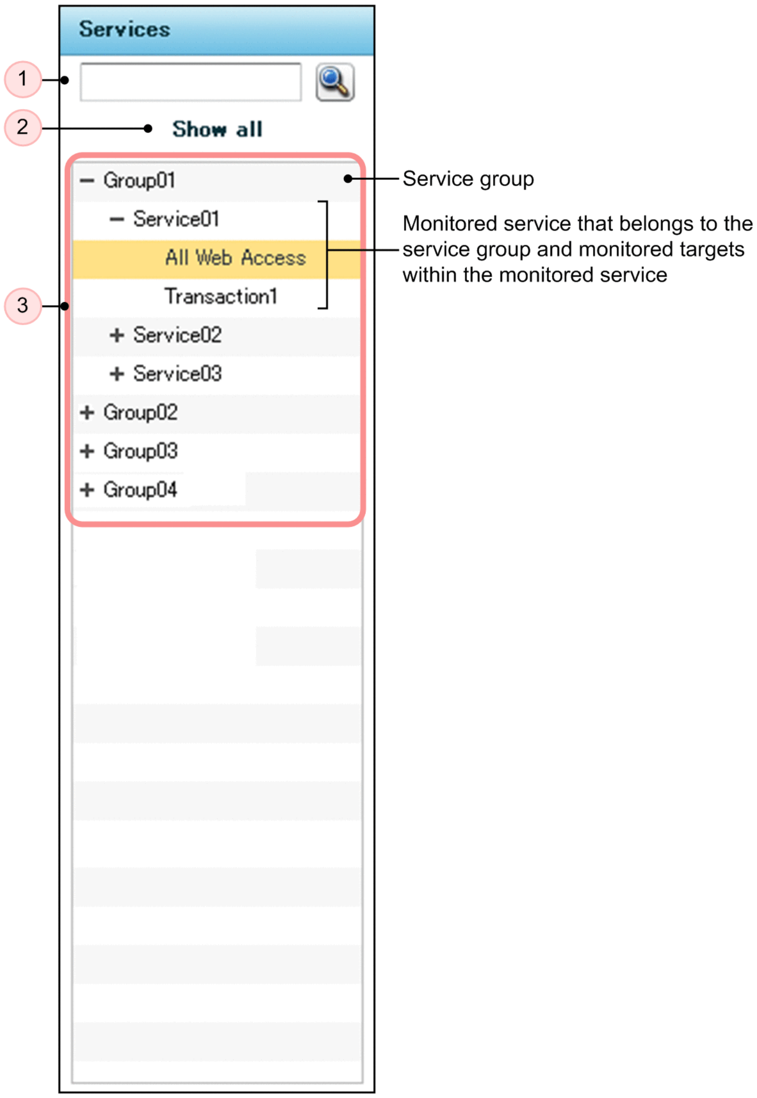
Monitoring is possible through linkage with Performance Management.

#2

Out-of-range value detection detected from a combination of multiple monitoring items is not shown.

(3) Services area

The **Services** area is for selecting the services to be monitored. It is displayed in the Real-time Monitor window, Troubleshoot window, Report window, and Settings window, where the monitoring is carried out.



The **Services** area displays a hierarchical list of the service groups, monitored services, and monitored targets within the monitored services that the logged-in user is responsible for monitoring. By selecting a service group, monitored service, or monitored target within a monitored service, you can configure the selected item, or drill down to see what is displayed in the **Service performance information** area or the **Event** and **Performance chart** tabs area.

The following table lists the items displayed in the **Services** area.

No.	Item	Description
1	Text box for searching for monitored services and 🔍 (search) button	Enables a drill-down search for a monitored service in the list of service groups and monitored services. You can only search for the name of a monitored service. You cannot search for the name of a service group or a monitored target.

No.	Item	Description
1	Text box for searching for monitored services and 🔍 (search) button	To conduct a search, enter a character string in the text box, and then click the 🔍 (search) button or press the **Enter** key. Any monitored service whose name is at least a partial match for the entered character string is displayed, together with its service group. The service group is displayed as being open. A maximum of 64 characters can be entered in the text box. If a search is performed with nothing entered in the text box, the list of all the service groups that the logged-in user is responsible for monitoring is displayed.
2	**Show all**	Displays a hierarchical list of all the monitored services that the logged-in user is responsible for monitoring.
3	List of service groups, monitored services, and monitored targets within monitored services	Provides a hierarchical listing of service groups, monitored services, and monitored targets within the monitored services. Clicking a displayed service group, monitored service, or monitored target within a monitored service changes what is displayed in this area. When you select a service group after a search for monitored services, only the monitored services displayed as the search results are shown, not the other monitored services that belong to the same service group. Note that if you re-select an already-selected monitored service, or a monitored target within a monitored service, the window display is not updated.

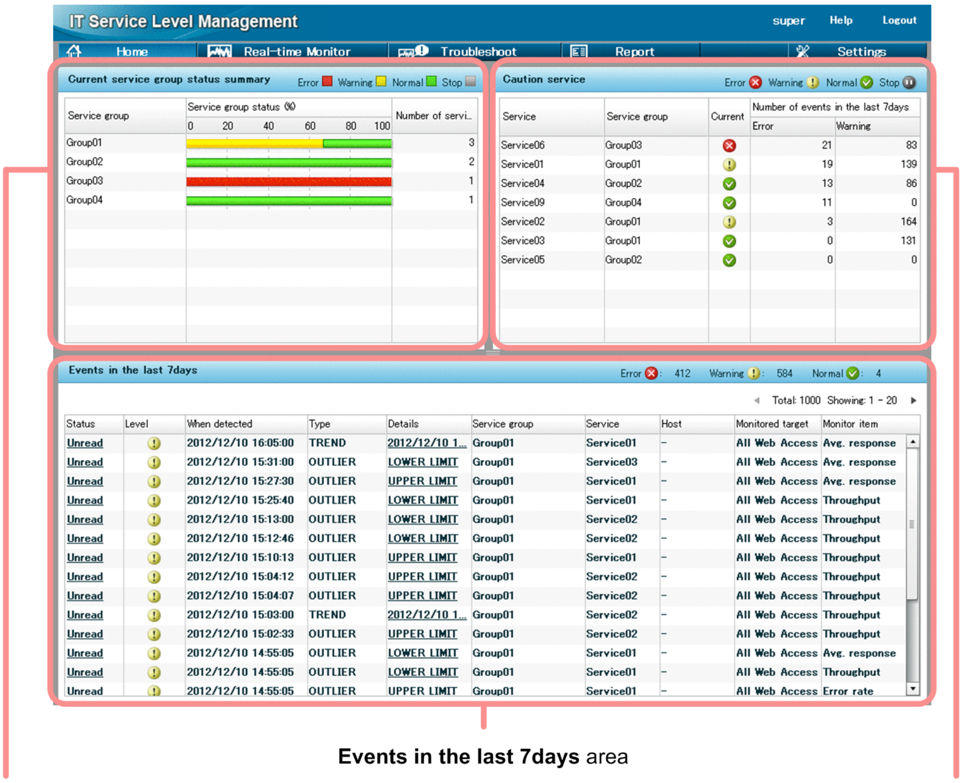
(4) Supplemental notes

- When you display the Troubleshoot window by clicking the **Troubleshoot** button at the top of a window, the **Services** area shows only the service groups, not the monitored services.
- While the Settings window is displaying the **Add/Delete monitor** area or the **Start/Stop monitor** area, the **Services** area cannot be used.
- If you select only a service group in the **Services** area of the Settings window, nothing is displayed in the **Web transaction setting** area, the **Configuration information settings** area, and the **Monitor settings** area. If you select a monitored service or a monitored target within a monitored service, the settings for the monitored targets within the monitored service are displayed in the **Web transaction setting** area, **Configuration information settings** area, and **Monitor settings** area.

10.2 Home window

10.2.1 Configuration of the Home window

(1) Window configuration



Current service group status summary

Error 🟥 Warning 🟨 Normal 🟩 Stop ▨

Service group	Service group status (%) 0 20 40 60 80 100	Number of servi...
Group01		3
Group02		2
Group03		1
Group04		1

Caution service

Error ✕ Warning ! Normal ✓ Stop ⏸

Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service06	Group03	✕	21	83
Service01	Group01	!	19	139
Service04	Group02	✓	13	86
Service09	Group04	✓	11	0
Service02	Group01	!	3	164
Service03	Group01	✓	0	131
Service05	Group02	✓	0	0

Events in the last 7days

Error ✕: 412 Warning !: 584 Normal ✓: 4

◂ Total: 1000 Showing: 1 - 20 ▸

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	!	2012/12/10 16:05:00	TREND	2012/12/10 1...	Group01	Service01	-	All Web Access	Avg. response
Unread	!	2012/12/10 15:31:00	OUTLIER	LOWER LIMIT	Group01	Service03	-	All Web Access	Avg. response
Unread	!	2012/12/10 15:27:30	OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	!	2012/12/10 15:25:40	OUTLIER	LOWER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!	2012/12/10 15:13:00	OUTLIER	LOWER LIMIT	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/10 15:12:46	OUTLIER	LOWER LIMIT	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/10 15:10:13	OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!	2012/12/10 15:04:12	OUTLIER	UPPER LIMIT	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/10 15:04:07	OUTLIER	UPPER LIMIT	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/10 15:03:00	TREND	2012/12/10 1...	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/10 15:02:33	OUTLIER	UPPER LIMIT	Group01	Service02	-	All Web Access	Throughput
Unread	!	2012/12/10 14:55:05	OUTLIER	LOWER LIMIT	Group01	Service01	-	All Web Access	Avg. response
Unread	!	2012/12/10 14:55:05	OUTLIER	LOWER LIMIT	Group01	Service01	-	All Web Access	Throughput
Unread	!	2012/12/10 14:55:05	OUTLIER	UPPER LIMIT	Group01	Service01	-	All Web Access	Error rate

Events in the last 7days area

Current service group status summary area

Caution service area

(2) Window description

The Home window is used in monitoring the status of monitored services.

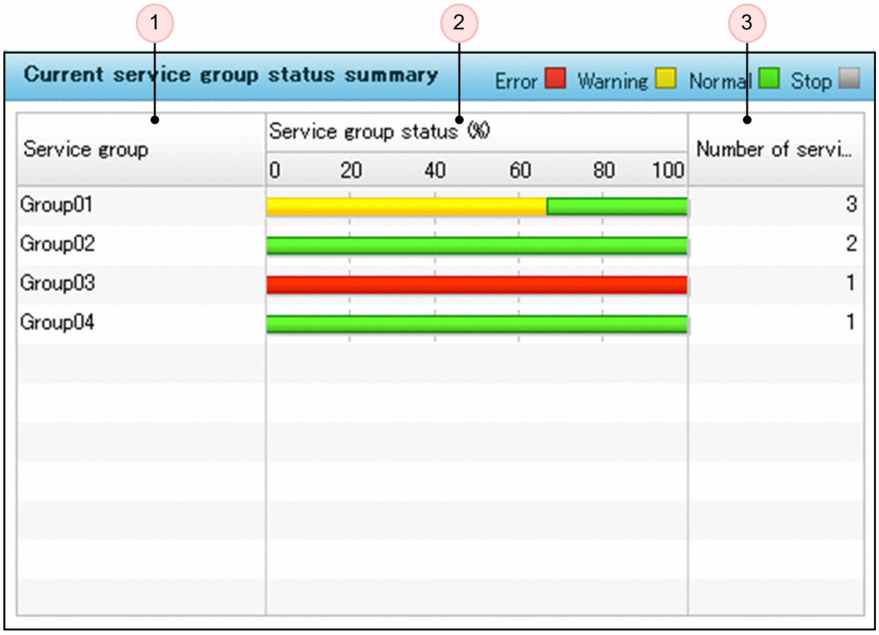
It keeps track in a single location of the errors and warnings that occur in all the monitored services you are responsible for monitoring, and lets you check on monitored services that require attention.

The Home window is composed of the following areas:

- **Current service group status summary** area
- **Caution service** area
- **Events in the last 7 days** area

10.2.2 Current service group status summary area

(1) Window configuration



Current service group status summary

Error 🟥 Warning 🟨 Normal 🟩 Stop ⬜

Service group	Service group status (%) 0 20 40 60 80 100	Number of servi...
Group01		3
Group02		2
Group03		1
Group04		1

(2) Window description

This window displays the status of the service groups that the logged-in user is responsible for monitoring. The display is updated every three seconds.

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This column displays the names of the service groups that the logged-in user is responsible for monitoring.
2	**Service group status (%)**	This column displays the current status of the monitored services belonging to each service group. A bar graph for each service group indicates the percentages of its monitored services whose status is error, warning, normal, and stopped, with 100% representing all the monitored services that belong to the service group. The colors in the bar graph indicate the following: Red (error) Percentage of monitored services in which an error has occurred in threshold monitoring. Yellow (warning) Percentage of monitored services in which a warning has occurred in trend monitoring or out-of-range value detection. Green (normal) Percentage of monitored services whose status is normal. Gray (monitoring stopped)# Percentage of monitored services that are not being monitored. If monitored targets within a monitored service have different statuses, the highest-priority status color is displayed, according to the following priority order (highest to lowest): red (error) > yellow (warning) > green (normal). (In the case where monitoring of a monitored service has stopped, only the stopped status is possible.)

No.	Item	Description
2	**Service group status (%)**	Consider an example with the following three statuses: • All Web Access: green (normal) • Web transaction 1: green (normal) • Web transaction 2: yellow (warning) In this case, the status of the monitored service would be yellow (warning).
3	**Number of services**	This column displays the number of monitored services belonging to each service group.

#

A monitored service is also counted as stopped if the process executing performance analysis of a monitored target within that monitored service experiences a memory shortage or abnormal termination of a thread after monitoring starts. In this case, stop the monitoring of the corresponding monitored service, restart monitoring after you have addressed the cause based on the *KNAS32021-E* message in the message log.

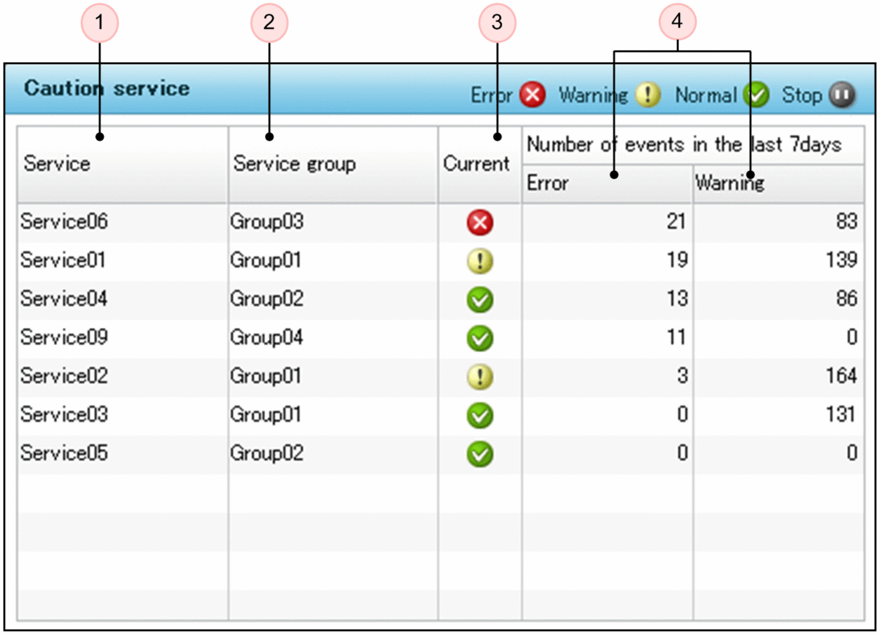
For details about the message log, see *7.2.3 Message logs*.

(3) Supplemental notes

- If you conduct trend monitoring, start the trend monitoring when you obtain service performance that is within at least 30% of the range of the most recent trend calculation. However, if the service performance decreases after monitoring starts, stop the monitoring and restart it once service performance stabilizes. At this time, it will be displayed as normal, rather than stopped, in the **Current service group status summary** area. Even if the trend has exceeded the threshold, it will be displayed as normal until service performance stabilizes.

10.2.3 Caution service area

(1) Window configuration



Service	Service group	Current	Number of events in the last 7days	
			Error	Warning
Service06	Group03	✖	21	83
Service01	Group01	!	19	139
Service04	Group02	✓	13	86
Service09	Group04	✓	11	0
Service02	Group01	!	3	164
Service03	Group01	✓	0	131
Service05	Group02	✓	0	0

(2) Window description

This window displays a ranked list of the monitored services based on the number of errors or warnings that occurred in each service during the last seven days. The display is updated every three seconds. The order in which the monitored services are listed is determined as follows:

1. The monitored service with the most errors appears first and the monitored service with the fewest errors appears last.
2. When the number of errors is the same, the monitored service with the most warnings appears first.
3. When the number of warnings is the same, the monitored services and service groups appear according to the Unicode ordering of their names.

The following table lists the items that are displayed:

No.	Item	Description
1	**Service**	This column displays the names of the monitored services that the logged-in user is responsible for monitoring.
2	**Service group**	This column displays for each monitored service the name of the service group to which it belongs.
3	**Current**	This column displays each monitored service's current composite monitoring result for average response time, throughput, and error rate, using the following icons: ❌ (error) There is at least one item for which an error has occurred in threshold monitoring. ⚠ (warning) There is at least one item for which a warning has occurred in trend monitoring or out-of-range value detection. ✅ (normal) The status of all items is normal. ⏸ (monitoring stopped)# The monitored service is not currently being monitored. If monitored targets within a monitored service have different statuses, the highest-priority status icon is displayed, according to the following priority order (highest to lowest): error > warning > normal. (In the case where monitoring of a monitored service has stopped, only the stopped status is possible.) Consider an example with the following three statuses: • All Web Access: ✅ (normal) • Web transaction 1: ✅ (normal) • Web transaction 2: ⚠ (warning) In this case, the status of the monitored service would be ⚠ (warning).
4	**Error**, **Warning**	These columns display for each monitored service the cumulative numbers of errors and warnings during the past seven days.

#

A monitored service will also be shown in the **Current** column as stopped if the process executing performance analysis of a monitored target within that monitored service experiences a memory shortage or abnormal termination of a thread after monitoring starts. In this case, stop the monitoring of the corresponding monitored service, and then restart monitoring after you have addressed the cause based on the *KNAS32021-E* message in the message log.

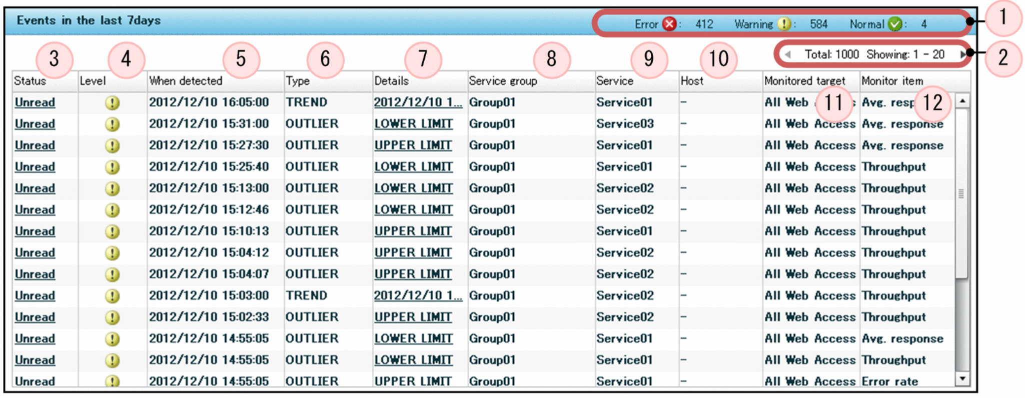
For details about the message log, see *7.2.3 Message logs*.

(3) Supplemental notes

- If you conduct trend monitoring, start the trend monitoring when you obtain service performance that is within at least 30% of the range of the most recent trend calculation. However, if the service performance decreases after monitoring starts, stop the monitoring and restart it once service performance stabilizes. At this time, it will be displayed as normal, rather than stopped, in the **Caution service** area. Even if the trend has exceeded the threshold, it will be displayed as normal until service performance stabilizes.

10.2.4 Events in the last 7 days area

(1) Window configuration



Events in the last 7days

Error ✖: 412 Warning !: 584 Normal ✓: 4

◀ Total: 1000 Showing: 1 - 20 ▶

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	!	2012/12/10 16:05:00	TREND	2012/12/10 1...	Group01	Service01	–	All Web	Avg. resp
Unread	!	2012/12/10 15:31:00	OUTLIER	LOWER LIMIT	Group01	Service03	–	All Web Access	Avg. response
Unread	!	2012/12/10 15:27:30	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2012/12/10 15:25:40	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2012/12/10 15:13:00	OUTLIER	LOWER LIMIT	Group01	Service02	–	All Web Access	Throughput
Unread	!	2012/12/10 15:12:46	OUTLIER	LOWER LIMIT	Group01	Service02	–	All Web Access	Throughput
Unread	!	2012/12/10 15:10:13	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2012/12/10 15:04:12	OUTLIER	UPPER LIMIT	Group01	Service02	–	All Web Access	Throughput
Unread	!	2012/12/10 15:04:07	OUTLIER	UPPER LIMIT	Group01	Service02	–	All Web Access	Throughput
Unread	!	2012/12/10 15:03:00	TREND	2012/12/10 1...	Group01	Service02	–	All Web Access	Throughput
Unread	!	2012/12/10 15:02:33	OUTLIER	UPPER LIMIT	Group01	Service02	–	All Web Access	Throughput
Unread	!	2012/12/10 14:55:05	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Avg. response
Unread	!	2012/12/10 14:55:05	OUTLIER	LOWER LIMIT	Group01	Service01	–	All Web Access	Throughput
Unread	!	2012/12/10 14:55:05	OUTLIER	UPPER LIMIT	Group01	Service01	–	All Web Access	Error rate

(2) Window description

This window displays the details of all the events that have occurred in the applicable monitored services during the last seven days. The events are listed in groups of 20 per page, starting with the most recent. Once it is displayed, an event continues to be listed until it reaches the seven-day cutoff. The display is updated every three seconds.

The following table lists the items that are displayed:

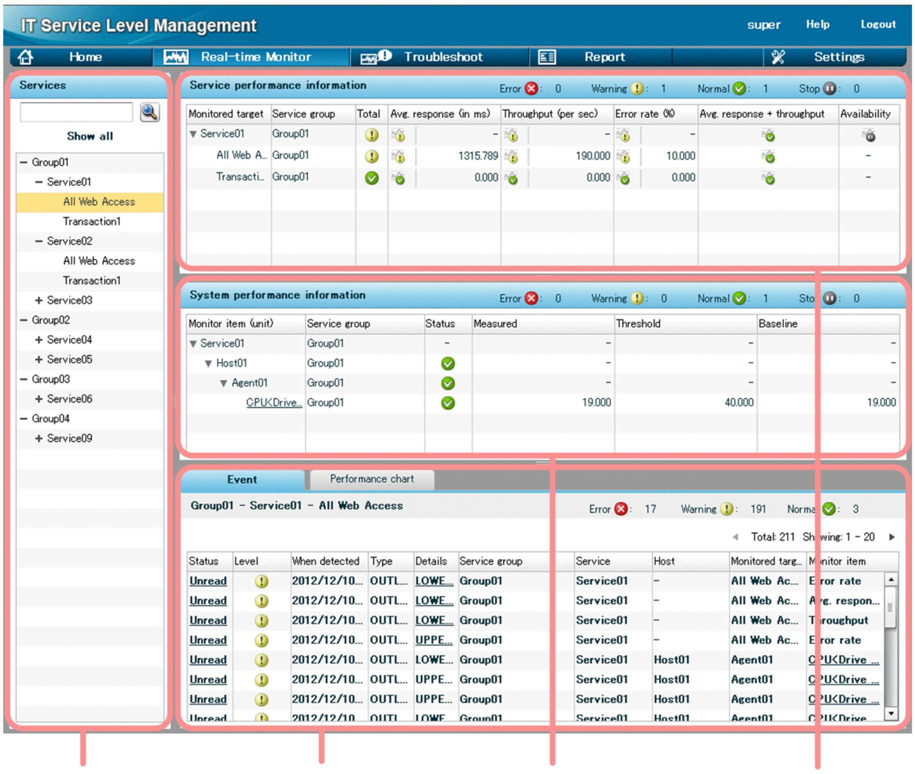
No.	Item	Description
1	Cumulative totals	This area shows the total number of events of each event type (error, warning, and normal) that occurred during the last seven days.
2	◀ **Total:** *n1* **Showing:** *n2*-*n3* ▶	When more than 20 events occurred in the monitored service in the last seven days, the additional events are displayed on subsequent pages. Click ◀ or ▶ to display the previous or next page, respectively. If there is no previous page or next page, you cannot click that icon. *n2* and *n3* indicate the range of event items displayed on the current page, and *n1* is the total number of events generated in the last seven days. Note that the maximum number of events displayed per page can be changed by specifying the `dashboardEventListRecentViewSize` property. When you change the number of items to be displayed per page, *n1* will reflect the changed value. For details about the `dashboardEventListRecentViewSize` property, see *5.6.2 Editable definitions*.
3	**Status**	This column indicates whether each event has been checked (read). **Unread** This is the default value, before the user has clicked the row's **Status** column. When **Unread** is displayed, the entire row is in displayed in boldface.

No.	Item	Description
3	**Status**	**Read** This setting indicates that the row's **Status** column has been clicked. After you check an event by reviewing the contents of its row, click the row in this column to change **Unread** to **Read**. Once an event's **Status** column entry is changed to **Read** it cannot be changed back to **Unread**.
4	**Level**	This column displays for each event one of the following icons indicating the status of the average response time, throughput, and error rate at the time the event occurred. The following icons are used: ✖ (error) An error occurred in threshold monitoring or availability monitoring. ! (warning) A warning occurred in trend monitoring or out-of-range value detection. ✓ (normal) Errors that occurred in availability monitoring have been recovered. When multiple service performance events are applicable simultaneously, the icon for the highest-priority event is displayed, according to the following priority order (highest to lowest): error > warning > normal.
5	**When detected**	This column displays the date and time the event occurred, in the format *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*).
6	**Type**	This column displays one of the following character strings indicting the type of the error or warning: **THRESHOLD** Monitoring detected that the threshold was exceeded (error). **OUTLIER** An out-of-range value that differs significantly from the norm for the monitored service was detected (warning). **TREND** A trend was detected indicating that the threshold seems likely to be exceeded (warning). **AVAILABILITY** Monitoring detected that the monitored service has stopped or has recovered from having stopped (error or normal).
7	**Details**	This column displays one of the following character strings providing more detail about the type of error or warning displayed in the **Type** column: **UPPER LIMIT** This is displayed when the **Type** column is **THRESHOLD** or **OUTLIER**. When the **Type** column is **THRESHOLD**, **UPPER LIMIT** indicates that the monitoring item's service performance or system performance exceeded the threshold. When the **Type** column is **OUTLIER**, **UPPER LIMIT** indicates that the monitoring item's service performance exceeded the upper limit value. **LOWER LIMIT** This is displayed when the **Type** column is **THRESHOLD** or **OUTLIER**. When the **Type** column is **THRESHOLD**, **LOWER LIMIT** indicates that the monitoring item's system performance exceeded the threshold. When the **Type** column is **OUTLIER**, **LOWER LIMIT** indicates that the monitoring item's service performance or system performance fell below the lower limit value. *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* This is displayed when the **Type** column is **TREND**, and indicates the date and time when it is expected that service performance or system performance of the monitoring item will exceed the threshold (*year*/*month*/*date hour*:*minute*:*second*).

No.	Item	Description
7	**Details**	**SERVICE FAILURE** This is displayed when the **Type** column is **AVAILABILITY**, and indicates that the monitoring item (indicated under **Monitor item**) has stopped. **SERVICE REPAIR** This is displayed when the **Type** column is **AVAILABILITY**, and indicates that the monitoring item (indicated under **Monitor item**) has recovered from a stop. If you click this column on a row, you will see in the Troubleshoot window a graph of the monitoring item's service performance. For details about how to do this, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.
8	**Service group**	This column displays the name of the service group in which the event occurred.
9	**Service**	This column displays the name of the monitored service in which the event occurred.
10	**Host**	An entry (other than a hyphen) is displayed in this column when system performance is monitored. The entry is the name of the host on which the event occurred. For an event associated with service performance monitoring, a hyphen (−) is displayed.
11	**Monitored target**	This column displays the name of the monitored target for which the event occurred.
12	**Monitor item**	This column displays the monitoring item for which the event occurred.

10.3.1 Configuration of the Real-time Monitor window

(1) Window configuration


IT Service Level Management
super
Help
Logout
Home
Real-time Monitor
Troubleshoot
Report
Settings
Services
Show all
Services area
Event and Performance chart tabs area
System performance information area
Service performance information area

- Group01
  - Service01
    - All Web Access
    - Transaction1
  - Service02
    - All Web Access
    - Transaction1
  - + Service03
- Group02
  - + Service04
  - + Service05
- Group03
  - + Service06
- Group04
  - + Service09

Service performance information — Error ✕: 0 Warning !: 1 Normal ✓: 1 Stop Ⅱ: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service01	Group01	!	! -	! -	! -	✓	Ⅱ
All Web A...	Group01	!	! 1315.789	! 190.000	! 10.000	✓	-
Transacti...	Group01	✓	✓ 0.000	✓ 0.000	✓ 0.000	✓	-

System performance information — Error ✕: 0 Warning !: 0 Normal ✓: 1 Sto Ⅱ: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service01	Group01	-	-	-	-
▼ Host01	Group01	✓	-	-	-
▼ Agent01	Group01	✓	-	-	-
CPU<Drive...	Group01	✓	19.000	40.000	19.000

Event | Performance chart

Group01 - Service01 - All Web Access — Error ✕: 17 Warning !: 191 Norma ✓: 3

◀ Total: 211 Sh wing: 1 - 20 ▶

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored targ...	M nitor item
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	-	All Web Ac...	E ror rate
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	-	All Web Ac...	A g. respon...
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	-	All Web Ac...	T roughput
Unread	!	2012/12/10...	OUTL...	UPPE...	Group01	Service01	-	All Web Ac...	E ror rate
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	Host01	Agent01	C PU<Drive ...
Unread	!	2012/12/10...	OUTL...	UPPE...	Group01	Service01	Host01	Agent01	C PU<Drive ...
Unread	!	2012/12/10...	OUTL...	UPPE...	Group01	Service01	Host01	Agent01	C PU<Drive ...
Unread	!	2012/12/10	OUTL	LOWE	Group01	Service01	Host01	Agent01	C PU<Drive

(2) Window description

The Real-time Monitor window is used in monitoring the status of monitored services.When it becomes clear that a monitored service requires attention, you can specify the monitored service and obtain the details of the problem immediately.After you have dealt with the problem, you can verify that the monitored service's status has returned to normal.

The Real-time Monitor window is composed of the following areas:

- **Services** area
- **Service performance information** area
- **System performance information** area
- The **Event** and **Performance chart** tabs area

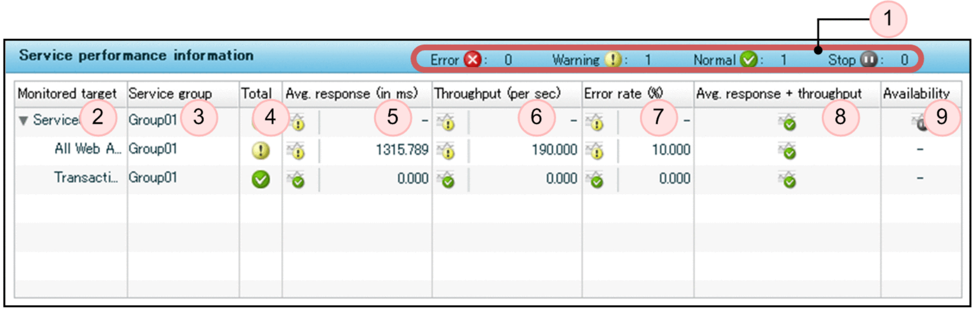
Use the **System performance information** area to interact with Performance Management. If no value has been set for the `pfmManagerHost` property in the `jp1itslm.properties` system definition file, it is assumed that Performance Management is not linked and the **System performance information** area is not displayed.

10.3.2 Services area

This area is common to all the ITSLM windows. For details about the **Services** area window, see *10.1.2(3) Services area*.

10.3.3 Service performance information area

(1) Window configuration



Service performance information

Error ✕: 0 Warning !: 1 Normal ✓: 1 Stop ⏸: 0

Monitored target	Service group	Total	Avg. response (in ms)	Throughput (per sec)	Error rate (%)	Avg. response + throughput	Availability
▼ Service	Group01		! -	! -	! -	✓	
All Web A...	Group01	!	! 1315.789	! 190.000	! 10.000	✓	-
Transacti...	Group01	✓	✓ 0.000	✓ 0.000	✓ 0.000	✓	-

(2) Window description

Depending on what you selected in the **Services** area, the service performance is displayed as follows:

- If you executed a search in the **Services** area in order to narrow down the list of monitored services, this window displays the service performance for only the monitored services that are displayed as search results.
- If you selected a service group in the **Services** area, this window displays the service performance of all the monitored services in that service group. When you click ▶ to the left of a monitored service, the icon changes to ▼ and the monitored targets and their service performance are displayed.
- If you selected in the **Services** area a monitored service or a monitored target within a monitored service, this window displays information about the selected monitored service and its monitored targets.
- If nothing was selected in the **Services** area, this window displays the service performance of all the monitored services that the logged-in user is responsible for monitoring.

The display is updated every three seconds.

The following table lists the items that are displayed:

No.	Item	Description
1	Cumulative totals	This area shows the total number of events of each event type (error, warning, normal, and stopped) for all the monitored targets in the monitored services that are displayed in the **Service performance information** area.
2	**Monitored target**	This column displays the names of the monitored services and monitored targets.
3	**Service group**	This column displays the name of the service group to which each monitored service belongs.
4	**Total**	This column displays as icons the overall monitoring results, determined comprehensively based on the conditions of the monitored services displayed under **Monitored target**. The following icons are used: ✕ (error) There is at least one item for which an error has occurred in threshold monitoring or availability monitoring.

No.	Item	Description
4	**Total**	⚠ (warning) There is at least one item for which a warning has occurred in trend monitoring or out-of-range value detection. ✓ (normal) The status of all items is normal. ⏸ (monitoring stopped)#1 The monitored service is not being monitored currently. In this case, ⏸ is also displayed on this row in the **Avg. response (in ms)**, **Throughput (per sec)**, **Error rate (%)**, and **Avg. response + throughput** columns. If multiple conditions occur in the monitoring results for a monitored service, or if multiple conditions occur in monitored targets belonging to a monitored service, the icon for the highest-priority event is displayed, according to the following priority order (highest to lowest): error > warning > normal. (In the case where monitoring of a monitored service has stopped, only the stopped status is possible.)
5	**Avg. response (in ms)**	These columns display for each monitoring item a measurement value (up to 3 digits after the decimal point) and an icon indicating the current status. The following icons are used: ✖ (error), ⚠ (warning), ✓ (normal),#2 and ⏸ (monitoring stopped).#1 On a row for a monitored service, if different conditions occur in multiple monitored targets within the monitored service, the icon for the highest-priority status is displayed, according to the following priority order (highest to lowest): error > warning > normal. (In the case where monitoring of a monitored service has stopped, only the stopped status is possible.) Consider an example with the following statuses: • All Web Access: ✓ (normal) • Web transaction 1: ✓ (normal) • Web transaction 2: ⚠ (warning) In this case, the status for the monitored service would show ⚠ (warning). The measurement values for a monitored service are always shown as −.
6	**Throughput (per sec)**	
7	**Error rate (%)**	
8	**Avg. response + throughput**	This column displays the out-of-range value detection status for average response time and throughput combined, using the following icons: ⚠ (warning), ✓ (normal)#2 or ⏸ (monitoring stopped).#1 On a row for a monitored service, if different conditions occur in multiple monitored targets within the monitored service, the icon for the highest-priority status is displayed, according to the following priority order (highest to lowest): error > warning > normal. (In the case where monitoring of a monitored service has stopped, only the stopped status is possible.)
9	**Availability**	This column displays the availability of a monitored service, using the following icons: ✖ (error), ✓ (normal), or ⏸ (monitoring stopped).#3 **Availability** is not displayed unless you are linked to Performance Management.#4 If availability monitoring has not been configured, a hyphen (−) is displayed. In addition, if it is determined that a monitored service was stopped by PFM - Agent for Service Response, an error is displayed under **Availability** for the monitored service, as well as under **Total**.

#1

A monitored service will also be shown in the **Total** column as stopped if the process executing performance analysis of a monitored target within that monitored service experiences a memory shortage or abnormal termination of a thread after monitoring starts. In this case, stop the monitoring of the corresponding monitored service, and then restart monitoring after you have addressed the cause based on the *KNAS32021-E* message in the message log.

For details about the message log, see *7.2.3 Message logs*.

#2

If threshold monitoring and out-of-range value detection have not been configured, this will always be shown as ✓ (normal) once monitoring of the monitored service has started. In this case, service performance can be acquired, but you cannot determine normal, warning, or error status from the icon.

#3

After monitoring starts, the icon displayed under **Availability** will not change to normal or abnormal until after the first monitoring results are received from the PFM - Agent for Service Response. Therefore, if it takes a long time after the start of service monitoring for the monitoring results to arrive from the PFM - Agent for Service Response, the monitoring stopped icon might continue to appear in the **Availability** column.

#4

If no value has been set for the `pfmManagerHost` property in the `jp1itslm.properties` system definition file, it is assumed that Performance Management is not linked.

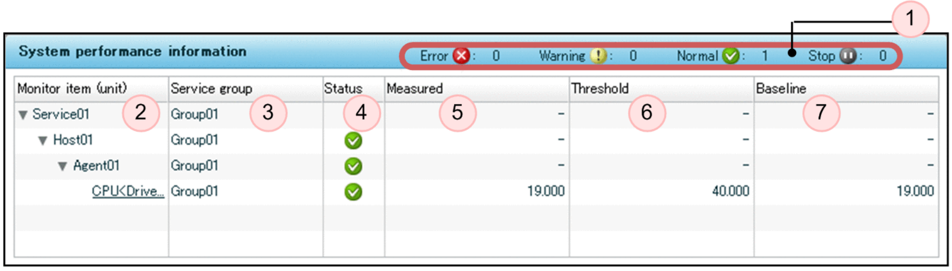
When you select one of the monitored services under **Monitored target**, it switches what is displayed in the **Event** and **Performance chart** tabs area.

(3) Supplemental notes

- On occasion, there might be a time lag of a few seconds to several tens of seconds before information is displayed in the **Service performance information** area and the **Event** and **Performance chart** tabs area.
- If you perform trend monitoring, start the trend monitoring when you obtain service performance that is within at least 30% of the range of the most recent trend calculation. However, if the service performance decreases after monitoring starts, stop monitoring and restart it once service performance stabilizes. At this time, it will be displayed in the **Service performance information** area as normal rather than stopped. Even if the trend has exceeded the threshold, it will be displayed as normal until service performance stabilizes.

10.3.4 System performance information area

(1) Window configuration



System performance information

Error ✕: 0 Warning !: 0 Normal ✓: 1 Stop ⏸: 0

Monitor item (unit)	Service group	Status	Measured	Threshold	Baseline
▼ Service01	Group01		-	-	-
▼ Host01	Group01	✓	-	-	-
▼ Agent01	Group01	✓	-	-	-
CPU<Drive...	Group01	✓	19.000	40.000	19.000

(2) Window description

The **System performance information** area is the window you use to interact with Performance Management. If no value has been set for the `pfmManagerHost` property in the `jp1itslm.properties` system definition file, it is assumed that Performance Management is not linked and the **System performance information** area is not displayed.

When you select a monitored service or monitored target in the **Services** area, the host that provides the monitored service you selected is displayed in this window.

Similarly, when you select a monitored service or monitored target in the **Service performance information** area, the host that provides the monitored service you selected is displayed in this window.

If you click ▶ to the left of the host, the icon changes to ▼ and the monitoring agent that belongs to the host is displayed.

If you then click ▶ to the left of the monitoring agent, the icon changes to ▼ and the system performance monitoring items are displayed.

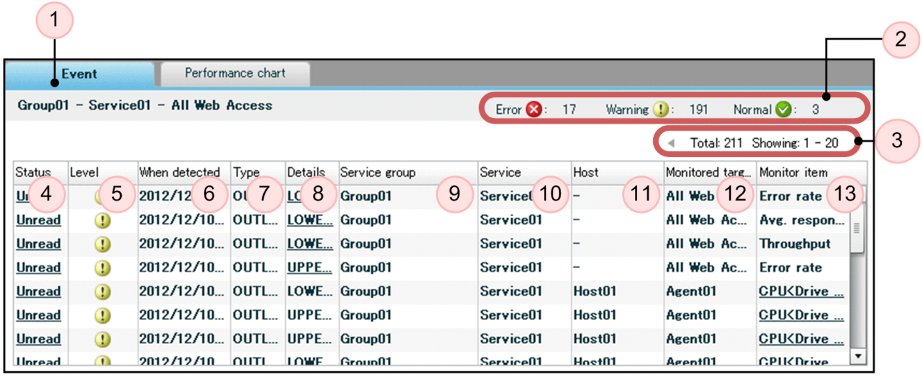
The update interval of the display can be set in the `dashboardSystemUpdateInterval` property in the `jp1itslm.properties` system definition file.

The following table lists the items that are displayed:

No.	Item	Description
1	Cumulative totals	This area shows the total number of events of each event type (error, warning, normal, and stopped) for all the monitored items that are displayed in the **System performance information** area.
2	**Monitor item (unit)**	This column displays the name of the monitored service, host, monitoring agent, or monitoring item.
3	**Service group**	This column displays the name of the service group to which the monitored service belongs.
4	**Status**	This column displays the monitoring results for the host, monitoring agent, or monitoring item displayed on the same row in the **Monitored target** column, using the following icons: ✖ (error) There is at least one item for which an error has occurred in threshold monitoring. ! (warning) There is at least one item for which a warning has occurred in trend monitoring or out-of-range value detection. ✓ (normal) The status of all items is normal. ⏸ (monitoring stopped) The monitored service is not being monitored. If different conditions occur in the monitoring results for different monitoring items in a single host or monitoring agent, the icon for the highest-priority results is displayed, according to the following priority order (highest to lowest): error > warning > normal. (In the case where monitoring of a monitored service has stopped, only the stopped status is possible.) The row for a monitored service displays a hyphen (-).
5	**Measured**	These three columns each display a value (up to 3 digits after the decimal point) for the item. If there is no data to display, a hyphen (-) is displayed.
6	**Threshold**	
7	**Baseline**	

10.3.5 Event and Performance chart tabs area (Event tab selected)

(1) Window configuration



Group01 - Service01 - All Web Access

Error ✖: 17 Warning !: 191 Normal ✓: 3

◀ Total: 211 Showing: 1 - 20

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored targ...	Monitor item
Ur		2012/12	OU	LC	Group01	Service(	-	All Web	Error rate
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	-	All Web Ac...	Avg. respon...
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	-	All Web Ac...	Throughput
Unread	!	2012/12/10...	OUTL...	UPPE...	Group01	Service01	-	All Web Ac...	Error rate
Unread	!	2012/12/10...	OUTL...	LOWE...	Group01	Service01	Host01	Agent01	CPU<Drive ...
Unread	!	2012/12/10...	OUTL...	UPPE...	Group01	Service01	Host01	Agent01	CPU<Drive ...
Unread	!	2012/12/10...	OUTL...	UPPE...	Group01	Service01	Host01	Agent01	CPU<Drive ...
Unread	!	2012/12/10	OUTL	LOWE	Group01	Service01	Host01	Agent01	CPU<Drive

(2) Window description

This window displays a list of events. The events displayed depend on the selections in the **Services** and **Service performance information** areas, as described below:

No.	Selection in the Services area	Selection in the Service performance information area	Events displayed on the Event tab (Event and Performance chart tabs area)
1	--	--	Displays events for the monitored targets within the monitored services of all service groups.
2	Service group	--	Displays events for the monitored targets in all the monitored services in the service group selected in the **Services** area.
3		Monitored service	Displays events for the monitored targets in the monitored service selected in the **Service performance information** area.
4		Monitored target	Displays events for the monitored target selected in the **Service performance information** area.
5	Monitored service	--	Displays events for all the monitored targets within the monitored service selected in the **Services** area.
6		Monitored service	Displays events for the monitored targets in the monitored service selected in the **Service performance information** area.
7		Monitored target	Displays events for the monitored target selected in the **Service performance information** area.
8	Monitored target	--	Displays events for the monitored target selected in the **Services** area.
9		Monitored service	Displays events for all the monitored targets in the monitored service selected in the **Service performance information** area.
10		Monitored target	Displays events for the monitored target selected in the **Service performance information** area.

Legend:

--: No selection.

Note that system performance monitoring and availability monitoring events are also displayed in the list of events. When you select a monitored target in the **Service performance information** area in order to set system performance monitoring or availability monitoring for a monitored service, the event list will display events related to the system performance and availability monitoring that were set for the monitored service to which that monitored target belongs.

The events displayed when you select a service group or monitored service are displayed in the same way as the service performance events.

Events are displayed with the most recent at the top. If you have narrowed down the displayed monitored targets by executing a search in the **Services** area, selecting a service group will display information for only the monitored targets that are shown in the search results.

Once it is displayed, an event continues to appear until it reaches its seven-day cutoff. The display is updated every three seconds.

The following table lists the items that are displayed:

No.	Item	Description
1	*X* - *Y* - *Z*	This area displays the names of the service group, the monitored service, and the monitored target whose events you have selected to view. *X* is the name of the service group, *Y* is the name of the monitored service, and *Z* is the name of the monitored target. Not all three names are always displayed: • If a service group was selected in the **Services** area, only *X* is displayed. • If a monitored service was selected in the **Services** area or **Service performance information** area, only *X* - *Y* are displayed. • If a monitored target was selected in the **Services** area or **Service performance information** area, *X* - *Y* - *Z* are displayed. • If nothing was selected in the **Services** and **Service performance information** areas, nothing is displayed.
2	Cumulative totals	This area shows the cumulative total for each event type (error, warning, or normal) that occurred during the last seven days.
3	◀ **Total:** *n1* **Showing:** *n2*-*n3* ▶	When more than 20 events occurred in the last seven days, the additional events are displayed on subsequent pages. Click ◀ or ▶ to display the previous or next page, respectively. If there is no previous page or next page, you cannot click icon. *n2* and *n3* indicate the range of event items displayed on the current page, and *n1* is the total number of displayed events. If there is more than one monitored service, the maximum number of events displayed per page can be changed by specifying the `dashboardEventListRecentViewSize` property. When you change the number of items to be displayed per page, *n1* will reflect the changed value. For details about the `dashboardEventListRecentViewSize` property, see *5.6.2 Editable definitions*.
4	**Status**	This column indicates whether each event has been checked (read). **Unread** This is the default value, before the user has clicked the row's **Status** column. When **Unread** is displayed, the entire row is in displayed in boldface. **Read** This setting indicates that the row's **Status** column has been clicked. After you check an event by reviewing the contents of its row, click the row in this column to change **Unread** to **Read**. Once an event's **Status** column entry is changed to **Read** it cannot be changed back to **Unread**.
5	**Level**	This column displays for each event one of the following icons indicating the status of the average response time, throughput, and error rate at the time the event occurred. The following icons are used: ⊗ (error) An error occurred in threshold monitoring or availability monitoring.

No.	Item	Description
5	**Level**	⚠ (warning) A warning occurred in trend monitoring or out-of-range value detection. ✓ (normal) Errors that occurred in availability monitoring have been recovered. When multiple service performance events are applicable simultaneously, the icon for the highest-priority event is displayed, according to the following priority order (highest to lowest): error > warning > normal.
6	**When detected**	This column displays the date and time that the event occurred, in the format *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*).
7	**Type**	This column displays one of the following character strings indicting the type of the error or warning: **THRESHOLD** Monitoring detected that the threshold was exceeded (error). **OUTLIER** An out-of-range value that differs significantly from the norm for the monitored service was detected (warning). **TREND** A trend was detected indicating that the threshold seems likely to be exceeded (warning). **AVAILABILITY** Monitoring detected that the monitored service has stopped or has recovered from having stopped (error or normal).
8	**Details**	This column displays one of the following character strings providing more detail about the type of error or warning displayed in the **Type** column: **UPPER LIMIT** This is displayed when the **Type** column is **THRESHOLD** or **OUTLIER**. When the **Type** column is **THRESHOLD**, **UPPER LIMIT** indicates that the monitoring item's service performance or system performance exceeded the threshold. When the **Type** column is **OUTLIER**, **UPPER LIMIT** indicates that the monitoring item's service performance exceeded the upper limit value. **LOWER LIMIT** This is displayed when the **Type** column is **THRESHOLD** or **OUTLIER**. When the **Type** column is **THRESHOLD**, **LOWER LIMIT** indicates that the monitoring item's system performance exceeded the threshold. When the **Type** column is **OUTLIER**, **LOWER LIMIT** indicates that the monitoring item's service performance or system performance fell below the lower limit value. *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* This is displayed when the **Type** column is **TREND**, and indicates the date and time when it is expected that service performance or system performance of the monitoring item will exceed the threshold (*year*/*month*/*date hour*:*minute*:*second*). **SERVICE FAILURE** This is displayed when the **Type** column is **AVAILABILITY**, and indicates that the monitoring item (indicated under **Monitor item**) has stopped. **SERVICE REPAIR** This is displayed when the **Type** column is **AVAILABILITY**, and indicates that the monitoring item (indicated under **Monitor item**) has recovered from a stop. If you click this column on a row, you will see in the Troubleshoot window a graph of the monitoring item's service performance. For details about how to do this, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.
9	**Service group**	This column displays the name of the service group in which the event occurred.

No.	Item	Description
10	**Service**	This column displays the name of the monitored service in which the event occurred.
11	**Host**	An entry (other than a hyphen) is displayed in this column when system performance is monitored. The entry is the name of the host on which the event occurred. For an event associated with service performance monitoring, a hyphen (−) is displayed.
12	**Monitored target**	This column displays the name of the monitored target for which the event occurred.
13	**Monitor item**	This column displays the monitoring item for which the event occurred.

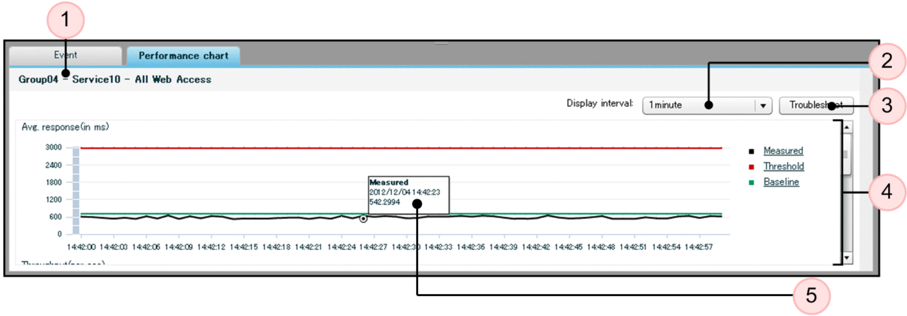
If you display the Troubleshoot window by clicking the **Troubleshoot** button on the **Performance chart** tab or by clicking the **Details** column on the **Event** tab in the **Event** and **Performance chart** tab area of the Real-time Monitor window, the Troubleshoot window will be displayed with the monitored service already selected.

(3) Supplemental notes

- On occasion, there might be a time lag of a few seconds to several tens of seconds before information is displayed in the **Service performance information** area and in the **Event** and **Performance chart** tabs area.

10.3.6 Event and Performance chart tabs area (Performance chart tab selected)

(1) Window configuration



Group04 - Service10 - All Web Access

Display interval: 1minute

(2) Window description

The **Performance chart** tab is selectable only when you have selected a monitored target for a monitored service in the **Services** area or the **Service performance information** area.

You cannot display a performance chart for a system performance monitoring item.

The **Performance chart** tab displays for each monitoring item a line graph of the service performance of the selected monitored target of the monitored service. The display is updated every three seconds.

The following table lists the items that are displayed:

No.	Item	Description
1	*X* - *Y* - *Z*	This area displays the names of the service group, monitored service, and monitored target for which performance charts are being displayed.

No.	Item	Description
1	*X* - *Y* - *Z*	*X* is the name of the service group, *Y* is the name of the monitored service, and *Z* is the name of the monitored target.
2	**Display interval** pull-down menu	Use this pull-down menu to select the interval to be used for aggregating the data to be displayed on the performance charts. The following values can be selected (the default is **1 minute**): • **1 minute** • **3 minutes** • **5 minutes**
3	**Troubleshoot** button	Clicking this button displays the Troubleshoot window for the monitored target of the monitored service. You can check the past status of the monitored target of the selected monitored service. For details about how to check the past status, see *4.4.2 Checking past data*.
4	Performance charts	This area displays performance charts for the selected monitored target of the monitored service. Performance charts for the following monitoring items can be displayed: • **Avg. response (in ms)** • **Throughput (per sec)** • **Error rate (%)** The following values can be plotted and displayed as line graphs on each performance chart: • **Measured** • **Threshold**#1 • **Baseline**#2 • **Error Predict. (upper limit)**#2 • **Error Predict. (lower limit)**#2 A legend showing the meaning of each graph line is generated and displayed on the right side of a performance chart. Use the Select items to be displayed dialog box to select the values to be plotted and displayed. Click the legend to display the Select items to be displayed dialog box. Select the check boxes for the items whose values you want to have plotted and displayed, and then click the **Settings** button. The values for **Measured**, **Threshold**, and **Baseline** are displayed by default. Each graph line is displayed based on values aggregated over the time period set in the **Display interval** pull-down menu.
5	Performance chart details	Details are displayed when you hover the cursor on a graph line on a performance chart. The following items are displayed: • Type of values plotted for the graph line • Date and time of the value where the cursor is hovered, in the format *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*) • Value at the point where the cursor is hovered

#1

This is displayed if you have set **SLO monitor settings** in the Settings window.

#2

This is displayed if you have set **Error Predict. settings** in the Settings window.

Real-time Monitor window (performance chart baseline)

- Note that **Baseline** will not be displayed until the number of days since the start of monitoring has reached the **Days till start** value that was set under **Error Predict. settings** in the Monitor settings area of the Settings window. For details about the **Days till start** setting in the Settings window, see *3.2.7 Setting up the monitoring items for service performance*.
- If there is no information for a specific time period (for example, if there is a period during which no data was stored because monitoring of the relevant monitored service had stopped), the applicable lines on the performance chart will not be displayed.

- From one hour before the end of daylight saving time until daylight saving time ends, the time is not displayed along the horizontal axis. In this case, check the time by moving the cursor over a line graph on the performance chart.

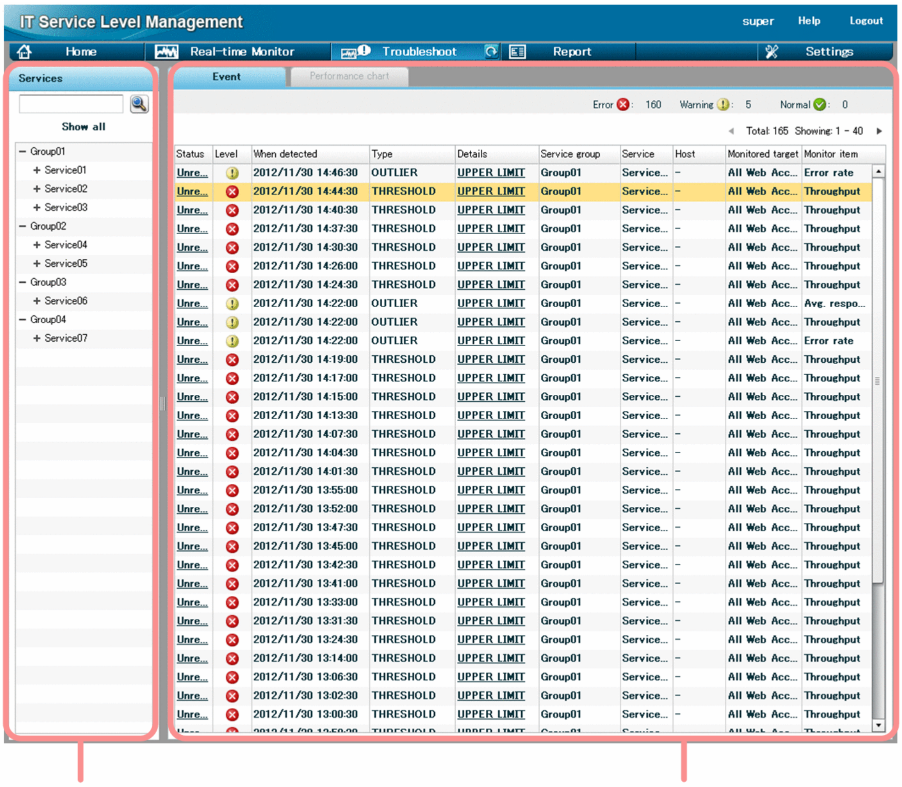
(3) Supplemental notes

- On occasion, there might be a time lag of a few seconds to several tens of seconds before information is displayed in the **Service performance information** area and the **Event** and **Performance chart** tabs area.
- If the system running ITSLM experiences heavy load conditions, it might delay display of the performance charts in the **Performance chart** tab. If this occurs, select **3 minutes** or **5 minutes** in the **Display interval** pull-down menu.

10.4 Troubleshoot window

10.4.1 Configuration of the Troubleshoot window

(1) Window configuration



Error ✕: 160 Warning !: 5 Normal ✓: 0

◀ Total: 165 Showing: 1 - 40 ▶

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unre...	!	2012/11/30 14:46:30	OUTLIER	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Error rate
Unre...	✕	2012/11/30 14:44:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:40:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:37:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:30:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:26:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:24:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	!	2012/11/30 14:22:00	OUTLIER	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Avg. respo...
Unre...	!	2012/11/30 14:22:00	OUTLIER	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	!	2012/11/30 14:22:00	OUTLIER	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Error rate
Unre...	✕	2012/11/30 14:19:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:17:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:15:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:13:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:07:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:04:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 14:01:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:55:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:52:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:47:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:45:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:42:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:41:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:33:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:31:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:24:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:14:00	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:06:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:02:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput
Unre...	✕	2012/11/30 13:00:30	THRESHOLD	UPPER LIMIT	Group01	Service...	-	All Web Acc...	Throughput

Services area

Event and **Performance chart** tabs area

(2) Window description

The Troubleshoot window is used when an error or warning has been detected to check when the event that caused the problem occurred. In addition, if Performance Management is linked, you can check for problems in the host or middleware that provides the affected monitored service.

The Troubleshoot window is composed of the following areas:

- **Services** area
- **Event** and **Performance chart** tabs area
- **Access log** area

(3) Supplemental notes

- The Troubleshoot window display is not updated in real time. To update the display, you must click the ⟳ (reload) button, which is one of the **Troubleshoot** buttons at the top of the window. When you update, the **Event** tab becomes selected in the **Event** and **Performance chart** tabs area.
- Depending on how you display the Troubleshoot window, the **Event** and **Performance chart** tabs area will display different events that occurred at different times:

  - If you display the Troubleshoot window immediately after login by clicking the **Troubleshoot** button at the top of a window, the displayed Troubleshoot window displays a list of the events that had occurred at the time of your login.
  - If you display the Troubleshoot window a while after login by clicking the **Troubleshoot** button at the top of a window, the displayed Troubleshoot window displays a list of the events that had occurred at the time you displayed the Troubleshoot window.
  - If you display the Troubleshoot window by clicking the **Details** column for an event in the **Events in the last 7 days** area of the Home window or in the **Event** and **Performance chart** tabs area of the Real-time Monitor window, the displayed Troubleshoot window displays performance charts representing the service performance at the time the clicked event occurred. If you then click the **Event** tab, the Troubleshoot window displays a list of the most recent events associated with the clicked event's monitored service at the time of the transition to the Troubleshoot window. If you click the **Details** column for an event in the **Event** and **Performance chart** tabs area in the Troubleshoot window, when you return to the **Event** tab from the **Performance chart** tab, the list of the most recent events will still be displayed there.
  - If you display the Troubleshoot window by clicking the **Troubleshoot** button in the **Event** and **Performance chart** tabs area of the Real-time Monitor window, the displayed Troubleshoot window displays performance charts representing the service performance at the time you clicked. If you then click the **Event** tab, the Troubleshoot window displays a list of the most recent events associated with the clicked event's monitored service at the time of the transition to the Troubleshoot window.
  - If you redisplay the Troubleshoot window (while the Troubleshoot window is already being displayed) by clicking the ⟳ (reload) button, which is one of the **Troubleshoot** buttons at the top of the window, the display will be of a list of events that had occurred at the time you clicked.

10.4.2 Services area

This area is common to all the ITSLM windows. For details about the **Services** area window, see *10.1.2(3) Services area*.

10.4.3 Event and Performance chart tabs area (Event tab selected)

(1) Window configuration and Window description

This window displays the same contents as the Real-time Monitor window, except that the Troubleshoot window displays 40 events per page. See *10.3.5 Event and Performance chart tabs area (Event tab selected)*.

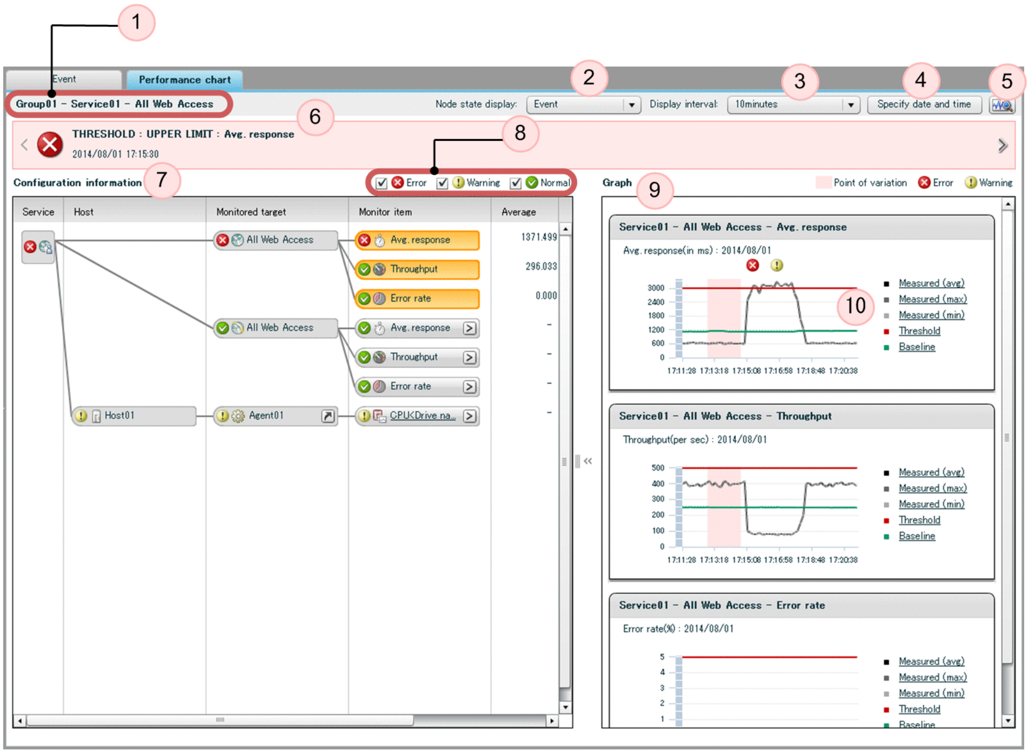
(2) Supplemental notes

- Depending on how you display the Troubleshoot window, the **Event** and **Performance chart** tabs area will display different events that occurred at different times:
  - If you display the Troubleshoot window by clicking the **Troubleshoot** button at the top of a window, the displayed Troubleshoot window displays a list of the events that had occurred at the time of your login.
  - If you display the Troubleshoot window by clicking the **Details** column for an event in the **Events in the last 7 days** area of the Home window or in the **Event** and **Performance chart** tabs area of the Real-time Monitor window, the displayed Troubleshoot window displays performance charts representing the service performance at the time you clicked. If you then click the **Event** tab, the Troubleshoot window displays a list of the events that had occurred at the time you clicked the **Details** column. However, if you click the **Details** column in the Troubleshoot window, it will not change the time displayed in the **Event** and **Performance chart** tabs area.

- If you display the Troubleshoot window by clicking the **Troubleshoot** button in the **Event** and **Performance chart** tabs area of the Real-time Monitor window, the displayed Troubleshoot window displays performance charts representing the service performance at the time you clicked. If you then click the **Event** tab, the Troubleshoot window displays a list of the events that had occurred at the time you clicked the **Troubleshoot** button.
- If you redisplay the Troubleshoot window (while the Troubleshoot window is already being displayed) by clicking the ⟳ (reload) button, which is one of the **Troubleshoot** buttons at the top of the window, the display will be of a list of events that had occurred at the time you clicked.

10.4.4 Event and Performance chart tabs area (Performance chart tab selected)

(1) Window configuration



Group01 - Service01 - All Web Access

Node state display: Event

Display interval: 10minutes

Specify date and time

THRESHOLD : UPPER LIMIT : Avg. response
2014/08/01 17:15:30

Service01 - All Web Access - Avg. response
Avg. response(in ms) : 2014/08/01

Service01 - All Web Access - Throughput
Throughput(per sec) : 2014/08/01

Service01 - All Web Access - Error rate
Error rate(%) : 2014/08/01

(2) Window description

This window displays performance charts for a monitored target within a monitored service.

The following table lists the items that are displayed:

No.	Item	Description
1	*X* - *Y* - *Z*	This area displays the names of the service group, monitored service, and monitored target within the monitored service whose performance charts you want to view. *X* is the name of the service group, *Y* is the name of the monitored service, and *Z* is the name of the monitored target within the monitored service.

No.	Item	Description
2	**Node state display** pull-down menu	Use this pull-down menu to select one of the following items as the base for determining the node state display for monitoring items (the default is **Event**): • **Event** • **Monitor item state** The display status of **Configuration information** and **Graph** depends on your selection here.
3	**Display interval** pull-down menu	Use this pull-down menu to select the interval to be used for aggregating the data to be displayed on the performance charts. The following values can be selected (the default is **1 hour**): • **1 minute** • **10 minutes** • **30 minutes** • **1 hour** • **6 hours** • **1 day** Regardless of the value you select, the number of values that will be plotted on each performance chart will be 61. The values calculated from data obtained over the time period you select will be plotted onto a chart divided into 61 equally-sized display intervals.
4	**Specify date and time** button	Click this button to display the Specify Date and Time dialog box that you use to specify the start date and time for the data to be displayed on the performance charts. You can specify a date and time up to 60 days in the past.
5	**Access log** button	Click this button to display the **Access log** area in the Troubleshoot window, where you can check the past status of the selected monitored target within the monitored service. For details about how to check the past status, see *4.4.2 Checking past data*.
6	❮ *message* ❯	This area is displayed when you display charts from a list of events. *message* in this area consists of an icon indicating the type of event, the type of event in text, the event details, the monitoring item, and the date and time the event occurred. The following format is used: *icon event-type* **:** *detail* **:** *monitoring-item* *YYYY*/*MM*/*DD hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*) If you click ❮ or ❯ at the left or right end of this area, the message for the preceding or subsequent event, respectively, is displayed. If there is no preceding or subsequent event, the corresponding icon cannot be clicked.
7	**Configuration information**	This area displays the relationships between monitored services and hosts. When you display performance charts from a list of events, this area displays configuration information for the monitored service in which the selected event occurred. When you select a monitored target from the **Services** area, this area displays configuration information for the service group or monitored service selected from the **Services** area. The configuration information that is displayed depends on what you select on the **Node state display** pull-down menu: • **Event** is selected The information that is displayed is based on events that occurred within the period of time displayed in **Graph**. • **Monitor item state** is selected The information that is displayed is based on the status of the monitoring item. Note that even if the parent node is normal, if the child node is in error or warning status, the status of the child node is propagated to the parent node. If multiple child nodes of a parent node have different statuses, the highest-priority status is propagated to the parent node, according to the following priority order (highest to lowest): error > warning > normal. However, no other status can propagate to a node whose status is that monitoring has stopped. In addition, if an error or warning is displayed for a system performance monitoring item, the status does not propagate to the monitored service.

No.	Item	Description
7	**Configuration information**	If an error or warning is displayed for a system performance monitoring item while the value of the `dashboardPropagateSystemStatus` property in ITSLM - Manager's system definition file (`jp1itslm.properties`) is set to `true`, the status is propagated to the monitored service. If this property is set to `false`, the status is not propagated to the monitored service. Click ▷ for a monitoring item to see a performance chart for that monitoring item. Up to 10 charts can be displayed in the **Graph** area. To hide a displayed performance chart, click ▁ for the monitoring item or click ✕ to the right of the performance chart itself. Click ↗ for a monitored target associated with a host to launch the PFM - Web Console window in a separate browser.
8	**Configuration information** legend	You can use the check box next to each legend icon to show or hide the corresponding monitor items in the **Configuration information** area.
9	**Graph**	This area displays performance charts for the selected events. The date and time (*YYYY*/*MM*/*DD hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*)) are displayed with the following performance charts: • **Avg. response (in ms)** • **Throughput (per sec)** • **Error rate (%)** If you are linked to Performance Management, you can also display performance charts for system performance. In each performance chart, the following items can be displayed as a line graph: • **Measured (avg)** The average measured values for the period divided into 61 equally-sized display intervals. • **Measured (max)** The maximum measured values for the period divided into 61 equally-sized display intervals. • **Measured (min)** The minimum measured values for the period divided into 61 equally-sized display intervals. • **Threshold** The value set under **SLO monitor settings** in the Settings window. • **Baseline** The average baseline value for the period divided into 61 equally-sized display intervals. This graph is not displayed unless **Error Predict. settings** is set in the Settings window. • **Error Predict. (upper limit)** The maximum baseline value for the period divided into 61 equally-sized display intervals. This graph is not displayed unless **Error Predict. settings** is set in the Settings window. • **Error Predict. (lower limit)** The minimum baseline value for the period divided into 61 equally-sized display intervals. This graph is not displayed unless **Error Predict. settings** is set in the Settings window. The upper part of the performance chart depends on what you select on the **Node state display** pull-down menu: • **Event** is selected Events that occurred within the period of time displayed in the performance chart are displayed as icons. • **Monitor item state** is selected Events that occurred within the period of time displayed in the performance chart are displayed as icons, plus the status of the monitoring item is displayed as a band. ⊗ (error): The band is displayed in red.

No.	Item	Description
9	**Graph**	⚠ (warning): The band is displayed in yellow. If your **Display interval** specification is six hours or one day, events are displayed as one icon per minute. For finer-grained checking of the details of event occurrence, specify one hour or a smaller interval in **Display interval**. A legend showing the meaning of each graph line is generated and displayed on the right side of a performance chart. Use the Select items to be displayed dialog box to select the values to be plotted and displayed. Click the legend to display the Select items to be displayed dialog box. Select the check boxes for the items whose values you want to have plotted and displayed, and then click the **Settings** button. The values for **Measured (avg)**, **Measured (max)**, **Measured (min)**, **Threshold**, and **Baseline** are displayed by default. Each graph line is displayed based on values aggregated over the time period set in the **Display interval** pull-down menu. However, the width of the bands indicating timeframes of variation is the same regardless of the display interval.
10	Performance chart details	Details are displayed when you hover the cursor over a graph line on a performance chart. The following items are displayed: • Type of values plotted for the graph line • Date and time of the value where the cursor is hovered, in the format *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* (*year*/*month*/*date hour*:*minute*:*second*) • Value at the point where the cursor is hovered

Table 10–3: Items displayed in the Configuration information area

No.	Header	Items displayed	
		Service performance-related node	System performance-related node
1	**Service**	Displays the monitored service.	
2	**Host**	Nothing	Displays the host belonging to the monitored service in the parent node.
3	**Monitored target**	Displays one of the following belonging to the monitored service in the parent node: • **All Web Access** • *web-transaction-name*	Displays the monitoring agents belonging to the host in the parent node.
4	**Monitor item**	Displays the service performance monitoring items belonging to the monitored target in the parent node. The following monitoring items can be displayed: • **Ave. Response** • **Throughput** • **Error rate**	Displays the system performance monitoring items belonging to the monitored target in the parent node.
5	**Average**#	Displays for each monitoring item the average value calculated from the data points (maximum of 61) used in the **Measured (avg)** graph.	
6	**Maximum**#	Displays for each monitoring item the maximum value calculated from the data points (maximum of 61) used in the **Measured (max)** graph.	
7	**Minimum**#	Displays for each monitoring item the minimum value calculated from the data points (maximum of 61) used in the **Measured (min)** graph.	
8	**Unit**	Displays the unit of measurement used for each monitoring item.	

#

If there are no data points for a calculation in the entire range from the left end to the right end of the performance chart, a hyphen (-) is displayed.

Cases where items are not displayed on the performance chart

- The performance chart baseline will not be displayed until the number of days since the start of monitoring has reached the **Days till start** value that was set under **Error Predict. settings** in the **Monitor settings** area of the Settings window. For details about the **Days till start** setting in the Settings window, see *3.2.7 Setting up the monitoring items for service performance*.
- If there is no information for a specific time period (for example, if there is a period during which no data was stored because monitoring of the relevant monitored service had stopped), the applicable lines on the performance chart will not be displayed. In addition, if monitoring of a monitored service stops before the calculation of a point of variation on the graph, the band indicating the variation point will not appear immediately prior to the stop.
- From one hour before the end of daylight saving time until daylight saving time ends, the time is not displayed along the horizontal axis. In this case, check the time by moving the cursor over a line graph on the performance chart.

Handling of missing performance data on the performance chart

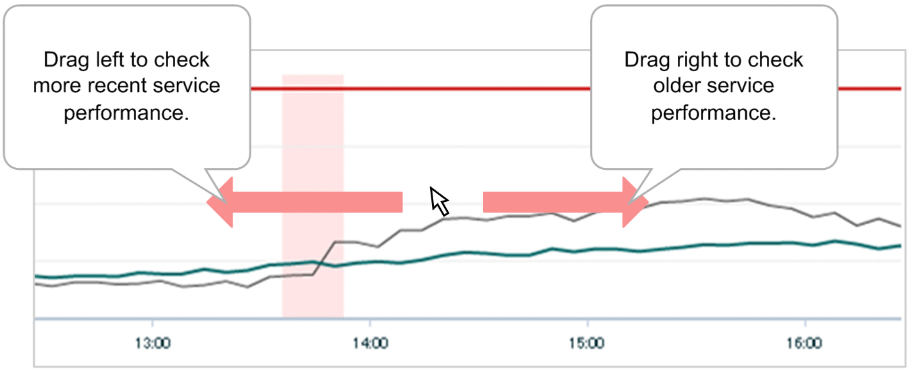
If there is a period for which no performance data was stored in the database, the immediately preceding status is displayed continuously up to the next recorded event.

Interval displayed in the performance charts

- When an event is selected from the event list while the **Performance chart** tab is displayed in the Troubleshoot window, the performance charts are displayed so that the display interval selected in **Display interval** is centered at the time the event occurred.
- When a monitored target is selected from the **Services** area or the reload button is clicked while the **Performance chart** tab is displayed in the Troubleshoot window, the performance charts are displayed so that the current time is positioned at the right end of the chart using the display interval selected in **Display interval**.
- When you specify a date and time in the Specify date and time dialog box, the performance charts are displayed so the time that you specified is centered using the display interval selected in **Display interval**.

Manipulating performance charts

By dragging a performance chart left and right, you can check the status of the monitored service in time periods before and after the occurrence of the event. With a single drag, you can see an interval that is the same duration as the current display interval. For example, if the display interval is 10 minutes, one drag lets you check a total of 20 minutes.


Drag left to check more recent service performance.
Drag right to check older service performance.
13:00
14:00
15:00
16:00

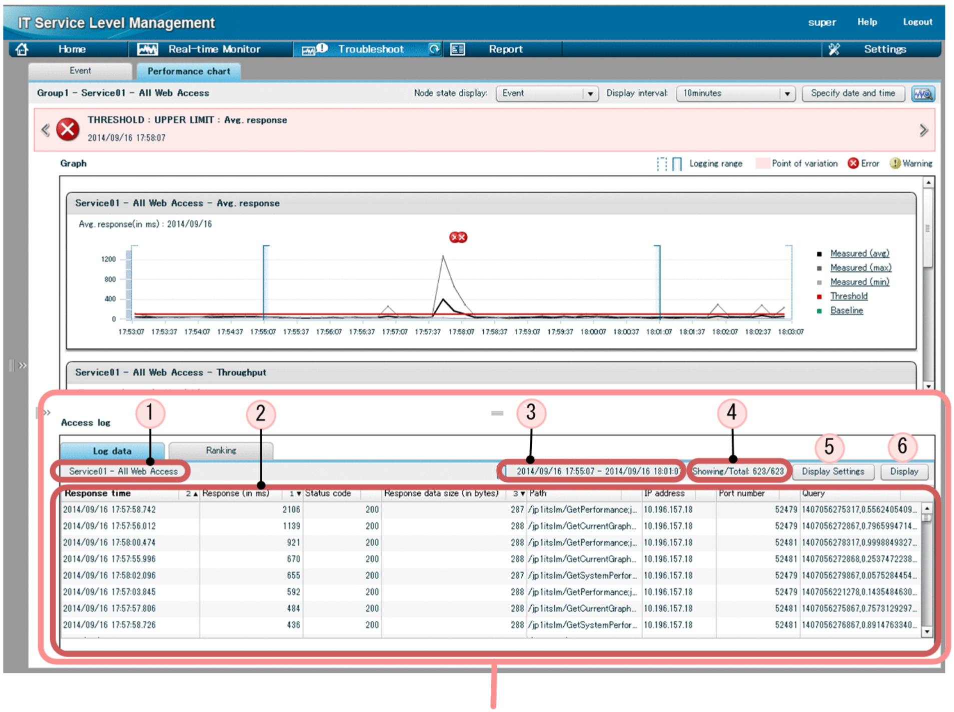
(3) Supplemental notes

- The **Performance chart** tab cannot be selected unless you have selected a monitored target within a monitored service in the **Services** area.
- Depending on how you display the Troubleshoot window, the **Event** and **Performance chart** tabs area will display different events that occurred at different times.

    - If you display the Troubleshoot window by clicking the **Troubleshoot** button at the top of a window, the displayed Troubleshoot window displays a list of the events that had occurred at the time of your login.
    - If you display the Troubleshoot window by clicking the **Details** column for an event in the **Events in the last 7 days** area of the Home window or in the **Event** and **Performance chart** tabs area of the Real-time Monitor window, the displayed Troubleshoot window displays performance charts representing the service performance at the time you clicked. If you then click the **Event** tab, the Troubleshoot window displays a list of the events that had occurred at the time you clicked the **Details** column. However, if you click the **Details** column in the Troubleshoot window, it will not change the time displayed in the **Event** and **Performance chart** tabs area.
    - If you display the Troubleshoot window by clicking the **Troubleshoot** button in the **Event** and **Performance chart** tabs area of the Real-time Monitor window, the displayed Troubleshoot window displays performance charts representing the service performance at the time you clicked. If you then click the **Event** tab, the Troubleshoot window displays a list of the events that had occurred at the time you clicked the **Troubleshoot** button.
    - If you redisplay the Troubleshoot window (while the Troubleshoot window is already being displayed) by clicking the ⟳ (reload) button, which is one of the **Troubleshoot** buttons at the top of the window, the display will be of a list of events that had occurred at the time you clicked.
- If you select another service group, monitored service, or monitored target in the **Services** area while the **Performance chart** tab is being displayed, the display will switch automatically to the **Event** tab.
- Performance charts are displayed in the Troubleshoot window based on the results of aggregating past data. However, when the **Display interval** pull-down menu is set to **1 minute**, the performance charts will be displayed based on the most recent data.
- If the data update interval for a system performance monitoring item is too long with respect to the value set in the **Display interval** pull-down menu, the performance charts might be displayed as points. In such a case, set a longer display interval.
- The performance chart might not be displayed correctly when data from a version earlier than 10-10 is stored in the database and **Monitor item state** was selected from **Node state display**. The following are examples:
    - The status of the monitoring item is treated as normal only when no event has been issued in the past.
    - Even when the monitoring item has recovered from an overage of a threshold or baseline, its band is not displayed correctly because the monitoring item's previous status (error or warning) is displayed until the end of the display range.
    - If the status of the monitoring item changed to a warning error within the display range, that change is displayed correctly, but if the status changed from error to warning, error continues to be displayed.

10.4.5 Access log area (Log data tab selected)

(1) Window configuration



Response time	2 ▲ Response (in ms)	1 ▼ Status code	Response data size (in bytes)	3 ▼ Path	IP address	Port number	Query
2014/09/16 17:57:58.742	2106	200	287	/jp1itslm/GetPerformance;j...	10.196.157.18	52479	1407056275317,0.5562405409...
2014/09/16 17:57:56.012	1139	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52479	1407056272867,0.7965994714...
2014/09/16 17:58:00.474	921	200	288	/jp1itslm/GetPerformance;j...	10.196.157.18	52481	1407056278317,0.9998849327...
2014/09/16 17:57:55.996	670	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52481	1407056272868,0.2537472238...
2014/09/16 17:58:02.096	655	200	287	/jp1itslm/GetSystemPerfor...	10.196.157.18	52479	1407056279867,0.0575284454...
2014/09/16 17:57:03.845	592	200	288	/jp1itslm/GetPerformance;j...	10.196.157.18	52479	1407056221278,0.1435484630...
2014/09/16 17:57:57.806	484	200	288	/jp1itslm/GetCurrentGraph...	10.196.157.18	52481	1407056275867,0.7573129297...
2014/09/16 17:57:58.726	436	200	288	/jp1itslm/GetSystemPerfor...	10.196.157.18	52481	1407056276867,0.8914763340...

Access log area

(2) Window description

This window displays a tabular list of access logs for a monitored target within a monitored service.

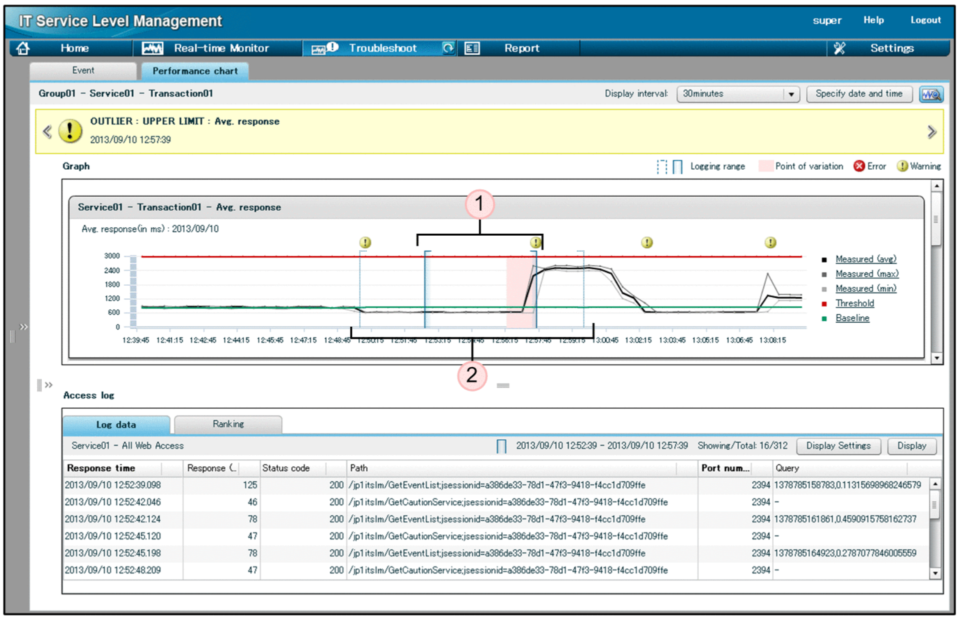
No.	Item	Description
1	*X* - **All Web Access**	This area displays the name of the service group whose performance charts are to be viewed. *X* is the name of a service group.
2	**Access log** list	This area displays a tabular list of access logs over the range indicated by the solid lines in the performance charts. The access logs displayed in the **Access log** area show data acquired up to five minutes before the current time. The items to display are selected in the Select items to be displayed window.
3	Logging range	This area displays the interval being displayed in the **Log data** tab using the following format. **Display format** *YYYY*/*MM*/*DD hh*:*mm*:*ss* - *YYYY*/*MM*/*DD hh*:*mm*:*ss*
4	**Showing/Total**	This area displays the number of access logs. **Showing** (*nnnn*) The number of access logs being displayed in the **Log data** tab **Total** (*mmmm*) The number of access logs in the range indicated by the solid lines in the performance charts

No.	Item	Description
4	**Showing/Total**	Display format *nnnn*/*mmmm*
5	**Display Settings** button	Clicking this button displays the Select items to be displayed window.
6	**Display** button	Clicking this button displays the **Confirmation of the display of the access log** window.

Logging range of the access logs

In the performance charts, dotted lines indicate the range targeted for display in the **Access log** area. Solid lines indicate the range actually being displayed in the **Access log** area.

Figure 10–2: Logging range in the Access log area



OUTLIER : UPPER LIMIT : Avg. response
2013/09/10 12:57:39

Service01 - All Web Access
2013/09/10 12:52:39 - 2013/09/10 12:57:39 Showing/Total: 16/312

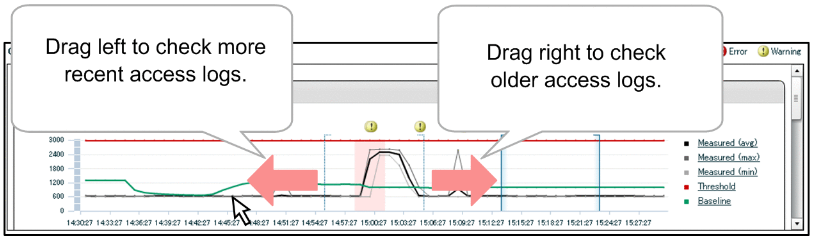
Response time	Response (...	Status code	Path	Port num...	Query
2013/09/10 12:52:39.098	125	200	/jp1itslm/GetEventList;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe	2394	1378785158783,0.11315698968246579
2013/09/10 12:52:42.046	46	200	/jp1itslm/GetCautionService;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe	2394	-
2013/09/10 12:52:42.124	78	200	/jp1itslm/GetEventList;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe	2394	1378785161861,0.4590915758162737
2013/09/10 12:52:45.120	47	200	/jp1itslm/GetCautionService;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe	2394	-
2013/09/10 12:52:45.198	78	200	/jp1itslm/GetEventList;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe	2394	1378785164923,0.2787077846005559
2013/09/10 12:52:48.209	47	200	/jp1itslm/GetCautionService;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe	2394	-

No.	Item	Description
1	Logging range (solid lines)	The range of access logs actually being displayed in the **Access log** area.
2	Logging range (dotted lines)	The range of access logs targeted for display in the **Access log** area.

The dotted lines are shown when the display interval in the **Performance chart** tab is 30 minutes or longer.

You can change the logging range of the access logs by clicking and dragging the performance chart.

Figure 10–3: Changing the logging range in the Access log area



Drag left to check more recent access logs.

Drag right to check older access logs.

Interval of the logging range (dotted lines)

The logging range indicated by the dotted lines in the **Access log** area changes depending on the display interval of the performance chart.

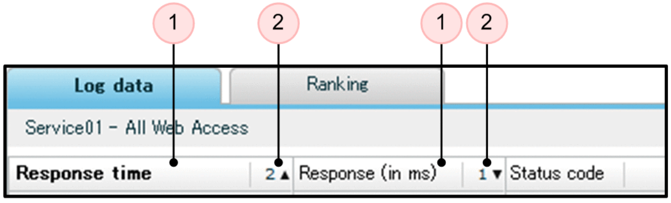
No.	Display interval in the Performance chart tab	Display interval in the Access log area	Logging range displayed between the dotted lines
1	1 minute	1 minute	The range of access logs shown in the **Performance chart** tab when you click the **Display** button.
2	10 minutes	10 minutes	
3	30 minutes	10 minutes	The range of access logs indicated by the dotted lines in the **Performance chart** tab when you click the **Display** button.
4	1 hour	10 minutes	
5	6 hours	10 minutes	
6	1 day	10 minutes	

Number of access logs displayed

A maximum of 5,000 access logs can be displayed in the **Access log** area. If the number of access logs in the logging range indicated by dotted lines exceeds this maximum, an error message is shown and only the maximum number of access logs are displayed, ordered by response time.

Sorting access logs

When the header areas of the display items in the **Log data** tab are clicked, the access logs are sorted by the header column that was clicked. The header area is divided into two parts, and the sorting behavior depends on which part is clicked.



No.	Sorting category	Sorting behavior
1	Sorting	Access logs are sorted in ascending order on the column header that is clicked. **If the same column header is clicked** The display does not change. **If a different column header is clicked** All existing sorting settings are cleared and then the access logs are re-sorted in ascending order based on the new column header that was clicked.
2	Reverse sorting and multi-column sorting	Access logs are sorted in ascending order on the column header that was clicked. Clicking this part of the header enables reverse sorting and multi-column sorting. **If the same column header is clicked** It is sorted in reverse order. **If a different column header is clicked** A new sorting setting for the column header that was clicked is added next to the previous sorting settings, and the access logs are sorted.

(3) Supplemental notes

- To record access logs, you must set the folder where the logs are to be recorded as a property in ITSLM - UR's system definition file (`jp1itslmur.properties`).

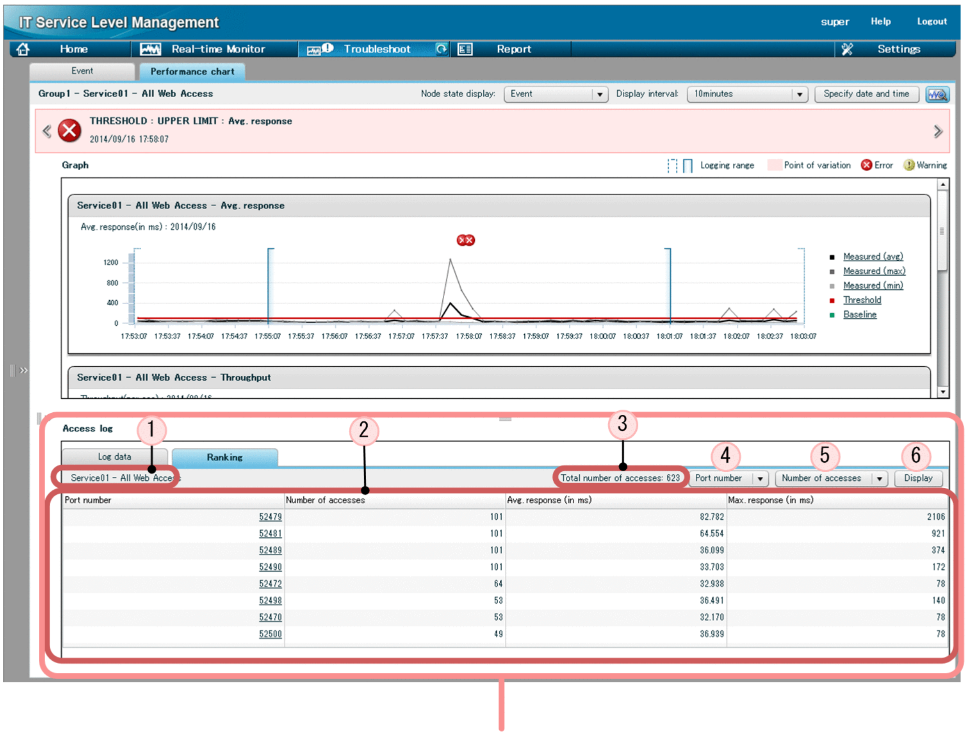
  For details, see *5.6 Editing the system definition files to change settings*.
- The following actions re-initialize the **Access log** area so that no access logs are displayed:
  - Displaying a different service or transaction in the **Services** area
  - Displaying the Troubleshoot window by clicking the **Details** column in the **Event** tab

- Displaying the Troubleshoot window by clicking the **Troubleshoot** button in the Real-time Monitor window

- The access logs are retained for a period of 194 hours (8 days x 24 hours + 2 hours in output). Access logs that exceed this maximum display period are deleted.

10.4.6 Access log area (Ranking tab selected)

(1) Window configuration



THRESHOLD : UPPER LIMIT : Avg. response
2014/09/16 17:58:07

Service01 - All Web Acce

Total number of accesses: 623

Port number	Number of accesses	Avg. response (in ms)	Max. response (in ms)
52479	101	82.782	2106
52481	101	64.554	921
52489	101	36.099	374
52490	101	33.703	172
52472	64	32.938	78
52498	53	36.491	140
52470	53	32.170	78
52500	49	36.939	78

Access log area

(2) Window description

This window displays a ranked list of access logs from the **Log data** tab, in which access logs that match the display items are ranked according to their average response or number of accesses.

No.	Item	Description
1	*X* - **All Web Access**	This area displays the name of the service group whose performance charts are to be viewed. *X* is the name of the service group.
2	Ranking list	This area displays a tabular list of items that are ranked according to the selected display item and type. The first column from the left shows the value of the selected display item.
3	**Total number of accesses**	This area shows the total number of accesses being displayed.
4	Display item drop-down list	The display items that can be used as targets for ranking are displayed in a drop-down list. The following display items can be used as targets for ranking: • **Path** • **IP address** • **Port number**

No.	Item	Description
4	Display item drop-down list	• **Status code**
5	**Type** drop-down list	Ranking categories are displayed in a drop-down list. The following ranking categories can be selected: • **Avg. response** • **Number of accesses**
6	**Display** button	Click this button to display a list of items ranked according to the selected display item and type.

Drilling down in the ranking

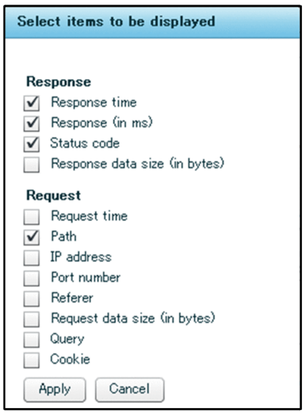
The access logs displayed in the **Log data** tab are filtered by the values of the display items that were clicked in the **Ranking** tab.

These filter conditions are stored in a drilldown history that can be browsed in the **Confirmation of the display of the access log** window.

The filter conditions specified in the **Ranking** tab are cleared when either the **Display** button or the **Display Settings** button in the **Log data** tab is clicked.

10.4.7 Select items to be displayed window

(1) Window configuration



Select items to be displayed

Response

☑ Response time

☑ Response (in ms)

☑ Status code

□ Response data size (in bytes)

Request

□ Request time

☑ Path

□ IP address

□ Port number

□ Referer

□ Request data size (in bytes)

□ Query

□ Cookie

(2) Window description

This window is used to select items to be displayed in the **Log data** tab in the **Access log** area.

No.	Item to display	Details about the item to display
1	**Response**	This area is used to set the response data display items in the **Log data** tab in the **Access log** area. The items that can be set are as follows. • **Response time** • **Response (in ms)** • **Status code** • **Response data size (in bytes)** To set an item for display, select its check box. If an item's check box is not selected, it will not be displayed.
2	**Request**	This area is used to set the request data display items in the **Log data** tab in the **Access log** area.

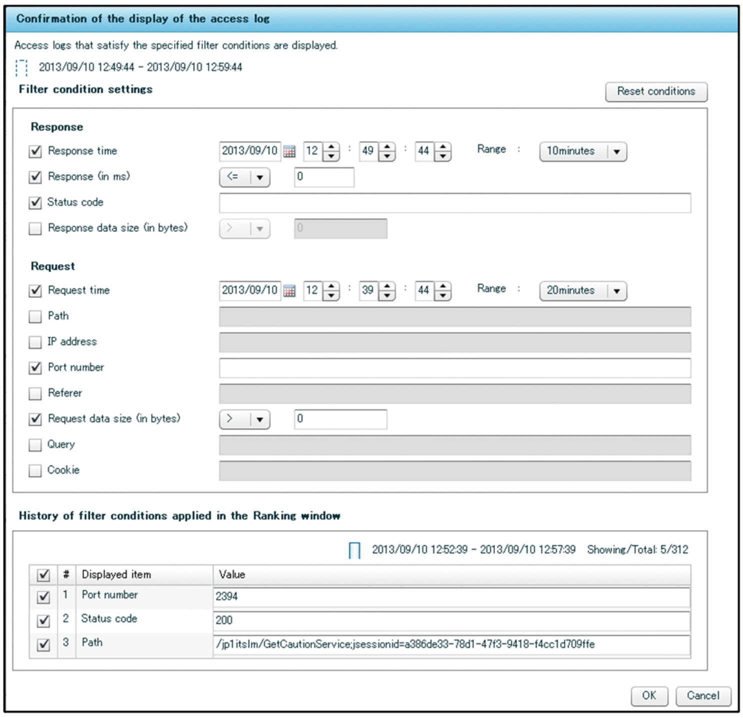
No.	Item to display	Details about the item to display
2	**Request**	The items that can be set are as follows. • **Request time** • **Path** • **IP address** • **Port number** • **Referer** • **Request data size (in bytes)** • **Query** • **Cookie** To set an item for display, select its check box. If an item's check box is not selected, it will not be displayed.
3	**Apply** button	Click this button to apply these settings to the display items in the **Log data** tab in the **Access log** area. When you click the **Apply** button the view returns to the **Log data** tab in the **Access log** area.
4	**Cancel** button	Click this button to return to the **Log data** tab in the **Access log** area without saving the settings.

(3) Supplemental notes

- At least one display item must be selected.

10.4.8 Confirmation of the display of the access log window

(1) Window configuration



Confirmation of the display of the access log

Access logs that satisfy the specified filter conditions are displayed.

2013/09/10 12:49:44 - 2013/09/10 12:59:44

Filter condition settings

Response

☑ Response time 2013/09/10 12 : 49 : 44 Range : 10minutes

☑ Response (in ms) <= 0

☑ Status code

□ Response data size (in bytes) > 0

Request

☑ Request time 2013/09/10 12 : 39 : 44 Range : 20minutes

□ Path

□ IP address

☑ Port number

□ Referer

☑ Request data size (in bytes) > 0

□ Query

□ Cookie

History of filter conditions applied in the Ranking window

2013/09/10 12:52:39 - 2013/09/10 12:57:39 Showing/Total: 5/312

☑	#	Displayed item	Value
☑	1	Port number	2394
☑	2	Status code	200
☑	3	Path	/jp1itslm/GetCautionService;jsessionid=a386de33-78d1-47f3-9418-f4cc1d709ffe

(2) Window description

This window is for setting the filter conditions for the **Log data** tab. It is used to both view the drilldown history specified in the **Ranking** tab and to set the filter conditions for the **Log data** tab.

No.	Setting item	Conditions that can be set
1	**Reset conditions** button	Click this button to return the filter condition settings to their initial state (when the **Confirmation of the display of the access log** window was displayed).
2	**Filter condition settings**	This area is used to select the conditions to be use to filter the access logs, and to set the values for the conditions. For details, see *Details about filter condition settings*.
3	**History of filter conditions applied in the Ranking window**	This area is used to display the history of filter conditions applied in the Ranking window, and to set them as filter conditions on access logs. For details, see *Details about the history of filter conditions applied in the Ranking window*.
4	**OK** button	Click this button to filter the access logs displayed in the **Log data** tab in the **Access log** area by the specified filter conditions. When you click the **OK** button it returns the view to the **Log data** tab in the **Access log** area.
5	**Cancel** button	Click this button to return to the **Log data** tab in the **Access log** area without saving the settings.

Details about filter condition settings

Each item whose check box is selected under **Filter condition settings** is set as a filter condition on the access logs displayed in the **Log data** tab of the **Access log** area. The unselected items are not set as filter conditions. The values that can be specified for filter conditions are indicated in the following table:

No.	Setting item	Conditions that can be set
1	**Response time**	Specify a response time range. The permissible values fall within the range of the dotted lines (the display range of the access logs).
2	**Response (in ms)**	Specify an operator and a response time (in milliseconds). The permissible values are shown below. **Operators that can be selected** >: Greater than the specified value >=: Greater than or equal to the specified value ==: Equal to the specified value <=: Less than or equal to the specified value <: Less than the specified value !=: Not equal to the specified value **Permissible values** `0` to `600000`
3	**Status code**	This item displays the access logs that match the specified regular expression. The permissible values are shown below. **Number of characters that can be entered** 0 to 40 characters **Input restrictions** • It must conform to Java regular expressions. The regular expression syntax is described in the API specification of the `java.util.regex.Pattern` class in Java Platform Standard Edition 6. • Non-ASCII characters cannot be used. • Double-byte characters cannot be used. • URL encoded characters in UTF-8 can be used. If this field is left blank, all status codes are displayed.

No.	Setting item	Conditions that can be set
4	**Response data size (in bytes)**	Specify an operator and a response data size (in bytes). The permissible values are shown below. **Operators that can be selected** See item number 2 for details. **Permissible values** `0` to `2147483647`
5	**Request time**	Specify a request time range. Permissible values range from the start time of the dotted lines (the display range of the access logs) minus ten minutes.
6	**Path**	This item displays the access logs that match the specified regular expression. The permissible values are shown below. **Number of characters that can be entered** 0 to 255 characters **Input restrictions** See item number 3 for details. If this field is left blank, all paths are displayed.
7	**IP address**	Specify a regular expression for IP addresses. The permissible values are shown below. **Number of characters that can be entered** 0 to 40 characters **Input restrictions** See item number 3 for details. If this field is left blank, all IP addresses will be displayed.
8	**Port number**	This item displays the access logs that match the specified regular expression. The permissible values are shown below. **Number of characters that can be entered** 0 to 40 characters **Input restrictions** See item number 3 for details. If this field is left blank, all port numbers will be displayed.
9	**Referer**	This item displays the access logs that match the specified regular expression. The permissible values are shown below. **Number of characters that can be entered** 0 to 255 characters **Input restrictions** See item number 3 for details. If this field is left blank, all referrers will be selected.
10	**Request data size (in bytes)**	Specify an operator and a request data size (in bytes). The permissible values are shown below. **Operators that can be selected** See item number 2 for details. **Permissible values** `0` to `2147483647`
11	**Query**	Enter a query condition. Click the text box to bring up the Edit query window, where a key and the corresponding value can be entered. If you define multiple query conditions in the Edit query window, they will be displayed in no particular order, separated by spaces. For details about the Edit query window, see *10.6.10 Edit query window*.

No.	Setting item	Conditions that can be set
12	**Cookie**	Enter a cookie condition. Click the text box to bring up the Edit cookie window, where a key and the corresponding value can be entered. If you define multiple cookie conditions in the Edit cookie window, they will be displayed in no particular order, separated by spaces. For details on the Edit cookie window, see *10.6.9 Edit cookie window*.

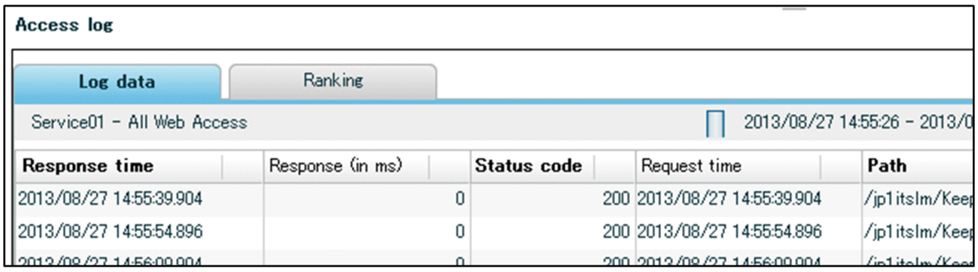
Details about the history of filter conditions applied in the Ranking window

This area of the window displays the drilldown history specified in the **Ranking** tab in the **Access log** area. If there is no drilldown history, then nothing is displayed.

No.	Displayed item	Data that is displayed
1	Total number of accesses	This area displays the number of access logs. **Showing** (*nnnn*) The number of access logs that are displayed in the **Log data** tab **Total** (*mmmm*) The number of access logs in the range displayed between the solid lines in the **Performance chart** tab Display format *nnnn* / *mmmm*
2	Check boxes	When a drilldown history checkbox is selected, that item is set as a filter condition on the access logs displayed in the **Log data** tab in the **Access log** area. Similarly, if the checkbox is not selected, then the filter condition is not set.
3	#	The number in the drilldown history.
4	**Displayed item**	The item to be used as a filter condition.
5	**Value**	The value to use in the filter condition.

(3) Supplemental notes

- As shown below, the display items that are specified by filter conditions in the **Confirmation of the display of the access log** window are shown in bold in the **Log data** tab in the **Access log** area. Similarly, in the **Ranking** tab, if filter conditions are specified, those headers are shown in bold.



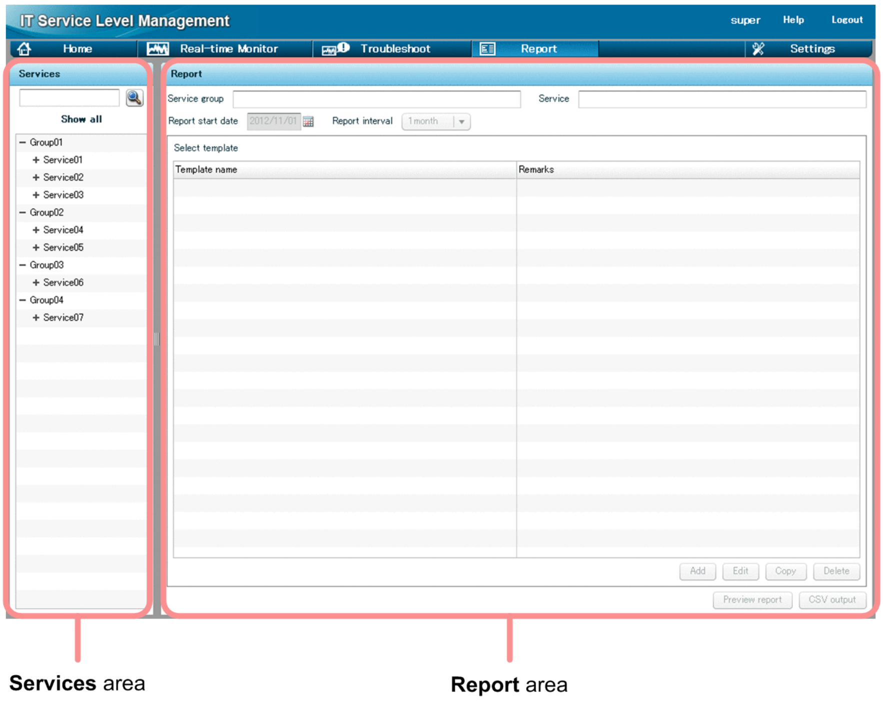
Service01 - All Web Access   2013/08/27 14:55:26 - 2013/0

Response time	Response (in ms)	**Status code**	Request time	**Path**
2013/08/27 14:55:39.904	0	200	2013/08/27 14:55:39.904	/jp1itslm/Keep
2013/08/27 14:55:54.896	0	200	2013/08/27 14:55:54.896	/jp1itslm/Keep
2013/08/27 14:56:00.004	0	200	2013/08/27 14:56:00.004	/jp1itslm/Keep

- Filter conditions can also be set for items that are not shown in the **Log data** tab in the **Access log** area (items not selected in the Select items to be displayed window).
- Once the filter conditions are set by clicking the **OK** button in the drilldown history table, the items in the drilldown history whose check box were not selected will be deleted.

10.5.1 Configuration of the Report window

(1) Window configuration



Report start date 2012/11/01

Report interval 1month

(2) Window description

The Report window is used to create reports for periodic reporting of monitoring results. Information can be displayed on the screen and output to a CSV file.

The Report window is composed of the following areas:

- **Services** area
- **Report** area

(3) Supplemental notes

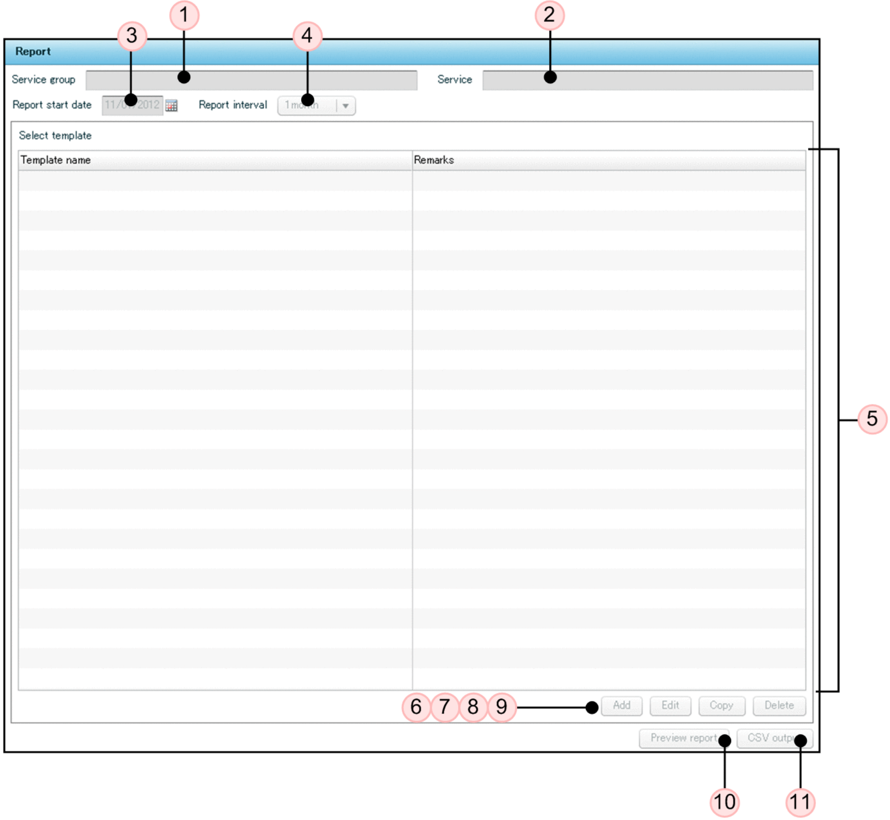
- If a monitored target of a monitored service being displayed in the Report window has been deleted by another service group administrator, at attempt to output the report data will result in an empty CSV file.
- If an error occurs during downloading of report output, delete the CSV output file manually due to the possibility of incomplete data.

10.5.2 Services area

This area is common to all the ITSLM windows. For details about the **Services** area window, see *10.1.2(3) Services area*.

10.5.3 Report area

(1) Window configuration



(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This box displays the name of the selected service group.
2	**Service**	This box displays the name of the selected monitored service.
3	**Report start date**	Use this box to specify the start date for the report. A specific date must be set for the report start date. The default is the first day of the current month, as determined from the system date.
4	**Report interval** pull-down menu	Use this pull-down menu to select the interval (timeframe) to be covered by the report. The following values can be selected (the default is **1 month**): • **1 day** • **1 week** • **1 month** • **3 months**
5	**Select template**	When you have selected a monitored service or monitored target, this area displays a list of templates that have been registered. You can select a template from the list if there is one available that you want to edit, copy, or delete, or one whose report you want to review and output to a CSV file.
6	**Add** button	Click this button to create a new template. Clicking the **Add** button opens the Add template window where you can create a template.

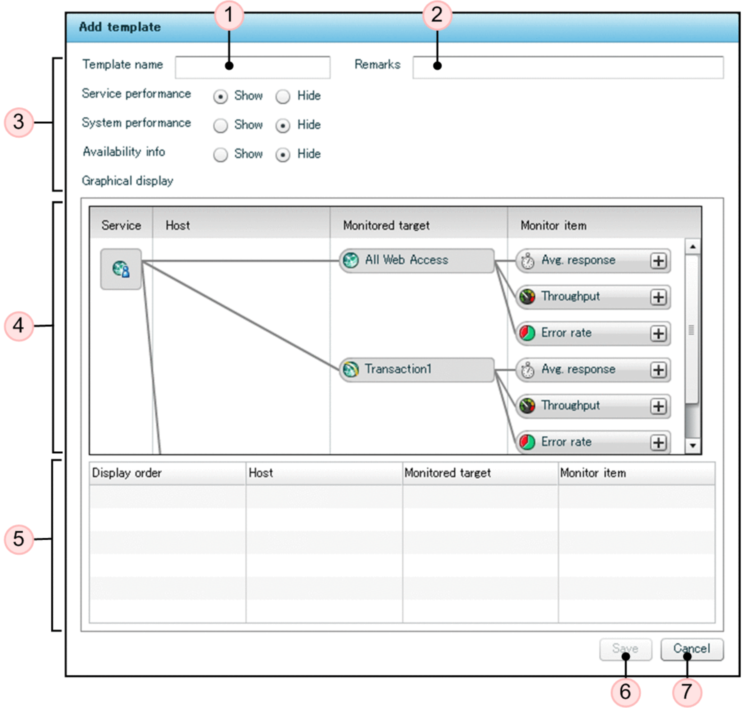
No.	Item	Description
7	**Edit** button	Click this button to edit an existing template. First, select a template for editing, then click the **Edit** button to open the Edit template window where you can edit the selected template.
8	**Copy** button	Click this button to copy the settings from an existing template to create a new template. First, select a template for copying, then click the **Copy** button to open the Copy template window where a template whose settings have been copied from the existing template will be displayed.
9	**Delete** button	Click this button to deleted the selected existing template. Note that you cannot delete the Default template.
10	**Preview report** button	Click this button to preview the information that has been output by the selected template by displaying it on the screen. Clicking the **Preview report** button opens the Preview report window.
11	**CSV output** button	Click this button to output a report in CSV format using the settings of the selected template.

(3) Supplemental notes

- Templates can be registered for each monitored service. A maximum of 32 templates can be registered for one monitored service.
- Nonexistent dates in the report interval are not aggregated into report tables, performance charts, or CSV files. For example, if the report start date is May 31, and the report interval is set to 1 month, the period from May 31 to June 30 is included in the report interval, but June 31 is not included. Or, in the case of a comparison to previous data, the period from May 1 to May 30 is counted as falling within the report interval, but April 31 is excluded.
- Because the retention period for ITSLM report data is five years, you cannot specify a report start date that is earlier than the same date five years previous, based on the system time on the host on which you are displaying the ITSLM windows.

10.5.4 Add template window

(1) Window configuration


Add template

Template name

Remarks

Service performance ● Show ○ Hide

System performance ○ Show ● Hide

Availability info ○ Show ● Hide

Graphical display

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Template name**	Enter in this box a name for the template that is to be created. A maximum of 64 characters can be entered. Do not enter any platform-dependent characters. This area is blank when you create a new template.
2	**Remarks**	Enter in this area a remark for the template you are creating. A maximum of 64 characters can be entered. This area is blank when you create a new template.
3	Display settings for performance and availability information	Use this area to select whether the items listed below are to be displayed in the report: • **Service performance** • **System performance** • **Availability info** For each item you wish to display, select its **Show** radio button; for each item you do not want to display, select its **Hide** radio button. The defaults for the radio buttons depend on the value set for the `dashboardPrioritizeSystem` property in ITSLM - Manager's system definition file (`jp1itslm.properties`): • `true` Service performance: **Hide** System performance: **Show** Availability information: **Hide** • `false`

No.	Item	Description
3	Display settings for performance and availability information	Service performance: **Show** System performance: **Hide** Availability information: **Hide**
4	Selection of monitoring items to graph	Use this area to select the monitoring items you wish to graph. Click ⊞ for each monitoring item you wish to display. This will add that monitoring item to the bottom of the selections list. To remove a monitoring item that is already selected, click ⊟ for that monitoring item and it will be removed from the selections list. A maximum of 50 monitoring items can be selected, but no more than 10 can be graphed in the Preview report window.
5	Selections list	This area displays the list of monitoring items you have selected. You can drag monitoring items up and down to rearrange the order in which they are displayed. When you click a system performance monitoring item, the Monitor item details window is displayed, where you can see that monitoring item's name and key field information. The Preview report window can display graphs for up to 10 selected monitoring items, displayed in the order they are listed in this area (only the first 10 are displayed).
6	**Save** button	Clicking this button saves the template using the settings displayed on the screen. Click the **Save** button to save the template and return to the **Report** area.
7	**Cancel** button	Clicking this button returns to the **Report** area without saving the template settings.

10.5.5 Edit template window

This window displays the same contents as the Add template window, except that **Template name**, **Remarks**, the display settings for performance and availability information, and the selection of monitoring items to graph have all been set to the values in the selected template. For details, see *10.5.4 Add template window*.

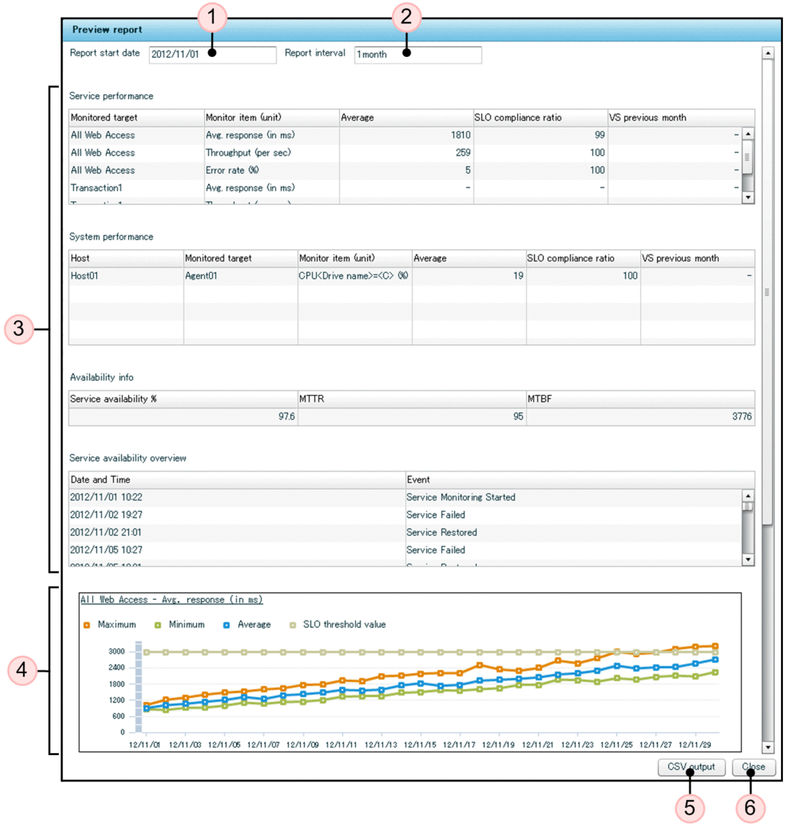
Note that if you are editing the Default template, you cannot change the **Template name** and **Remarks**.

10.5.6 Copy template window

This window displays the same contents as the Add template window, except that the **Template name** and **Remarks** fields are blank, and the display settings for performance and availability information, and the selection of monitoring items to graph, are set to the values in the selected template. For details, see *10.5.4 Add template window*.

10.5.7 Preview report window

(1) Window configuration



Report start date 2012/11/01 Report interval 1month

Service performance

Monitored target	Monitor item (unit)	Average	SLO compliance ratio	VS previous month
All Web Access	Avg. response (in ms)	1810	99	-
All Web Access	Throughput (per sec)	259	100	-
All Web Access	Error rate (%)	5	100	-
Transaction1	Avg. response (in ms)	-	-	-

System performance

Host	Monitored target	Monitor item (unit)	Average	SLO compliance ratio	VS previous month
Host01	Agent01	CPU<Drive name>=<C> (%)	19	100	-

Availability info

Service availability %	MTTR	MTBF
97.6	95	3776

Service availability overview

Date and Time	Event
2012/11/01 10:22	Service Monitoring Started
2012/11/02 19:27	Service Failed
2012/11/02 21:01	Service Restored
2012/11/05 10:27	Service Failed

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Report start date**	This box displays the report start date that was set in the **Report** area.
2	**Report interval**	This box displays the report interval that was set in the **Report** area.
3	Comprehensive evaluations	This area displays aggregated performance information on the monitored services over the interval set in the **Report** area.
4	Performance charts	This area displays performance charts for the monitored services over the interval set in the **Report** area. Performance charts for the monitoring items selected under **Graphical display** in the template are stacked vertically. A maximum of 50 monitoring items can be selected under **Graphical display** in the template, but no more than 10 charts can be displayed.#
5	**CSV output** button	Clicking this button outputs all the performance chart data to a single CSV file. Note that the comprehensive evaluation information is not output to the CSV file. When you click the **CSV output** button, the Preview report window closes and the Report window is displayed.
6	**Close** button	Clicking this button closes the Preview report window without displaying the report and returns to the **Report** area.

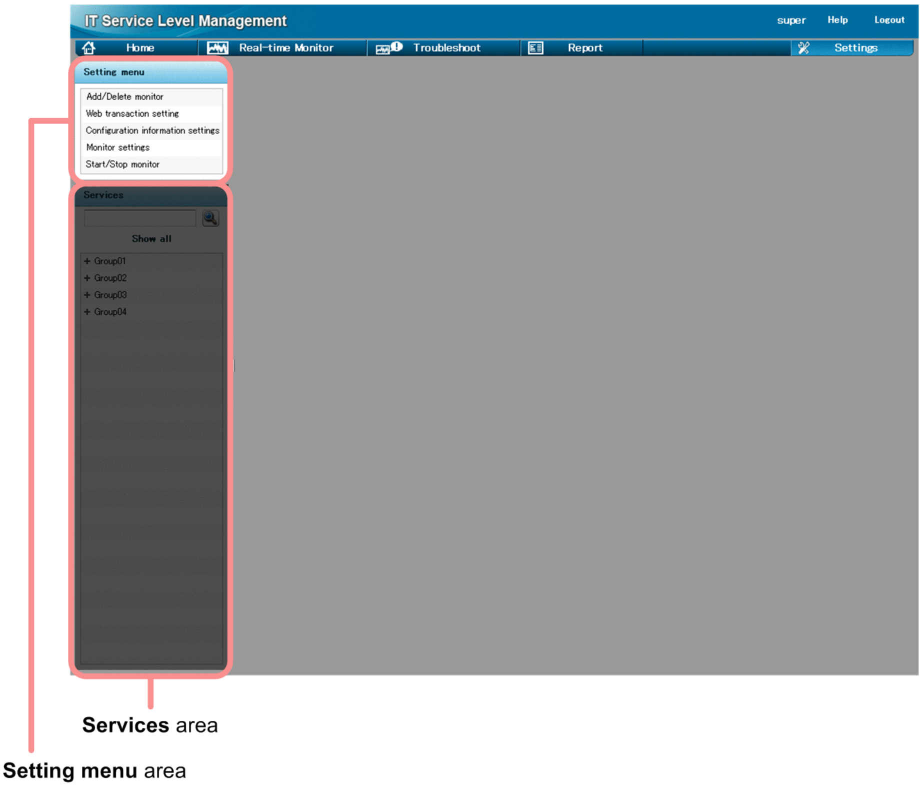
#

Performance charts are displayed for the monitoring items selected in the Edit template window whose display order is 1 through 10. Performance charts for monitoring items whose display order is 11 or higher are not displayed, but they are output to the CSV file.

10.6 Settings window and windows displayed from the Settings window

10.6.1 Configuration of the Settings window

(1) Window configuration



(2) Window description

The Settings window is used to add or delete monitored services, to set monitoring items, and to start and stop monitoring.

The Settings window is composed of the following areas:

- **Setting menu** area
- **Services** area

In addition, depending on the item selected in the **Setting menu** area, one of the following areas will be displayed:

- **Add/Delete monitor** area
- **Web transaction setting** area
- **Configuration information settings** area
- **Monitor settings** area
- **Start/Stop monitor** area

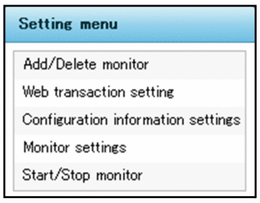
When you select **Add/Delete monitor** or **Start/Stop monitor** in the **Setting menu** area, the **Services** area is grayed out and cannot be used.

10.6.2 Services area

This display is common to all the ITSLM windows. For details about the **Services** area window, see *10.1.2(3) Services area*.

10.6.3 Setting menu area

(1) Window configuration


Setting menu

- Add/Delete monitor
- Web transaction setting
- Configuration information settings
- Monitor settings
- Start/Stop monitor

(2) Window description

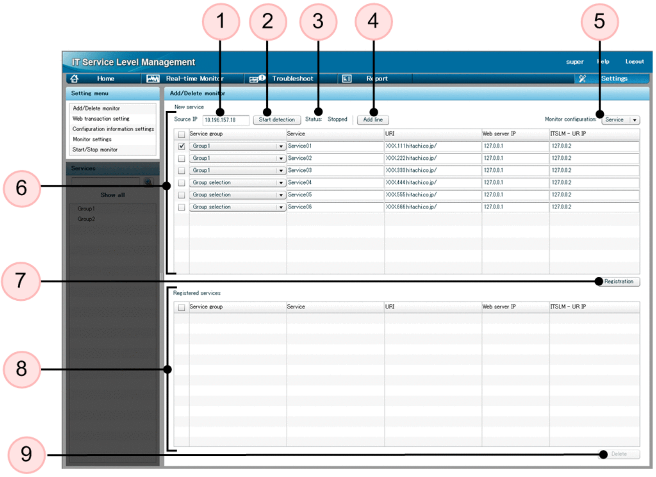
When you select an item, the area of the same name is displayed on the right side of the **Setting menu** area.

The following areas can be displayed from the **Setting menu** area:

- **Add/Delete monitor** area
- **Web transaction setting** area
- **Configuration information settings** area
- **Monitor settings** area
- **Start/Stop monitor** area

10.6.4 Add/Delete monitor area

(1) Window configuration



Source IP 10.196.157.18

Status: Stopped

Monitor configuration: Service

☐	Service group	Service	URI	Web server IP	ITSLM - UR IP
☑	Group1	Service01	XXX.111.hitachi.co.jp/	127.0.0.1	127.0.0.2
☐	Group1	Service02	XXX.222.hitachi.co.jp/	127.0.0.1	127.0.0.2
☐	Group1	Service03	XXX.333.hitachi.co.jp/	127.0.0.1	127.0.0.2
☐	Group selection	Service04	XXX.444.hitachi.co.jp/	127.0.0.1	127.0.0.2
☐	Group selection	Service05	XXX.555.hitachi.co.jp/	127.0.0.1	127.0.0.2
☐	Group selection	Service06	XXX.666.hitachi.co.jp/	127.0.0.1	127.0.0.2

☐	Service group	Service	URI	Web server IP	ITSLM - UR IP

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Source IP**	Specifies the IP address of the source. When you launch URI detection for monitored services, only sources that match this IP address are detected. By default, this area displays the IP address of the machine you are currently working on (the machine on which you launched the browser to access ITSLM). If the system is configured to convert IP addresses through a device such as a router or load balancer, you must change this IP address to the converted IP address. An IP address is entered in the format *XXX*`.`*XXX*`.`*XXX*`.`*XXX* (*XXX*: `0` to `255`).
2	**Start detection** button or **Stop detection** button	• **Start detection** button Clicking this button starts URI detection. This button is displayed while the status is **Stopped** and when the **Add/Delete monitor** area is being displayed. Once you click this button to start detection, it changes into the **Stop detection** button. • **Stop detection** button Clicking this button stops URI detection. This button is displayed while the status is **Detecting**. Once you click it to stop detection, it changes into the **Start detection** button.
3	**Status**	This field indicates whether monitored services are being detected. One of the following is displayed: **Detecting**: Monitored services are being detected. **Stopped**: Monitored services are not being detected.
4	**Add line** button	Clicking this button adds a blank line so that you can enter a URI directly.
5	**Monitor configuration** pull-down menu	When ITSLM is linked to Performance Management, select one of the following monitoring configurations for the service to be registered: • **Service** • **System** This field is displayed when ITSLM is linked to Performance Management. The default depends on the value set for the `dashboardPrioritizeSystem` property in ITSLM - Manager's system definition file (`jp1itslm.properties`): `true`: **System** is the default. `false`: **Service** is the default.
6	**New service**	This area displays the monitored services for which a URI has been detected. Select a service group and enter the name of a monitored service. • Check boxes Select the check boxes for the monitored services that are to be registered. If you select the check box in the header, the check boxes in all rows become selected. Similarly, if you clear the check box in the header, the check boxes in all the rows are cleared. • **Service group** Select the service group to which each monitored service belongs. The pull-down menu contains the names of the service groups that the logged-in user is responsible for monitoring (the resource group names registered in JP1/Base). • **Service** Enter a name for each monitored service. A monitored service's URI is displayed by default. You can enter between 1 and 64 characters. Do not use `"`, `,`, `'`, \, space, tab, platform-dependent characters, or control characters. We recommend that you not begin the name with a hyphen (`-`) so that it is not confused with a command option. • **URI**# This column displays each monitored service's URI.

No.	Item	Description
6	**New service**	You can enter between 1 and 255 characters. You cannot enter space, ", #, <, >, ?, [, \,], ^, `, {, |, }, or non-ASCII characters. The notation must conform to RFC 3986. Enter a URI to which the user has full access. An entry can be made in this field when ITSLM is linked to Performance Management and **Service** is selected in **Monitor configuration**. • **Web server IP** This column displays the IP address of the Web server that is executing each monitored service. An entry can be made in this field when ITSLM is linked to Performance Management and **Service** is selected in **Monitor configuration**. • **ITSLM - UR IP** This column displays the IP address of the ITSLM - UR that is performing detection of each monitored service. An entry can be made in this field when ITSLM is linked to Performance Management and **Service** is selected in **Monitor configuration**. IP addresses are entered using the format *XXX*.*XXX*.*XXX*.*XXX* (*XXX*: 0 to 255).
7	**Registration** button	Clicking this button registers the monitored services whose check boxes are selected in the new services area. Monitored services that have been successfully registered are displayed under **Registered services**.
8	**Registered services**	This area displays a list of the monitored services that have been registered. • Check boxes Select monitored services to be deleted. If you select the check box in the header, the check boxes in all rows become selected. Similarly, if you clear the check box in the header, the check boxes in all rows are cleared. A check box that has been selected is cleared if you click the **Start detection** button, **Stop detection** button, or **Registration** button. • **Service group** This column displays the name of the service group to which each monitored service belongs. • **Service** This column displays the name of each monitored service. • **URI** This column displays the URI of each monitored service. The URI is displayed when ITSLM is linked to Performance Management and the monitoring configuration for the monitored service is **Service**. If the monitoring configuration for the monitored service is **System**, - is displayed. • **Web server IP** This column displays the IP address of the Web server that is executing each monitored service. The IP address of the Web server is displayed when ITSLM is linked to Performance Management and the monitoring configuration for the monitored service is **Service**. If the monitoring configuration for the monitored service is **System**, - is displayed. • **ITSLM - UR IP** This column displays the IP address of the ITSLM - UR that is performing the detection of each monitored service. The IP address of the ITSLM - UR is displayed when ITSLM is linked to Performance Management and the monitoring configuration for the monitored service is **System**. If the monitoring configuration for the monitored service is **System**, - is displayed.
9	**Delete** button	Clicking this button deletes the monitored services whose check boxes have been selected in the **Registered services** area.

#: Make sure that each URI ends with a slash (/). However, if a URI does not end with a slash immediately after it was detected and you do not edit it, you can still register it as a monitored service if all the URI paths are monitored targets. A URI is specified in the following format:

authority path

- *authority*

  This part must be a host name or a port number. A host name must consist of 1 to 255 characters. If it exceeds 255 characters, only the first 255 characters are used. A port number must be an integer between `0` and `65535`. If no port number is specified, all ports are targeted.

- *path*

  A path must consist of 1 to 255 characters. If it exceeds 255 characters, only the first 255 characters are used. URL-encoded characters in UTF-8 can be used.

(3) Supplemental notes

Detecting a monitored service

- If you click the **Start detection** button after monitoring of monitored services has started, an error message is displayed and detection of monitored services is not initiated.
- Once you click the **Start detection** button, all areas outside the **Add/Delete monitor** area cannot be used until after you click the **Stop detection** button.
- Once you click the **Start detection** button, you cannot click the **Registration** or **Delete** button until after you click the **Stop detection** button.
- In the event of a failure or termination in some part of ITSLM - UR processing after you start detection of services by clicking the **Start detection** button, detection of services by ITSLM - UR will nevertheless continue if possible. However, if ITSLM - UR is unavailable, detection will fail and remain in **Stopped** status. Similarly, when you stop detection of services by clicking the **Stop detection** button, a failure somewhere in ITSLM - UR will result in an error message but stop processing will continue.
- If you exit the browser or log out by pressing the **F5** key on the keyboard while **Status** shows **Detecting**, detection will stop after a two-minute timeout. Even if you log in again during this two minutes, it will not be possible to detect monitored services until the timeout is completed.

Registering a monitored service

- Multiple service names can be registered under the same URI. Even though they share the same URI, the services will be treated as separate services.
- All monitored services in the same service group must have unique service names. An error message will be displayed if you try to register under a service group a monitored service that has a name that has already been used in that service group. Monitored services with the same service name can be registered under different service groups.
- If you register multiple monitored services at the same time, the registration process proceeds in order from the top of the list. If registration of a monitored service fails during registration processing of the list, the monitored service before the one that fails will be registered, but registration stops with the failed monitored service and the subsequent monitored services are not registered.
- If you attempt to register a monitored service that has been deleted from another browser, an error message will be displayed.
- If multiple users are logged into ITSLM - Manager, and a service group administrator registers a monitored target, the timing for reflecting the change on the other users' screens is described in *3.2.9(1) Timing of updating the number of registered monitored targets*.
- If the IP address of a monitored service's Web server changes (such as after a server migration, for example), it will need to be re-registered as a new service.

Deleting a monitored service

- If you attempt to delete a monitored service that has been deleted from another browser, an error message will be displayed.

- If multiple users are logged into ITSLM - Manager, and a service group administrator deletes a monitored target, the timing for reflecting the change on the other users' screens is described in *3.2.9(1) Timing of updating the number of registered monitored targets*.
- If you attempt to delete a Web transaction belonging to a deleted monitored service, an error message will be displayed.
- If you attempt to delete a monitored service whose monitoring has not stopped, an error message will be displayed.
- If you delete multiple monitored services at the same time, the deletion process proceeds in order starting from the top of the list. If deletion of a monitored service fails during processing of the list, the monitored service before the one that fails will be deleted, but deletion stops with the failed monitored service and the subsequent monitored services are not deleted.
- When you delete a monitored service, some of its data will remain in the ITSLM - Manager database. Especially after you have deleted a number of monitored services, we recommend that you execute the database cleanup command to delete data that is no longer needed so that unwanted data does not accumulate in the database.

  For details about the cleanup command, see *jslmmgrdbcleanup (cleans up database)* in *9. Commands*.
- When you delete a monitored service, its access logs are not deleted.

URIs supported by ITSLM

- The URIs supported by ITSLM depend on the version of ITSLM. The ITSLM version-specific URI formats shown in the table below are based on the following URI notation:
  - *scheme*://*authority path* <?*query*><#*fragment*>

  The following table shows the supported formats.

  Table 10–4: Supported URI formats depending on the ITSLM version

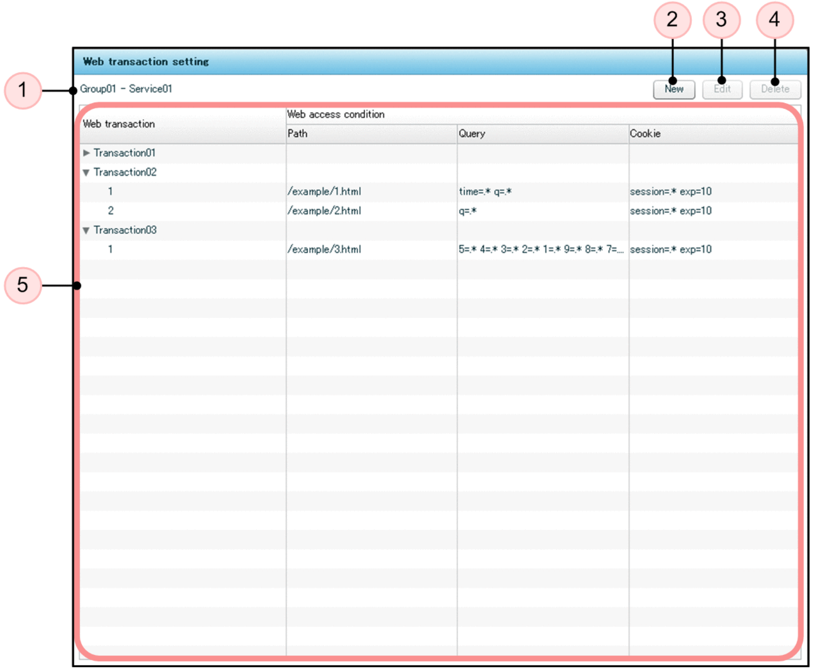
No.	URI element	Supported formats	
		09-50	09-51 and later
1	*scheme*	Only `http` is supported. `https` is not supported.	
2	*authority*	Only host names are supported. If a port number is specified, an error message will be displayed when monitoring of the monitored service begins. A host name must consist of 1 to 255 characters. If it exceeds 255 characters, only the first 255 characters are used.	Host names and port numbers are both supported. A host name must consist of 1 to 255 characters. If it exceeds 255 characters, only the first 255 characters are used. A port number must be an integer between `0` and `65535`.
3	*path*	Not supported	The path format is supported. A path must consist of 1 to 255 characters. If it exceeds 255 characters, only the first 255 characters are used. URL-encoded characters in UTF-8 can be used.
4	*query*	Not supported	The query format is supported. URL-encoded characters in UTF-8 can be used.
5	*fragment*	Not supported	

  Only an entry in the applicable supported format is considered a URI. If an unsupported format is specified, the entry will be ignored.

  If your system configuration has ITSLM - Manager or ITSLM - UR in a mixture of version 09-50 and version 09-51 or later, only version 09-50 URIs are supported.
- You cannot register a URI that specifies a loopback address, or a URI where `localhost` is specified as the host name. Service detection will run, but upon detection the URI will not be displayed as a new service in the **Add/ Delete monitor** area.

10.6.5 Web transaction setting area

(1) Window configuration



Web transaction setting

Group01 - Service01

Web transaction	Web access condition		
	Path	Query	Cookie
▶ Transaction01			
▼ Transaction02			
1	/example/1.html	time=.* q=.*	session=.* exp=10
2	/example/2.html	q=.*	session=.* exp=10
▼ Transaction03			
1	/example/3.html	5=.* 4=.* 3=.* 2=.* 1=.* 9=.* 8=.* 7=...	session=.* exp=10

(2) Window description

The **Web transaction setting** area is used for such activities as editing, deleting, and adding Web transactions, as well as for viewing a list of Web transactions for a monitored service selected in the **Services** area.

The following table lists the items that are displayed:

No.	Item	Description
1	Name of service group and monitored service	This area displays the name of the monitored service selected in the **Services** area and the name of its service group. The following format is used: *service-group-name* − *monitored-service-name*
2	**New** button	Clicking this button opens the Register Web transaction window that you use to register a new Web transaction. The button is deactivated once 10 Web transactions have been registered for a monitored service, or when the total number of instances of All Web Access and Web transactions combined registered into the ITSLM - Manager reaches 50.
3	**Edit** button	Clicking this button opens the Edit Web transaction window that you use to edit a registered Web transaction that has been selected. This button is activated when you select a Web transaction in the **Web transaction** and **Web access condition** area.
4	**Delete** button	Clicking this button deletes a registered Web transaction that has been selected.
5	**Web transaction** and **Web access condition**	This area displays the registered Web transactions. When you click ▶ to the left of a Web transaction name, it changes to ▼ and the Web access conditions of the selected Web transaction are displayed under **Web access condition**. If there are multiple Web access conditions for the selected Web transaction, they are displayed on separate lines. You can drag the name of a Web transaction up and down to rearrange the order in which it is displayed. If you drag a Web transaction name into the header line, the Web transaction is moved to the bottom of the list.

No.	Item	Description
5	**Web transaction** and **Web access condition**	The following items are displayed under **Web access condition**: • **Path** This column displays the path condition of each Web access condition. • **Query** This column displays the query conditions of each Web access condition. If there are multiple query conditions for a Web access condition, they are displayed in no particular order and delimited by a space. • **Cookie** This column displays the cookie conditions of each registered Web transaction. If there are multiple cookie conditions for a Web access condition, they are displayed in no particular order and delimited by a space.

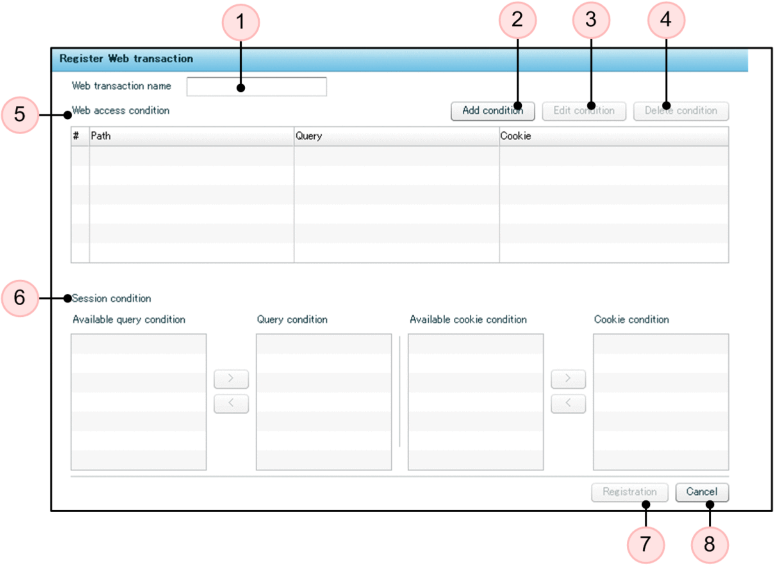
(3) Supplemental notes

- To edit a Web transaction that has been set, select it for editing from the **Web transaction setting** area of the Settings window and then click the **Edit** button. The Edit Web transaction window will be displayed, and will show the settings for the selected Web transaction already filled in. You can edit the Web access conditions, the order of the Web access conditions, and the session conditions.
- If you attempt to delete a Web transaction that has already been deleted from another browser, an error message will be displayed.
- If you attempt to delete a Web transaction that belongs to a monitored service whose monitoring has not stopped, an error message will be displayed.
- When you delete a Web transaction, some of its data will remain in the ITSLM - Manager database. Especially after you have deleted a number of Web transactions, we recommend that you execute the database cleanup command to delete data that is no longer needed so that unwanted data does not accumulate in the database.

  For details about the cleanup command, see *jslmmgrdbcleanup (cleans up database)* in *9. Commands*.
- If multiple users are logged in to ITSLM - Manager, and a service group administrator registers or deletes a monitored target, the timing for reflecting the change on the other users' screens is described in *3.2.9(1) Timing of updating the number of registered monitored targets*.

10.6.6 Register Web transaction window

(1) Window configuration



(2) Window description

The Register Web transaction window is used to specify a name for a Web transaction, adjust the priority of its Web access conditions, and set session conditions. In addition, you can add, edit, and delete Web access conditions.

The following table lists the items that are displayed:

No.	Item	Description
1	**Web transaction name**	Enter in this box a name for a Web transaction that is to be registered. If you are editing a Web transaction that has already been registered, the name of the registered Web transaction is displayed here. A Web transaction name can consist of 1 to 64 characters. You can enter more than 64 characters, but we recommend that you keep within the 64-character limit to avoid errors. Do not use `"`, `,`, `'`, \, space, tab, platform-dependent characters, and control characters.
2	**Add condition** button	Clicking this button displays the Add Web access condition window that you use to add a new Web access condition. However, once there are five Web access conditions, the button is deactivated because the maximum number of conditions has been reached.
3	**Edit condition** button	Clicking this button displays the Edit Web access condition window that you use to edit the Web access condition selected in the **Web access condition** area. The Web access conditions are displayed in the **Define Web access condition** area of the Edit Web access condition window.
4	**Delete condition** button	Clicking this button deletes the Web access condition selected in the **Web access condition** area.
5	**Web access condition**	When you wish to edit a registered Web transaction, this area displays the Web transaction's Web access conditions. In the case of a new registration, nothing is displayed. • **#** This column displays a number indicating the order of each Web access condition. • **Path** This column displays the path condition of each Web access condition. • **Query**

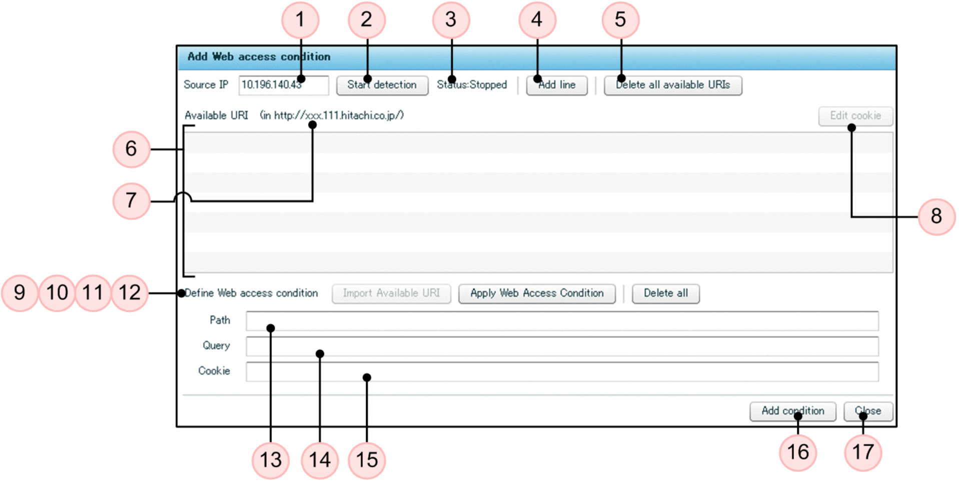
No.	Item	Description
5	**Web access condition**	This column displays the query conditions of each Web access condition. If there are multiple query conditions for the same Web access condition, they are displayed in no particular order delimited by the space. • **Cookie** This column displays the cookie conditions of each registered Web transaction. If there are multiple cookie conditions for the same Web access condition, they are displayed in no particular order delimited by the space.
6	**Session condition**	This area is for setting query conditions and cookie conditions for determining whether a Web access is from the same user. • **Available query condition** This column displays the keys for the common queries from all the Web access conditions displayed in **Web access condition**. • **Query condition** This column displays the query conditions. • **Available cookie condition** This column displays the keys for the common cookies from all the Web access conditions displayed in **Web access condition**. • **Cookie condition** This column displays the cookie conditions. • >
This button moves items selected under **Available query condition** or **Available cookie condition** into **Query condition** or **Cookie condition**. • < This button moves items selected under **Query condition** or **Cookie condition** into **Available query condition** or **Available cookie condition**. A combined maximum of 10 conditions can be set under **Query condition** and **Cookie condition**.
7	**Registration** button	Clicking this button applies the Web transaction settings in the Register Web transaction window to the **Web transaction setting** area and closes the Register Web transaction window. Monitoring of the registered Web transaction will begin the next time you start monitoring a monitored service, including the defined Web transactions.
8	**Cancel** button	Clicking this button closes the Register Web transaction window and returns to the **Web transaction setting** area. The settings in the Register Web transaction window are not applied.

(3) Supplemental notes

- You cannot interact with other windows while working in the Register Web transaction window.

10.6.7 Add Web access condition window

(1) Window configuration



Add Web access condition

Source IP 10.196.140.43

Status:Stopped

Available URI (in http://xxx.111.hitachi.co.jp/)

(2) Window description

The Add Web access condition window is used to set multiple URIs, which can be entered directly or detected from monitored services, while providing for filtering of the Web access conditions to check their validity.

The following table lists the items that are displayed:

No.	Item	Description
1	**Source IP**	Specifies the IP address of the source. When you launch URI detection for monitored services, only sources that match this IP address are detected. By default, this area displays the IP address of the machine you are currently working on (the machine on which you launched the browser to access ITSLM). If the system is configured to convert IP addresses through a device such as a router or load balancer, you must change this IP address to the converted IP address. An IP address is entered in the format *XXX*`.`*XXX*`.`*XXX*`.`*XXX* (*XXX*: `0` to `255`). Values above 255 can be entered, but we recommend that you always enter values within the range of `0` to `255` to avoid errors.
2	**Start detection** button or **Stop detection** button	• **Start detection** button Clicking this button starts URI detection. This button is displayed while the status is **Stopped** and when the Add Web access condition window is being displayed. Once you click this button to start detection, it changes into the **Stop detection** button. From the time you click the **Start detection** button until you click the **Stop detection** button, you cannot interact with other items. • **Stop detection** button Clicking this button stops URI detection. This button is displayed while the status is **Detecting**. Once you click this button to stop detection, it changes into the **Start detection** button.
3	**Status**	This field indicates whether monitored services are being detected. One of the following is displayed: **Detecting**: URIs are being detected. **Stopped**: URIs are not being detected.
4	**Add line** button	Clicking this button adds a line in **Available URI** for direct input of a URI. Initially, the URI shown in **Service monitored target** is displayed on the new line.
5	**Delete all available URIs** button	Clicking this button deletes all the URIs displayed in the **Available URI** area.

No.	Item	Description
5	**Delete all available URIs** button	When you click this button, a confirmation dialog box is displayed. The deletion is performed when you click **OK** in the dialog box.
6	**Available URI**	This area displays the URIs that have been detected or entered directly. Click a displayed URI to edit it. The following restrictions apply to entering a URI: • A URI can consist of 1 to 255 characters. You can enter more than 255 characters, but we recommend that you keep within the 255-character limit to avoid errors. • You cannot enter space, ", <, >, [, \,], ^, `, {, |, }, and non-ASCII characters. • Specify a URI under which there are monitored services. The notation must conform to RFC 3986.
7	Service monitored target	The area displays the URI of the monitored services.
8	**Edit cookie** button	Clicking this button opens the Edit cookie window, which displays the cookies for the URI selected in the **Available URI** area. Cookies for which no key or value has been entered are not displayed.
9	**Define Web access condition**	This area is for entering a Web access condition for a registered Web transaction.
10	**Import Available URI** button	Clicking this button enters automatically in the **Path**, **Query**, and **Cookie** columns below the path, query, and cookie information, respectively, for the URI selected in the **Available URI** area. If there is no path, query, or cookie information in the URI selected in **Available URI**, the corresponding columns are left blank. Also, if nothing has been entered for the key or value of a query or cookie, that information is also not entered in the **Define Web access condition** area. Once the total number of query conditions and cookie conditions combined that have been imported reaches 20, the **Add condition** button is deactivated.
11	**Apply Web Access Condition** button	Clicking this button narrows down the URIs displayed in the **Available URI** area to only those that exactly match the conditions in the **Define Web access condition** area.
12	**Delete all** button	Clicking this button blanks out all the text boxes in the **Define Web access condition** area.
13	**Path**	Use this box to enter a path condition. A path condition specifies the path of a URI to be monitored as a Web transaction. The following restrictions apply to the entry: • It must conform to Java regular expressions. The regular expression syntax is as described in the API specification of the `java.util.regex.Pattern` class in Java Platform Standard Edition 6. • It can consist of 1 to 255 characters. If escape characters are used, each escape character counts as a single character. You can enter more than 255 characters, but we recommend that you keep within the 255-character limit to avoid errors. • No spaces or non-ASCII characters can be entered. • URL-encoded characters in UTF-8 can be used. If you click the **Add condition** button or **Refresh** button with no entry in **Path**, the path condition will be `.*` (all paths apply).
14	**Query**	This box displays query conditions. Clicking this text box opens the Edit query window that you use to specify a key and a value for a query condition. If you define multiple query conditions in the Edit query window, they are displayed here in no particular order delimited by the space.
15	**Cookie**	This box displays cookie conditions. Clicking this text box opens the Edit cookie window that you use to specify a key and a value for a cookie condition. If you define multiple cookie conditions in the Edit cookie window, they are displayed here in no particular order delimited by the space.
16	**Add condition** button or **Refresh** button	• **Add condition** button

No.	Item	Description
16	**Add condition** button or **Refresh** button	Clicking this button adds the Web access conditions entered in the **Define Web access condition** area to the Web access conditions in the Register Web transaction window or Edit Web transaction window. Once they have been added, the text boxes in the **Define Web access condition** area are blanked out. A maximum of five Web access conditions can be defined for one Web transaction. • **Refresh** button Clicking this button applies your edits to the Web access conditions to the Web access conditions in the Register Web transaction window or Edit Web transaction window, then closes the Edit Web access condition window and returns to the Register Web transaction window or Edit Web transaction window.
17	**Close** button	Clicking this button closes the Add Web access condition window and returns to the Register Web transaction window or Edit Web transaction window.

(3) Supplemental notes

- If a failure or termination occurs in some part of ITSLM - UR processing after you started URI detection by clicking the **Start detection** button in the Add Web access condition window, detection of services by ITSLM - UR will nevertheless continue if possible. However, if ITSLM - UR is unavailable, detection will fail and remain in **Stopped** status. Similarly, when you stop detection of services by clicking the **Stop detection** button, a failure in ITSLM - UR will result in an error message but stop processing will continue.
- If you exit your browser or log out by pressing **F5** on the keyboard while **Status** in the Add Web access condition window shows **Detecting**, detection stops after a two-minute timeout. Even if you log in again during this two-minute period, you will not be able to detect monitored services in the **Add/Delete monitor** area of the Settings window, or detect URIs in the Add Web access condition window or Edit Web access condition window, until the timeout completes.
- You cannot interact with other windows while working in the Add Web access condition window.

10.6.8 Edit Web access condition window

(1) Window configuration and Window description

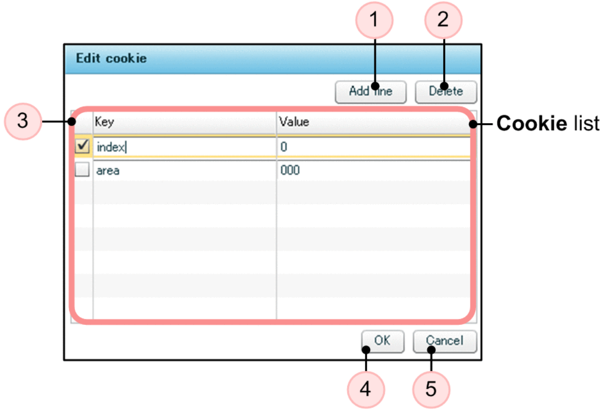
This window exhibits the same information and behavior as the Add Web access condition window, except that the **Add condition** button in the Add Web access condition window appears as the **Refresh** button in this window. For details, see *10.6.7 Add Web access condition window*.

(2) Supplemental notes

- If a failure or termination occurs in some part of ITSLM - UR processing after you started URI detection by clicking the **Start detection** button in the Edit Web access condition window, detection of services by ITSLM - UR will nevertheless continue if possible. However, if ITSLM - UR is unavailable, detection will fail and remain in **Stopped** status. Similarly, when you stop detection of services by clicking the **Stop detection** button, a failure in ITSLM - UR will result in an error message but stop processing will continue.
- If you exit your browser or log out by pressing **F5** on the keyboard while **Status** in the Edit Web access condition window shows **Detecting**, detection stops after a two-minute timeout. Even if you log in again during this two-minute period, you will not be able to detect monitored services in the **Add/Delete monitor** area of the Settings window, or detect URIs in the Add Web access condition window or Edit Web access condition window, until the timeout completes.
- You cannot interact with other windows while working in the Edit Web access condition window.

10.6.9 Edit cookie window

(1) Window configuration



(2) Window description

The Edit cookie window is used to enter and edit cookie conditions for the following windows:

- Add Web access condition window
- Edit Web access condition window
- **Confirmation of the display of the access log** window

The Edit cookie window is also used to review and edit cookies for the URIs in the **Available URI** area of the following windows:

- Add Web access condition window
- Edit Web access condition window

The following table lists the items that are displayed:

No.	Item	Description
1	**Add line** button	Clicking this button adds a blank line to the cookie list.
2	**Delete** button	Clicking this button deletes all the cookies in the cookie list whose check box has been selected.
3	**Cookie** list	This area displays a list of cookies. • Check box To delete a cookie, select its checkbox. • **Key** This column displays each cookie's key. You can click the text box to edit the key. • **Value** This column displays the value for the key on the same row. You can click the text box to edit it. The following restrictions apply to entry of a key and a value: • The entry must conform to Java regular expressions. The regular expression syntax is as described in the API specification of the `java.util.regex.Pattern` class in Java Platform Standard Edition 6.

No.	Item	Description
3	**Cookie** list	• The key and value combined can consist of 1 to 255 characters. You can enter more than 255 characters, but we recommend that you keep within the 255-character limit to avoid errors. • For the key, you cannot use space, =, or non-ASCII characters. • Each key must be unique (regular expressions are treated as character strings). • For the value, you cannot use spaces or non-ASCII characters. • URL-encoded characters in UTF-8 can be used. If you click the **OK** button with nothing entered for **Value**, **Value** will be set to `.*` (all values apply).
4	**OK** button	Clicking this button applies the edits to the cookies to the Add Web access condition window or Edit Web access condition window.
5	**Cancel** button	Clicking this button closes the Edit cookie window without applying the edits to the cookies, and returns to the Add Web access condition window or Edit Web access condition window.

(3) Supplemental notes

- You cannot interact with other windows while working in the Edit cookie window.

10.6.10 Edit query window

(1) Window configuration and Window description

This window displays the same contents as the Edit cookie window, except that *query* is substituted for *cookie*. For details, see *10.6.9 Edit cookie window*.

(2) Supplemental notes

- You cannot interact with other windows while working in the Edit query window.

10.6.11 Edit Web transaction window

(1) Window configuration and Window description

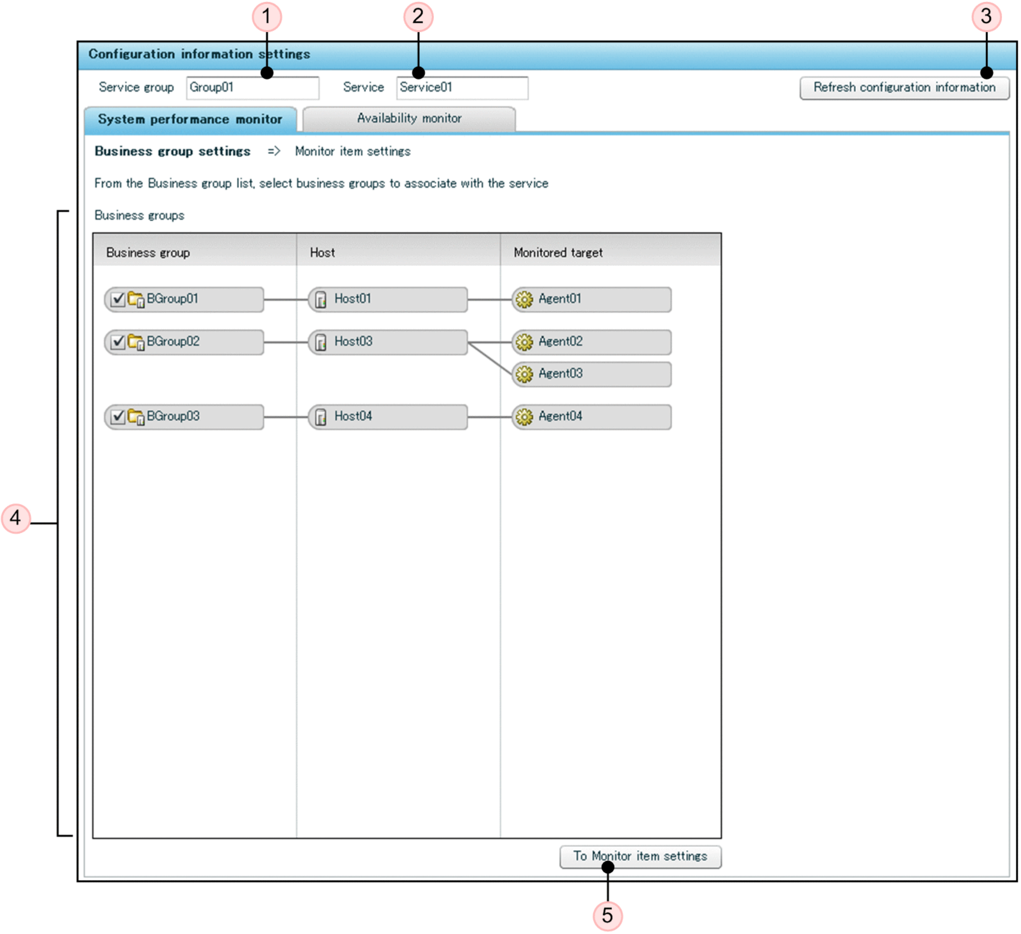
This window exhibits the same information and behavior as the Register Web transaction window, except that the **Registration** button in the Register Web transaction window appears as the **Refresh** button in this window. For details, see *10.6.6 Register Web transaction window*.

(2) Supplemental notes

- You cannot interact with other windows while working in the Edit Web transaction window.

10.6.12 Configuration information settings area (Business group settings with the System performance monitor tab selected)

(1) Window configuration



Configuration information settings

Service group: Group01

Service: Service01

Business group settings => Monitor item settings

From the Business group list, select business groups to associate with the service

Business groups

Business group	Host	Monitored target
☑ BGroup01	Host01	Agent01
☑ BGroup02	Host03	Agent02
		Agent03
☑ BGroup03	Host04	Agent04

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This box displays the name of the service group selected in the **Services** area.
2	**Service**	This box displays the name of the monitored service selected in the **Services** area.
3	**Refresh configuration information** button	Clicking this button displays the Confirmation of refreshing configuration information window that you use to review the most recent (refreshed) contents of the **Business groups** area. The **Refresh configuration information** button is deactivated when Performance Management is not linked.#
4	**Business groups**	This area displays a list of business groups that the user can access. By selecting the check box for a business group, you can associate it with a monitored service. You can associate multiple business groups with a single monitored service. A business group that is already associated with a monitored service appears with its check box selected.
5	**To Monitor item settings** button	Clicking this button displays the monitoring item settings.

#

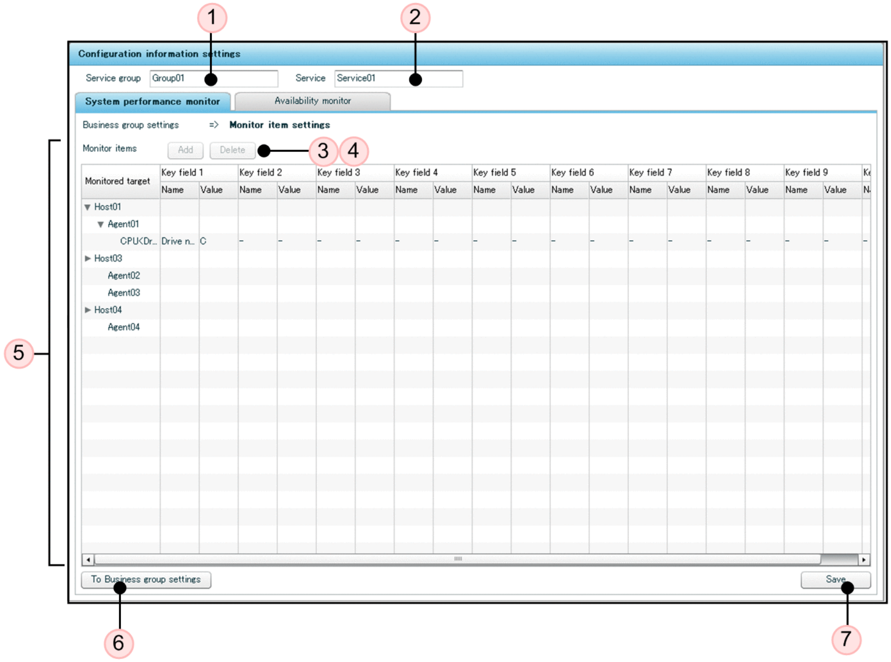
If no value has been set for the `pfmManagerHost` property in the `jp1itslm.properties` system definition file, it is assumed that Performance Management is not linked.

(3) Supplemental notes

- While the **Configuration information settings** area is being displayed for a monitored service, even if monitoring item settings for that monitored service are changed in another browser, the changed information will not be reflected on the screen until the **Configuration information settings** area is refreshed.

10.6.13 Configuration information settings area (Monitoring item settings with the System performance monitor tab selected)

(1) Window configuration



Service group Group01

Service Service01

Monitored target	Key field 1		Key field 2		Key field 3		Key field 4		Key field 5		Key field 6		Key field 7		Key field 8		Key field 9		Ke
	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	N.
▼ Host01																			
▼ Agent01																			
CPU<Dr...	Drive n...	C	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
▶ Host03																			
Agent02																			
Agent03																			
▶ Host04																			
Agent04																			

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This box displays the name of the service group selected in the **Services** area.
2	**Service**	This box displays the name of the monitored service selected in the **Services** area.
3	**Add** button	Clicking this button adds a monitoring item.
4	**Delete** button	Clicking this button deletes a monitoring item.
5	**Monitor items**	• **Monitored target** This column displays a hierarchical list of hosts, monitoring agents, and monitoring items selected from the business group settings. • **Key field** *X*

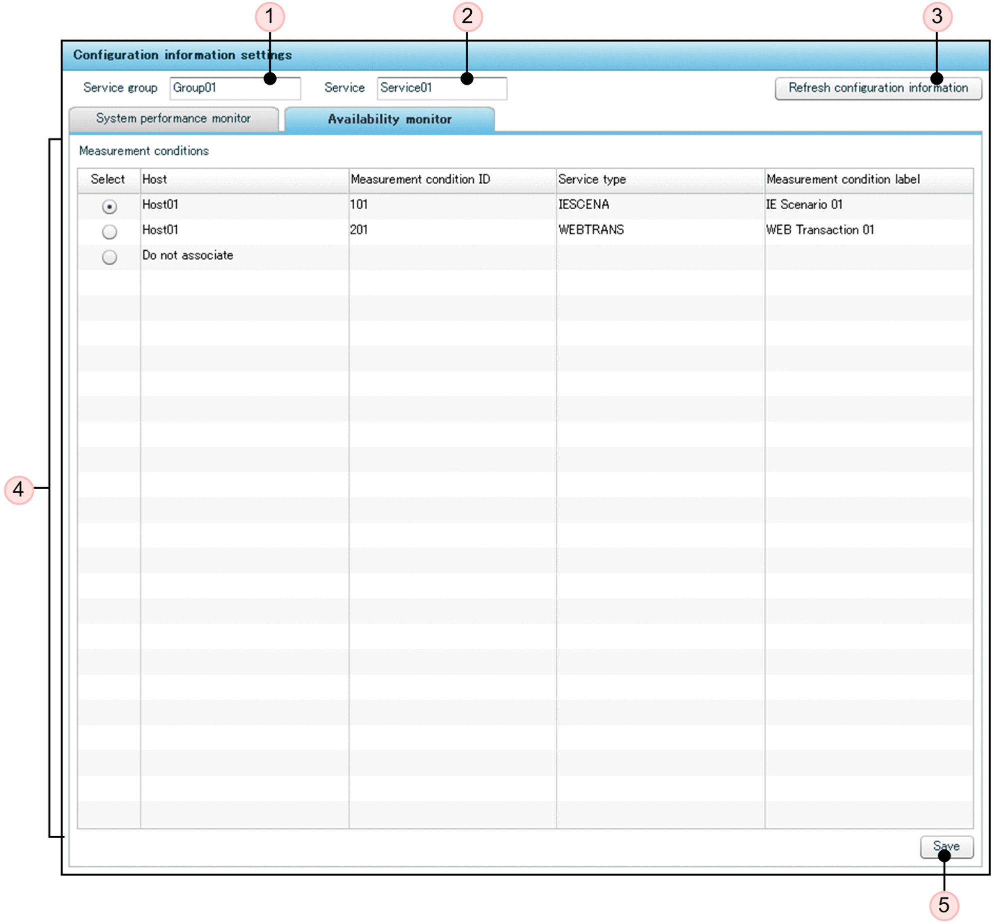
No.	Item	Description
5	**Monitor items**	*X* is a number from 1 to 10. If the monitoring item is a single instance, the hyphen (-) is displayed. If the monitoring item has multiple metrics, the key field information is displayed.
6	**To Business group settings** button	Clicking this button displays the business group settings.
7	**Save** button	Clicking this button saves the monitoring item settings displayed on the screen.

(3) Supplemental notes

- While the **Configuration information settings** area is being displayed for a monitored service, even if monitoring item settings for that monitored service are changed in another browser, the changed information will not be reflected on the screen until the **Configuration information settings** area is refreshed.
- If you do any of the following before you click the **Save** button, the settings will be discarded:
  - Select another service from the **Services** area.
  - Click the **To Business group settings** button.
  - Navigate to somewhere outside the **Configuration information settings** area
- If multiple users are logged in to ITSLM - Manager, and a service group administrator registers or deletes a monitored target, the timing for reflecting the change on the other users' screens is described in *3.2.9(1) Timing of updating the number of registered monitored targets*.

10.6.14 Configuration information settings area (with the Availability monitor tab selected)

(1) Window configuration



1
2
3
4
5
Configuration information settings
Refresh configuration information
System performance monitor
Availability monitor
Measurement conditions
Save

Service group: Group01

Service: Service01

Select	Host	Measurement condition ID	Service type	Measurement condition label
●	Host01	101	IESCENA	IE Scenario 01
○	Host01	201	WEBTRANS	WEB Transaction 01
○	Do not associate			

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This box displays the name of the service group selected in the **Services** area.
2	**Service**	This box displays the name of the monitored service selected in the **Services** area.
3	**Refresh configuration information** button	Clicking this button displays the Confirmation of refreshing configuration information window that you use to review the most recent (refreshed) Performance Management configuration information from the **Measurement conditions** area. The **Refresh configuration information** button is deactivated when Performance Management is not linked.#
4	**Measurement conditions**	• **Select** Select the radio button for the measurement condition you wish to associate with the monitored service. To clear the radio button settings, select the **Do not associate** radio button. If a measurement condition is already associated with the monitored service, its radio button appears already selected.

No.	Item	Description
4	**Measurement conditions**	- **Host** This column displays the name of the host of the measurement condition. - **Measurement condition ID** This column displays the ID of the measurement condition. - **Service type** This column indicates whether the service is running as an IE scenario or a Web transaction. - **Measurement condition label** This column displays the remark for the measurement condition.
5	**Save** button	Clicking this button saves the measurement condition settings that were entered.

#

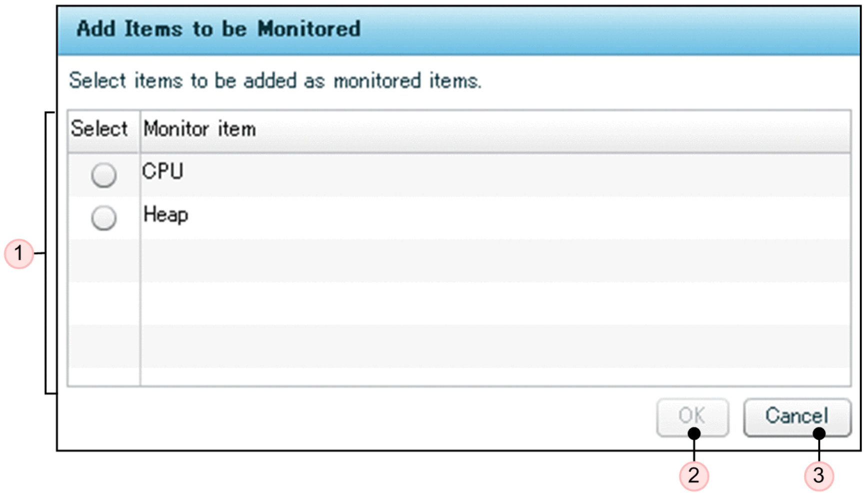
If no value is set for the `pfmManagerHost` property in the `jp1itslm.properties` system definition file, it is assumed that Performance Management is not linked.

(3) Supplemental notes

- While the **Configuration information settings** area is being displayed for a monitored service, even if the monitoring item settings for that monitored service are changed from another browser, the changed information will not be reflected on the screen until the **Configuration information settings** area is refreshed.
- If you do any of the following before you click the **Save** button, the settings will be discarded:
  - Select another service from the **Services** area.
  - Navigate to somewhere outside the **Configuration information settings** area.
- When measurement conditions are acquired, any measurement condition that is the same before and after acquisition will inherit the previous radio button setting for associating it with the monitored service.
- When measurement conditions are acquired, a measurement condition that is added on the Performance Management side will be added to the ITSLM measurement conditions in an unassociated state. For a measurement condition that is deleted on the Performance Management side, its association is automatically canceled and it is deleted from the ITSLM measurement conditions.
- If you change the measurement condition ID and service type of a measurement condition on the Performance Management side, on the ITSLM side it is assumed that the original measurement condition was deleted and a new measurement condition was added.
- If the host of the PFM - Agent for Service Response belongs to a business group, the measurement conditions will be visible only to service group administrators with permission to view that business group. If the host of the PFM - Agent for Service Response does not belong to a business group, the measurement conditions will be visible to all system administrators.
- If different service group administrators are changing the settings of the same service group at the same time, the settings of the last service group administrator to change the settings are the ones that take effect.
- If multiple service group administrators are changing settings, and a service group administrator clicks the **Save** button, until the settings are applied to ITSLM, the other service group administrators will not be able to click the **Save** button to apply their settings to ITSLM.

10.6.15 Add Items to be Monitored window

(1) Window configuration



Add Items to be Monitored

Select items to be added as monitored items.

Select	Monitor item
○	CPU
○	Heap

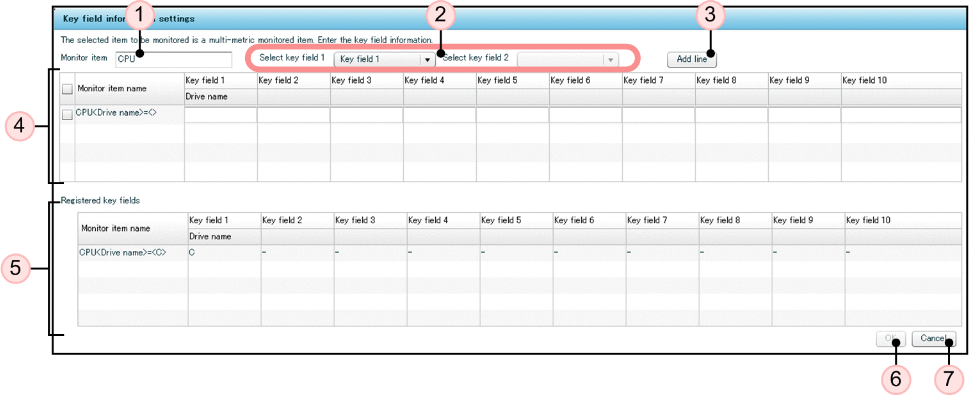
(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	Monitoring items	This area displays a list of monitoring items that belong to the monitoring agent that was selected when you clicked the **Add** button in the **Configuration information settings** area (**Monitor item settings** with the **System performance monitor** tab selected). Nothing is selected at the time the window is displayed.
2	**OK** button	For a single-instance monitoring item, clicking the **OK** button adds the monitoring item and returns to the **Configuration information settings** area. For a multi-instance monitoring item, clicking the **OK** button displays the Key field information settings window.
3	**Cancel** button	Clicking this button stops addition of monitoring items and returns to the **Configuration information settings** area.

10.6.16 Key field information settings window

(1) Window configuration



The selected item to be monitored is a multi-metric monitored item. Enter the key field information.

Monitor item: CPU

Select key field 1: Key field 1 ▾ Select key field 2: ▾

□ Monitor item name	Key field 1 Drive name	Key field 2	Key field 3	Key field 4	Key field 5	Key field 6	Key field 7	Key field 8	Key field 9	Key field 10
□ CPU<Drive name>=<>										

Registered key fields

Monitor item name	Key field 1 Drive name	Key field 2	Key field 3	Key field 4	Key field 5	Key field 6	Key field 7	Key field 8	Key field 9	Key field 10
CPU<Drive name>=<C>	C	-	-	-	-	-	-	-	-	-

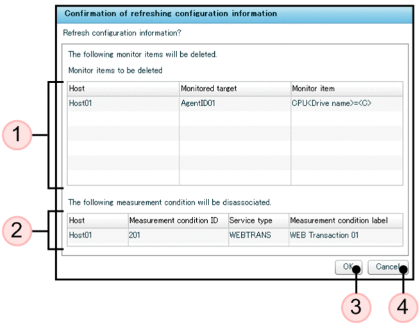
(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Monitor item**	This box displays the monitoring item selected in the Add Items to be Monitored window.
2	Select key field pull-down menus	The key fields used to generate the name of the monitoring item are selected from these pull-down menus. You must make a selection from **Select key field 1**, but **Select key field 2** is optional.
3	**Add line** button	Clicking this button adds one line to the key field information for the monitoring item.
4	Key field information for the monitoring item	• Check box Select a monitoring item's check box to register the monitoring item. If you select the check box in the header, the check boxes in all rows are selected. Similarly, if you clear the check box in the header, the check boxes in all rows are cleared. • **Monitor item name** This column displays the monitoring item name generated from the value in **Monitor item** and the values selected in the Select key field pull-down menus. • **Key field** *X* Enter in the text boxes in these columns the key field information for the monitoring item. The number of key field items is determined by the monitoring item that is being registered. All columns are blank by default. A character string consisting of 0 to 1,024 bytes can be specified in a text box.
5	**Registered key fields**	This area displays the registered key field information.
6	**OK** button	Clicking this button registers the key field information. The only thing that will be registered will be the key field information you selected from the monitoring item's key field information list. When you click the **OK** button, the Key field information settings window closes and the monitoring item registered in the Key field information settings window is added below the monitored target that was selected when you clicked the **Add** button in the **Configuration information settings** area.
7	**Cancel** button	Clicking this button cancels registration of the key field information.

10.6.17 Confirmation of refreshing configuration information window

(1) Window configuration



Confirmation of refreshing configuration information

Refresh configuration information?

The following monitor items will be deleted.

Monitor items to be deleted

Host	Monitored target	Monitor item
Host01	AgentID01	CPU<Drive name>=<C>

The following measurement condition will be disassociated.

Host	Measurement condition ID	Service type	Measurement condition label
Host01	201	WEBTRANS	WEB Transaction 01

(2) Window description

The following table lists the items that are displayed:

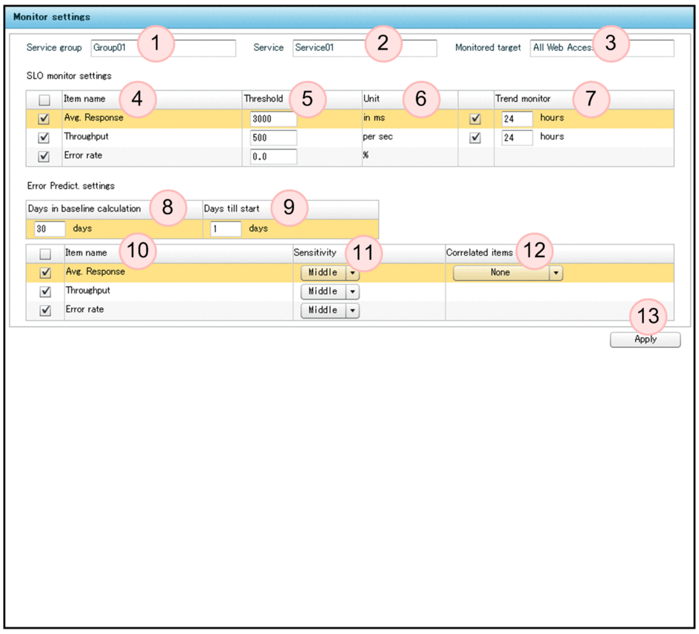
No.	Item	Description
1	**Monitor items to be deleted**	This area displays a table of the monitoring items that are to be deleted by the process for updating the configuration information. If no monitoring items are to be deleted, **No monitor items to delete** is displayed in place of the table.
2	Measurement conditions to be disassociated	This area displays a table of the measurement conditions that are to be disassociated when measurement conditions are deleted by the process for updating the configuration information and dissolving the associations between the selected monitored services and the measurement conditions. If no measurement conditions are being disassociated, **No measurement conditions to be disassociated** is displayed in place of the table.
3	**OK** button	Clicking this button executes the updates to the configuration information and measurement conditions.
4	**Cancel** button	Clicking this button cancels the updates to the configuration information and measurement conditions.

(3) Supplemental notes

- Configuration information cannot be updated simultaneously from multiple browsers within the same ITSLM system. However, it is permissible to update the configuration information from another browser in the period from when you click the **Refresh configuration information** button in the **Configuration information settings** area until you click the **OK** button in the Confirmation of refreshing configuration information window, because this period is not considered to be part of the update process.
- In the period from when you click the **Refresh configuration information** button in the **Configuration information settings** area until you click the **OK** button in the Confirmation of refreshing configuration information window, if a different browser updates the configuration information for the same monitored service, causing an inconsistency in the contents of the Confirmation of refreshing configuration information window, the following actions will be performed when you click the **OK** button:
    - The configuration information update process will abort.
    - A notification will be posted that configuration information updating has been executed from another browser, and you will be prompted to restart the configuration information process.

10.6.18 Monitor settings area (monitored target within the monitored service selected in the Services area)

(1) Window configuration



Monitor settings

Service group: Group01 Service: Service01 Monitored target: All Web Acces

SLO monitor settings

□	Item name	Threshold	Unit		Trend monitor
☑	Avg. Response	3000	in ms	☑	24 hours
☑	Throughput	500	per sec	☑	24 hours
☑	Error rate	0.0	%		

Error Predict. settings

Days in baseline calculation	Days till start
30 days	1 days

□	Item name	Sensitivity	Correlated items
☑	Avg. Response	Middle	None
☑	Throughput	Middle	
☑	Error rate	Middle	

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This box displays the name of the service group to which the monitored target selected in the **Services** area belongs.
2	**Service**	This box displays the name of the monitored service to which the monitored target selected in the **Services** area belongs.
3	**Monitored target**	This box displays the name of the monitored target selected in the **Services** area.
SLO monitor settings		
4	**Item name**	This column displays a list of monitoring items. Use the check box for each monitoring item to specify whether threshold monitoring is to be performed: Selected: Perform threshold monitoring. Cleared: Do not perform threshold monitoring. If you select the check box in the header row, the check boxes for all the monitoring item rows are selected. Similarly, if you clear the check box in the header row, the check boxes for all the monitoring item rows are cleared.
5	**Threshold**	Enter in this column a threshold value for each monitoring item. The following restrictions apply: **Avg. Response** monitoring item • You can specify a value in the range of `1` to `300000`. You can enter a value greater than `300000`, but we recommend that you not do so to avoid errors. • The unit is milliseconds. • You must specify a threshold value for average response time that is shorter than the length of the monitored service's timeout period. If you specify a period that is longer

No.	Item	Description
5	**Threshold**	than the timeout period, monitoring will be disabled so that the average response time will not exceed the threshold. **Throughput** monitoring item • You can specify a value in the range of `1` to `1000000`. You can enter a value greater than `1000000`, but we recommend that you not do so to avoid errors. • The unit is per second. **Error rate** monitoring item • You can specify a value in the range of `0` to `99.9`. You can enter a value greater than `99.9`, but we recommend that you not do so to avoid errors. • The unit is percent (%). • Only numeric digits and the period (`.`) can be entered. • The value is truncated at the second decimal place.
6	**Unit**	This column displays the unit of each monitoring item's value, as follows: **Avg. Response**: **in ms** (milliseconds) **Throughput**: **per sec** (transactions per second) **Error rate**: **%**
7	**Trend monitor**	You make entries in this column when trend monitoring is to be performed for each monitoring item. To perform trend monitoring, threshold monitoring must be selected with the applicable check box under **Item name**. Check box Selected: Perform trend monitoring. Cleared: Do not perform trend monitoring. Text box Specify in each text box the amount of time over which trend monitoring is to be performed for that monitoring item. A warning will be issued if a trend is detected that indicates that the threshold might be exceeded within the specified period from the present time. The following restrictions apply: • You can specify a value in the range from `1` to `168`. You can enter a value greater than 168, but we recommend that you not do so to avoid errors. • The unit is hours.
Error Predict. settings#		
8	**Days in baseline calculation**	Enter in this text box the number of days' worth of service performance that are to be used in the calculation of the baseline. A value must be entered even if out-of-range value detection is not performed. The following restrictions apply: • You must specify a value in the range from `1` to `60`. • The unit is days. • The entered value must satisfy the condition **Days in baseline calculation ≥ Days till start**.
9	**Days till start**	Enter in this text box the number of days' worth of past service performance for the monitored service that are to be obtained before out-of-range value detection will be started. A value must be entered even if out-of-range value detection is not performed. The following restrictions apply: • You must specify a value in the range from `1` to `60`. • The unit is days. • The entered value must satisfy the condition **Days in baseline calculation ≥ Days till start**.
10	**Item name**	This column displays a list of monitoring items. Use each monitoring item's check box to specify whether out-of-range value detection is to be performed for it: Selected: Perform out-of-range value detection.

No.	Item	Description
10	**Item name**	Cleared: Do not perform out-of-range value detection. If you select the check box in the header, the check boxes on all the rows are selected. Similarly, if you clear the check box in the header, the check boxes on all the rows are cleared.
11	**Sensitivity**	In this column, use the pull-down menu for each monitoring item to specify its sensitivity for out-of-range value detection. You can select for each monitoring item a sensitivity of **High**, **Middle**, or **Low**. The higher the sensitivity, the more likely detection becomes.
12	**Correlated items**	Use this column to specify whether out-of-range value detection is to be performed for a combination of multiple monitoring items. Use the pull-down menu to select the monitoring item to be combined. No selection can be made for a monitoring item that does not allow out-of-range value detection in combination with another monitoring item; nothing is displayed in this field in such a case. Note that even if **Throughput** is selected from this pull-down menu, out-of-range value detection of throughput alone will not be performed. To perform out-of-range value detection of throughput alone, you must use the separate **Throughpu**t item to specify out-of-range value detection.
13	**Apply** button	Clicking this button applies the settings.

#

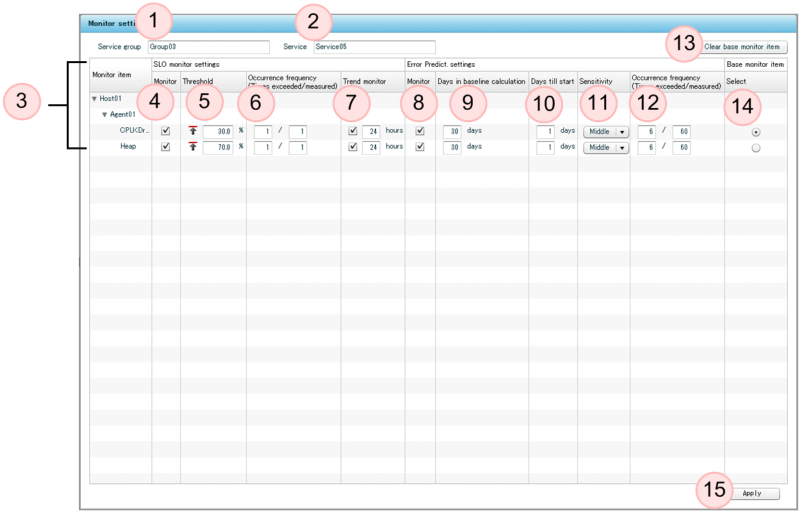
This area is for configuring out-of-range value detection.

(3) Supplemental notes

- If you attempt to set monitoring items without having stopped monitoring of the monitored service whose monitoring items are being set, an error message will be displayed when you click the **Apply** button and the settings will not be applied.
- Even when text boxes are not active, the values entered in them are retained until another monitored service is selected or a transition to another window occurs.
- If a service group administrator sets monitoring items while multiple users are logged in to ITSLM - Manager, those settings will not be reflected on the screens of other service group administrators until those other service group administrators display or refresh the **Monitor settings** area of the Settings window.

10.6.19 Monitor settings area (monitored service selected in the Services area)

(1) Window configuration



Monitor setti

Service group Group03

Service Service05

Clear base monitor item

Monitor item	SLO monitor settings				Error Predict. settings					Base monitor item
	Monitor	Threshold	Occurrence frequency (Times exceeded/measured)	Trend monitor	Monitor	Days in baseline calculation	Days till start	Sensitivity	Occurrence frequency (Times exceeded/measured)	Select
▼ Host01										
▼ Agent01										
CPU<Dr...	☑	↑ 30.0 %	1 / 1	☑ 24 hours	☑	30 days	1 days	Middle ▾	6 / 60	●
Heap	☑	↑ 70.0 %	1 / 1	☑ 24 hours	☑	30 days	1 days	Middle ▾	6 / 60	○

Apply

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Service group**	This box displays the name of the service group to which the monitored service selected in the **Services** area belongs.
2	**Service**	This box displays the name of the monitored service selected in the **Services** area.
3	**Monitor item**	This column displays the names of the monitoring items.
SLO monitor settings		
4	**Monitor**	Use the check boxes in this column to specify for each item whether threshold monitoring is to be performed: Selected: Perform threshold monitoring. Cleared: Do not perform threshold monitoring.
5	**Threshold**	This column indicates whether the threshold of the monitoring item is an upper-limit threshold value or a lower-limit threshold value: ↑ : Upper-limit threshold value ↓ : Lower-limit threshold value Enter in the text box a threshold value for the monitoring item. You can enter a value that is greater than or equal to `0` for the threshold. A number with decimal places can be entered. However, because the precision is 7 digits, do not enter a value that exceeds 7 digits.
6	**Occurrence frequency (Times exceeded/measured)**	Specify in this column for each monitoring item the number of times the threshold can be exceeded within a specified number of measurements before an event is issued. You can specify a value in the range from `1` to `100` for the number of times exceeded and for the number of measurements. However, you cannot specify a value for the number of times exceeded that is greater than the number of measurements.
7	**Trend monitor**	For each monitoring item, specify the check box in this column if you wish to perform trend monitoring.

No.	Item	Description
7	**Trend monitor**	To perform trend monitoring, a threshold value must have been entered for the monitoring item for which you wish to perform trend monitoring. Check box Selected: Perform trend monitoring. Cleared: Do not perform trend monitoring. Text box Specify the amount of time during which trend monitoring is to be performed. A warning will be issued if a trend is detected indicating that the threshold might be exceeded within the specified period from the present time. The following restrictions apply: • You can specify a value in the range from `1` to `168`. You can enter a value that is greater than `168`, but we recommend that you not do so to avoid errors. • The unit is hours.
Error Predict. settings		
8	**Monitor**	For each monitoring item, select the check box in this column if you wish to perform out-of-range value detection: Selected: Perform out-of-range value detection. Cleared: Do not perform out-of-range value detection. If you select the check box in the header, the check boxes in all the rows are selected. Similarly, if you clear the check box in the header, the check boxes in all the rows are cleared.
9	**Days in baseline calculation**	Enter in this text box the number of days' worth of service performance that are to be used in the calculation of the baseline. A value must be entered even if out-of-range value detection is not performed. The following restrictions apply: • You must specify a value in the range from `1` to `60`. • The unit is days.
10	**Days till start**	Enter in this text box the number of days' worth of past service performance that are to be obtained before out-of-range value detection will be started. A value must be entered even if out-of-range value detection is not performed. The following restrictions apply: • You must specify a value in the range from `1` to `60`. • The unit is days.
11	**Sensitivity**	In this column, use the pull-down menu for each monitoring item to specify its sensitivity for out-of-range value detection. You can select for each monitoring item a sensitivity of **High**, **Middle**, or **Low**. The higher the sensitivity, the more likely detection becomes.
12	**Occurrence frequency (Times exceeded/measured)**	Specify in this column for each monitoring item the number of times the threshold can be exceeded within a specified number of measurements before an event is issued. You can specify a value in the range from `1` to `100` for the number of times exceeded and for the number of measurements. However, you cannot specify a value for the number of times exceeded that is greater than the number of measurements.
13	**Clear base monitor item** button	Click this button to reset the settings for the monitoring item specified in **SLO monitor settings** and **Error Predict. settings** to the default (all unselected status). This button is displayed when the service monitoring configuration is **System**.
14	**Base monitor item** radio button	Select the radio button for the monitoring item to be used as the base for selecting the dates to be used for creating the baseline. These radio buttons are displayed when the service monitoring configuration is **System**.
15	**Apply** button	Clicking this button applies the settings.

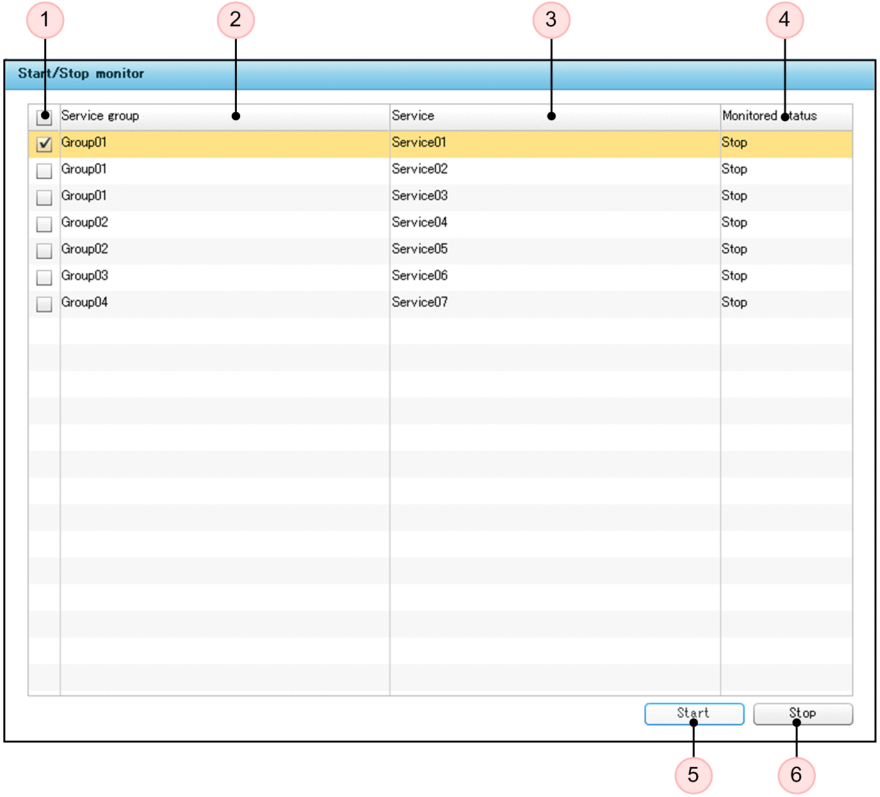
(3) Supplemental notes

- The settings will be discarded if you do any of the following before you click the **Save** button:

- Select another service in the **Services** area.
- Select anything outside the **Monitor settings** area.

10.6.20 Start/Stop monitor area

(1) Window configuration



☐	Service group	Service	Monitored status
☑	Group01	Service01	Stop
☐	Group01	Service02	Stop
☐	Group01	Service03	Stop
☐	Group02	Service04	Stop
☐	Group02	Service05	Stop
☐	Group03	Service06	Stop
☐	Group04	Service07	Stop

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	Check boxes	Select the check boxes for the monitored services whose monitoring you wish to start or stop. If you select the check box in the header, the check boxes for all the rows are selected. Similarly, if you clear the check box in the header, the check boxes for all the rows are cleared.
2	**Service group**	This column displays the name of the service group for each monitored service.
3	**Service**	This column displays the name of each monitored service.
4	**Monitored status**	This column displays the current monitoring status of each monitored service: **Start**: Monitoring has started (monitoring is being performed). **Stop**: Monitoring has stopped (monitoring is not being performed).
5	**Start** button	Clicking this button starts monitoring of the monitored services whose check box is selected.
6	**Stop** button	Clicking this button stops monitoring of the monitored services whose check box is selected.

(3) Supplemental notes

- Until start monitoring processing has finished for the selected monitored services, no other operations can be performed.
- If no check boxes are selected in the **Start/Stop monitor** area, you cannot click the **Start** button.
- If you click the **Start** button while a monitored service that is already being monitored is selected, its monitoring status does not change.
- When you select multiple monitored services and start monitoring, their start processes are executed in parallel. As a result, even if an error occurs in the start process for one monitored service, the start processes continue for the other monitored services. However, if you attempt to start monitoring of a monitored service that has been deleted by another user, an error message will be displayed and the start processes for all the monitored services will be suspended. In such a case, you must start over by selecting the monitored services whose monitoring is to be started and clicking the **Start** button again.
- If monitoring fails to start for any of the selected monitored services, an error message is displayed. Correct the error, and then click the **Start** button again.
- If the ITSLM - UR that is to monitor the selected monitored services is not running, monitoring of those monitored services will not start. You can check which monitored services failed to start in the *KNAS16304-E* message that is output to the message log.
- When monitoring of a monitored service starts, the start time is output to the message log. The messages that are output for the various types of monitoring are listed below.

  Service performance monitoring

  - Threshold monitoring: *KNAS32017-I* message.
  - Trend monitoring: *KNAS32018-I* message.
  - Error detection: *KNAS32019-I* message.

  System performance monitoring

  - Threshold monitoring: message *KNAS32023-I*.
  - Trend monitoring: *KNAS32024-I* message.
  - Error detection: *KNAS32025-I* message.

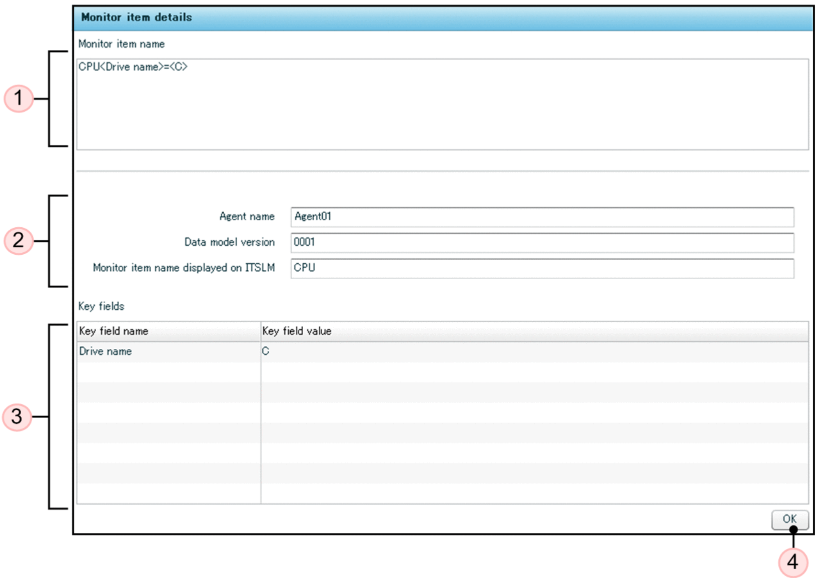
  Availability monitoring

  - Availability monitoring: *KNAS32027-I* message.
- When you start monitoring a monitored service, monitoring by the ITSLM - UR that is being used to monitor stops and then restarts. This means that, for Web transactions that are monitored by the same ITSLM - UR as the monitored services that are starting, their monitoring will start fresh again from the first Web access following restart.
- Until stop monitoring processing has finished for the selected monitored services, no other operations can be performed.
- If no check boxes are selected in the **Start/Stop monitor** area, you cannot click the **Stop** button.
- If you select a monitored service whose monitoring has already stopped and click the **Stop** button, its monitored status will not change.
- When you select multiple monitored services and stop monitoring, their stop processes are executed in parallel. As a result, even if an error occurs in the stop process for one monitored service, the stop processes continue for the other monitored services. However, if you attempt to stop monitoring of a monitored service that has been deleted by another user, an error message will be displayed and the stop processes for all the monitored services will be suspended. In such a case, you must start over by selecting the monitored services whose monitoring is to be stopped and clicking the **Stop** button again.

- If monitoring fails to stop for some of the monitored services, an error message is displayed. Correct the error, and then click the **Stop** button again.
- Even if the ITSLM - UR that is monitoring the selected monitored services is not running, monitoring of the selected monitored services will stop successfully. The *KNAS16414-W* message indicating that ITSLM - UR is not running will be output to the message log.
- When you stop monitoring a monitored service, monitoring by the ITSLM - UR that is being used to monitor stops and then restarts. This means that, for Web transactions that are monitored by the same ITSLM - UR as the monitored services that are starting, their monitoring will start fresh again from the first Web access following restart.
- If you start (resume) monitoring more than 24 hours after stopping monitoring, there might not be a full minute's worth of acquired information since the time monitoring finally stopped to use for the baseline calculation. In this case, you can correct this situation by continuing to monitor for at least one hour, or by stopping monitoring and restarting.

10.6.21 Monitor item details window

(1) Window configuration



Monitor item name

CPU<Drive name>=<C>

Agent name: Agent01

Data model version: 0001

Monitor item name displayed on ITSLM: CPU

Key fields

Key field name	Key field value
Drive name	C

(2) Window description

The following table lists the items that are displayed:

No.	Item	Description
1	**Monitor item name**	This area displays the name of a system performance monitoring item. If the name of the monitoring item is too long to fit in the area, an abbreviated version of the name is displayed.
2	Monitoring item information	• **Agent name** This box displays the name of the monitoring agent to which the monitoring item belongs. • **Data model version** This box displays the data model version of the monitoring agent to which the monitoring item belongs. • **Monitor item name displayed on ITSLM**

No.	Item	Description
2	Monitoring item information	This box displays the monitoring item name that was set in Performance Management and that is displayed in ITSLM.
3	**Key fields**	This area displays a table of the key field names and key field values. In the case of a single instance, this table will be empty. If any character string is too long to fit in the window, you can move the cursor over it to view the entire character string.
4	**OK** button	Clicking this button closes the Monitor item details window.

11 Messages

This chapter explains the messages issued by ITSLM.

11.1 Format of messages

This section describes the output format of the ITSLM messages, as well as the format of the explanations used in this manual.

11.1.1 Output format of messages

A message output by ITSLM consists of a message ID that starts with `KNAS`, followed by a message text.

```
KNASnnnnn-Zmessage-text
```

The elements of the message ID are as follows:

`KNAS`

An identifier indicating that the message is an ITSLM message.

nnnnn

The serial number of the message.

Z

The type of message.

The following table shows the message types, the contents of each message type, and the corresponding Windows event log type.

Table 11–1: Message types, their contents, and the Windows event log types

Type	Contents	Type of Windows event log
E	Indicates an error message. These messages instruct the user that corrective action is required.	Error
I	Indicates a notification message. These messages provide the user with information.	Information
Q	Indicates a notification message. These messages ask the user to select an action.	Notification
W	Indicates a warning message. These messages issue a warning, although processing continues. The user is recommended to take corrective action as necessary.	Warning

11.1.2 Format of message explanations

The format of the explanations of ITSLM output messages used in this manual is shown below. Not all of these items are provided for some messages.

message-ID

message-text

xx....xx: Indicator of a variable value contained in the message text.

Explanation of the variable shown in the message text (*xx....xx* is lower-case letters).

Description

Description of the message.

(S)

Processing performed by the system at the time the message is output.

(O)

Corrective action to be taken by the operator when the message has been output.

11.1.3 For system administrators

When a problem occurs, begin by collecting data needed to investigate why the message was issued, as detailed in *7.1.6 Collecting the data needed for determining the cause of a problem*.

If an error dialog box is displayed when the problem occurs, start collecting data while the dialog box is being displayed.

11.2 Message destinations

The following table shows the destinations of the ITSLM messages.

Table 11–2: Message destinations

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS02000-I	N	Y	Y	Y
KNAS02001-I	N	Y	Y	Y
KNAS02002-E	N	Y	Y	Y
KNAS02003-I	N	N	Y	Y
KNAS02004-I	N	N	Y	Y
KNAS02005-I	N	N	Y	Y
KNAS02006-I	N	N	Y	Y
KNAS02007-I	N	N	N	N
KNAS02008-I	N	N	N	N
KNAS02009-E	N	N	N	N
KNAS02010-E	N	N	Y	Y
KNAS02025-E	N	N	Y	Y
KNAS02035-E	N	N	Y	Y
KNAS02036-E	N	N	Y	Y
KNAS02043-I	N	N	Y	Y
KNAS02089-I	N	N	Y	Y
KNAS02090-I	N	N	Y	Y
KNAS02091-E	N	N	Y	Y
KNAS02092-W	N	N	Y	Y
KNAS02094-E	N	N	Y	Y
KNAS02095-E	N	N	Y	Y
KNAS02099-E	N	N	Y	Y
KNAS02102-I	N	N	Y	Y
KNAS02118-E	N	N	Y	Y
KNAS02119-E	N	N	Y	Y
KNAS02120-E	N	N	Y	Y
KNAS02121-E	N	N	Y	Y
KNAS02125-W	N	N	Y	N
KNAS02126-W	N	N	Y	Y
KNAS02127-I	N	N	Y	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS02128-E	N	N	Y	Y
KNAS02129-E	N	N	Y	Y
KNAS03004-E	N	N	N	Y
KNAS03005-E	N	N	N	Y
KNAS03007-E	N	N	N	Y
KNAS03016-W	N	N	N	Y
KNAS03020-E	N	N	N	Y
KNAS03022-I	N	N	N	Y
KNAS03023-I	N	N	N	Y
KNAS03024-I	N	N	N	Y
KNAS03025-I	N	N	N	Y
KNAS03026-I	N	N	N	Y
KNAS03027-E	N	N	N	Y
KNAS03028-E	N	N	N	Y
KNAS03029-W	N	N	N	Y
KNAS03030-E	N	N	N	Y
KNAS03031-E	N	N	N	Y
KNAS03032-E	N	N	N	Y
KNAS03033-W	N	N	N	Y
KNAS03034-W	N	N	N	Y
KNAS03035-W	N	N	N	Y
KNAS03036-I	N	N	N	Y
KNAS03037-I	N	N	N	Y
KNAS03038-E	N	N	N	Y
KNAS03039-E	N	N	N	Y
KNAS03040-W	N	N	N	Y
KNAS03041-W	N	N	N	Y
KNAS03042-W	N	N	N	Y
KNAS03044-E	N	N	N	Y
KNAS05000-E	N	N	N	Y
KNAS09000-E	N	N	Y	N
KNAS09001-E	N	N	N	N
KNAS09002-E	N	N	Y	N
KNAS09003-E	N	N	Y	N

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS09004-E	N	N	Y	N
KNAS09005-W	N	N	Y	N
KNAS09007-E	N	N	N	Y
KNAS09008-E	N	N	N	Y
KNAS09009-E	N	N	N	Y
KNAS09014-E	N	N	Y	N
KNAS09015-W	N	N	Y	N
KNAS09016-E	N	N	N	Y
KNAS09021-E	N	N	N	Y
KNAS09022-E	N	N	Y	N
KNAS09023-E	N	N	N	Y
KNAS09100-E	N	N	N	Y
KNAS10000-I	Y	N	N	N
KNAS10001-E	Y	N	N	N
KNAS10002-Q	Y	N	N	N
KNAS10003-I	Y	N	N	N
KNAS11400-I	Y	N	N	N
KNAS11500-I	Y	N	N	N
KNAS11600-Q	Y	N	N	N
KNAS11601-E	Y	N	N	N
KNAS11602-W	Y	N	N	N
KNAS11603-I	Y	N	N	N
KNAS11604-Q	Y	N	N	N
KNAS11605-I	Y	N	N	N
KNAS11606-Q	Y	N	N	N
KNAS11607-I	Y	N	N	N
KNAS11700-I	Y	N	N	N
KNAS11701-Q	Y	N	N	N
KNAS11702-I	Y	N	N	N
KNAS11703-I	Y	N	N	N
KNAS11704-I	Y	N	N	N
KNAS11705-Q	Y	N	N	N
KNAS11706-I	Y	N	N	N
KNAS11707-Q	Y	N	N	N

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS11708-Q	Y	N	N	N
KNAS11709-Q	Y	N	N	N
KNAS11710-I	Y	N	N	N
KNAS11711-E	Y	N	N	N
KNAS11712-I	Y	N	N	N
KNAS11713-Q	Y	N	N	N
KNAS11714-Q	Y	N	N	N
KNAS11715-I	Y	N	N	N
KNAS11716-I	Y	N	N	N
KNAS11717-I	Y	N	N	N
KNAS11718-Q	Y	N	N	N
KNAS11719-Q	Y	N	N	N
KNAS11720-E	Y	N	N	N
KNAS15000-I	Y	N	N	Y
KNAS15001-E	Y#	N	N	Y
KNAS15005-E	Y#	N	N	Y
KNAS15006-E	Y#	N	N	Y
KNAS15007-E	Y#	N	N	Y
KNAS15008-E	Y	N	N	Y
KNAS15009-I	Y	N	N	Y
KNAS15300-I	N	N	N	Y
KNAS15301-E	Y	N	N	Y
KNAS15302-E	Y	N	N	Y
KNAS15304-E	Y	N	N	Y
KNAS15305-E	Y	N	N	Y
KNAS15306-I	N	N	N	Y
KNAS15307-E	N	N	N	Y
KNAS15308-E	Y	N	N	Y
KNAS15309-E	Y	N	N	Y
KNAS15310-E	Y	N	N	Y
KNAS15311-E	N	N	N	Y
KNAS15312-E	Y	N	N	Y
KNAS15313-E	Y	N	N	N
KNAS15400-I	N	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
`KNAS15401-E`	N	N	N	Y
`KNAS15403-E`	N	N	N	Y
`KNAS15404-E`	N	N	N	Y
`KNAS15405-I`	N	N	N	Y
`KNAS15500-I`	N	N	N	Y
`KNAS15501-E`	Y	N	N	Y
`KNAS15502-E`	Y#	N	N	Y
`KNAS15503-E`	Y	N	N	Y
`KNAS15504-E`	Y#	N	N	Y
`KNAS15505-E`	Y	N	N	Y
`KNAS15507-E`	Y	N	N	Y
`KNAS15508-E`	Y	N	N	Y
`KNAS15509-E`	Y	N	N	Y
`KNAS15510-E`	Y	N	N	Y
`KNAS15511-E`	Y	N	N	Y
`KNAS15600-I`	N	N	N	Y
`KNAS15601-E`	Y	N	N	Y
`KNAS15602-E`	Y#	N	N	Y
`KNAS15603-E`	Y	N	N	Y
`KNAS15604-E`	Y#	N	N	Y
`KNAS15605-E`	Y	N	N	Y
`KNAS15607-E`	Y	N	N	Y
`KNAS15608-E`	Y	N	N	Y
`KNAS15609-E`	Y	N	N	Y
`KNAS15712-I`	N	N	N	Y
`KNAS15713-E`	N	N	N	Y
`KNAS15714-E`	N	N	N	Y
`KNAS15715-E`	N	N	N	Y
`KNAS15716-E`	Y#	N	N	Y
`KNAS15717-E`	Y	N	N	Y
`KNAS15718-E`	Y	N	N	Y
`KNAS15719-W`	Y	N	N	Y
`KNAS15720-E`	Y	N	N	Y
`KNAS15721-E`	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS15722-E	Y#	N	N	Y
KNAS15723-E	Y	N	N	Y
KNAS15810-I	N	N	N	Y
KNAS15811-E	N	N	N	Y
KNAS15812-E	N	N	N	Y
KNAS15813-E	N	N	N	Y
KNAS15814-E	Y	N	N	Y
KNAS15815-E	Y	N	N	Y
KNAS15816-W	Y	N	N	Y
KNAS15817-E	Y	N	N	Y
KNAS15818-E	Y#	N	N	Y
KNAS15908-E	N	N	N	Y
KNAS15909-E	N	N	N	Y
KNAS15910-E	N	N	N	Y
KNAS15911-E	Y	N	N	Y
KNAS15912-E	Y	N	N	Y
KNAS15913-E	Y	N	N	Y
KNAS15914-E	Y#	N	N	Y
KNAS15915-E	Y	N	N	Y
KNAS16000-E	Y#	N	N	Y
KNAS16001-E	Y	N	N	Y
KNAS16002-E	Y#	N	N	Y
KNAS16003-E	Y	N	N	Y
KNAS16004-E	Y	N	N	Y
KNAS16100-I	N	N	N	Y
KNAS16101-E	Y	N	N	Y
KNAS16102-E	Y#	N	N	Y
KNAS16103-E	Y	N	N	Y
KNAS16104-E	Y#	N	N	Y
KNAS16105-E	Y	N	N	Y
KNAS16107-E	Y	N	N	Y
KNAS16108-E	Y	N	N	Y
KNAS16109-E	Y	N	N	Y
KNAS16110-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS16200-I	N	N	N	Y
KNAS16201-E	Y#	N	N	Y
KNAS16202-E	Y	N	N	Y
KNAS16203-E	Y#	N	N	Y
KNAS16204-E	Y	N	N	Y
KNAS16205-E	Y	N	N	Y
KNAS16206-E	Y	N	N	Y
KNAS16300-I	N	N	N	Y
KNAS16301-E	Y	N	N	Y
KNAS16302-E	N	N	N	Y
KNAS16303-E	N	N	N	Y
KNAS16304-E	N	N	N	Y
KNAS16305-E	N	N	N	Y
KNAS16306-E	N	N	N	Y
KNAS16307-E	N	N	N	Y
KNAS16308-E	Y	N	N	Y
KNAS16309-E	Y#	N	N	Y
KNAS16310-E	Y	N	N	Y
KNAS16311-E	Y#	N	N	Y
KNAS16312-E	Y	N	N	Y
KNAS16314-E	Y#	N	N	Y
KNAS16315-E	N	N	N	Y
KNAS16316-E	N	N	N	Y
KNAS16317-E	N	N	N	Y
KNAS16318-E	Y	N	N	Y
KNAS16319-E	Y	N	N	Y
KNAS16320-E	Y	N	N	Y
KNAS16321-E	Y	N	N	Y
KNAS16322-E	Y	N	N	Y
KNAS16323-W	N	N	N	Y
KNAS16324-E	N	N	N	Y
KNAS16325-E	Y	N	N	Y
KNAS16400-I	N	N	N	Y
KNAS16401-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS16402-E	N	N	N	Y
KNAS16403-E	N	N	N	Y
KNAS16404-E	N	N	N	Y
KNAS16405-E	N	N	N	Y
KNAS16407-E	N	N	N	Y
KNAS16408-E	Y	N	N	Y
KNAS16409-E	Y#	N	N	Y
KNAS16410-E	Y	N	N	Y
KNAS16411-E	Y#	N	N	Y
KNAS16412-E	Y	N	N	Y
KNAS16414-W	N	N	N	Y
KNAS16415-E	Y#	N	N	Y
KNAS16416-E	N	N	N	Y
KNAS16417-E	N	N	N	Y
KNAS16418-E	Y	N	N	Y
KNAS16419-W	Y	N	N	Y
KNAS16420-E	N	N	N	Y
KNAS16421-I	N	N	N	Y
KNAS16422-E	Y	N	N	Y
KNAS16423-E	Y	N	N	Y
KNAS16424-E	Y	N	N	Y
KNAS16425-E	N	N	N	Y
KNAS16500-E	Y#	N	N	Y
KNAS16501-E	Y	N	N	Y
KNAS16502-E	Y#	N	N	Y
KNAS16503-E	Y	N	N	Y
KNAS16600-E	Y#	N	N	Y
KNAS16601-E	Y	N	N	Y
KNAS16602-E	Y	N	N	Y
KNAS16700-E	Y#	N	N	Y
KNAS16701-E	Y	N	N	Y
KNAS16702-E	Y	N	N	Y
KNAS16800-E	Y#	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS16801-E	Y	N	N	Y
KNAS16802-E	Y#	N	N	Y
KNAS16803-E	Y	N	N	Y
KNAS16900-E	Y#	N	N	Y
KNAS16901-E	Y	N	N	Y
KNAS16902-E	Y	N	N	Y
KNAS17000-E	Y#	N	N	Y
KNAS17001-E	Y	N	N	Y
KNAS17002-E	Y	N	N	Y
KNAS17300-E	Y	N	N	Y
KNAS17301-E	Y	N	N	Y
KNAS17302-E	Y#	N	N	Y
KNAS17303-E	Y	N	N	Y
KNAS17400-E	Y	N	N	Y
KNAS17401-E	Y	N	N	Y
KNAS17402-E	Y#	N	N	Y
KNAS17403-E	Y	N	N	Y
KNAS17500-I	N	N	N	Y
KNAS17501-E	Y	N	N	Y
KNAS17502-E	Y	N	N	Y
KNAS17503-E	Y#	N	N	Y
KNAS17504-E	Y	N	N	Y
KNAS17561-E	Y#	N	N	Y
KNAS17562-E	Y	N	N	Y
KNAS17564-E	Y	N	N	Y
KNAS17565-E	Y	N	N	Y
KNAS17566-E	Y	N	N	Y
KNAS17567-E	Y	N	N	Y
KNAS17568-E	Y#	N	N	Y
KNAS17569-E	Y	N	N	Y
KNAS17570-E	Y#	N	N	Y
KNAS17571-E	Y	N	N	Y
KNAS17572-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS17573-E	Y	N	N	Y
KNAS17574-E	Y	N	N	Y
KNAS17575-I	N	N	N	Y
KNAS17576-E	Y	N	N	Y
KNAS17577-E	Y	N	N	Y
KNAS17578-E	Y	N	N	Y
KNAS17579-E	Y#	N	N	Y
KNAS17580-E	Y	N	N	Y
KNAS17581-E	Y	N	N	Y
KNAS17582-E	Y#	N	N	Y
KNAS17583-I	N	N	N	Y
KNAS17584-E	Y	N	N	Y
KNAS17585-E	Y	N	N	Y
KNAS17586-E	Y	N	N	Y
KNAS17587-E	Y#	N	N	Y
KNAS17588-E	Y	N	N	Y
KNAS17589-E	Y	N	N	Y
KNAS17590-E	Y#	N	N	Y
KNAS17591-I	N	N	N	Y
KNAS17592-E	Y	N	N	Y
KNAS17593-E	Y	N	N	Y
KNAS17594-E	Y#	N	N	Y
KNAS17595-E	Y	N	N	Y
KNAS17596-E	Y#	N	N	Y
KNAS17597-E	Y	N	N	Y
KNAS17598-E	Y	N	N	Y
KNAS17600-I	N	N	N	Y
KNAS17601-E	Y	N	N	Y
KNAS17602-E	Y#	N	N	Y
KNAS17603-E	Y	N	N	Y
KNAS17604-E	Y#	N	N	Y
KNAS17605-E	Y	N	N	Y
KNAS17606-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS17607-E	Y	N	N	Y
KNAS17608-E	Y	N	N	Y
KNAS17609-E	Y	N	N	Y
KNAS17610-E	Y	N	N	Y
KNAS17611-E	Y	N	N	Y
KNAS17700-I	N	N	N	Y
KNAS17701-E	Y	N	N	Y
KNAS17702-E	Y#	N	N	Y
KNAS17703-E	Y	N	N	Y
KNAS17704-E	Y#	N	N	Y
KNAS17705-E	Y	N	N	Y
KNAS17706-E	Y	N	N	Y
KNAS17707-E	Y	N	N	Y
KNAS17708-E	Y	N	N	Y
KNAS17709-E	Y	N	N	Y
KNAS17800-E	Y	N	N	Y
KNAS17801-E	Y	N	N	N
KNAS17802-E	Y	N	N	Y
KNAS17803-E	Y	N	N	Y
KNAS17804-*I*	Y	N	N	N
KNAS17805-W	Y	N	N	Y
KNAS17806-E	Y	N	N	Y
KNAS17807-E	N	N	N	Y
KNAS18100-I	N	N	N	Y
KNAS18101-E	Y#	N	N	Y
KNAS18102-E	Y	N	N	Y
KNAS18103-E	Y#	N	N	Y
KNAS18104-E	Y	N	N	Y
KNAS18105-E	Y	N	N	Y
KNAS18106-E	Y	N	N	Y
KNAS18107-E	Y	N	N	Y
KNAS18108-E	Y	N	N	Y
KNAS18109-E	Y	N	N	Y
KNAS18110-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS18200-E	Y#	N	N	Y
KNAS18201-E	Y	N	N	Y
KNAS18202-E	Y#	N	N	Y
KNAS18300-I	N	N	N	Y
KNAS18301-E	Y	N	N	Y
KNAS18302-E	Y#	N	N	Y
KNAS18303-E	Y	N	N	Y
KNAS18304-E	Y#	N	N	Y
KNAS18305-E	Y	N	N	Y
KNAS18306-E	Y	N	N	Y
KNAS18307-E	Y	N	N	Y
KNAS18308-E	Y	N	N	Y
KNAS18309-E	Y	N	N	Y
KNAS18310-E	Y	N	N	Y
KNAS18400-I	N	N	N	Y
KNAS18401-E	Y	N	N	Y
KNAS18402-E	Y#	N	N	Y
KNAS18403-E	Y	N	N	Y
KNAS18404-E	Y	N	N	Y
KNAS18405-E	Y	N	N	Y
KNAS18406-E	Y	N	N	Y
KNAS18407-E	Y	N	N	Y
KNAS18408-E	Y	N	N	Y
KNAS18409-E	Y	N	N	Y
KNAS18410-W	N	N	N	Y
KNAS18411-E	Y	N	N	Y
KNAS18412-I	N	N	N	Y
KNAS18413-E	Y#	N	N	Y
KNAS18414-E	Y	N	N	Y
KNAS18415-E	Y	N	N	Y
KNAS18416-E	Y	N	N	Y
KNAS18417-E	Y	N	N	Y
KNAS18418-E	Y	N	N	Y
KNAS18419-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS18420-I	N	N	N	Y
KNAS18421-E	Y#	N	N	Y
KNAS18422-E	Y	N	N	Y
KNAS18423-E	Y	N	N	Y
KNAS18424-E	Y	N	N	Y
KNAS18425-E	Y	N	N	Y
KNAS18426-E	Y	N	N	Y
KNAS18427-E	Y	N	N	Y
KNAS18428-E	Y#	N	N	Y
KNAS18429-E	Y	N	N	Y
KNAS18430-E	Y	N	N	Y
KNAS18431-E	Y#	N	N	Y
KNAS18432-E	Y	N	N	Y
KNAS18433-E	Y	N	N	Y
KNAS18434-E	Y	N	N	Y
KNAS18435-E	Y	N	N	Y
KNAS18436-E	Y	N	N	Y
KNAS18437-E	Y#	N	N	Y
KNAS18438-E	Y#	N	N	Y
KNAS18439-E	Y	N	N	Y
KNAS18440-E	Y	N	N	Y
KNAS18441-E	Y	N	N	Y
KNAS18442-E	Y	N	N	Y
KNAS18443-E	Y	N	N	Y
KNAS18444-E	Y	N	N	Y
KNAS18445-E	Y	N	N	Y
KNAS18446-E	Y	N	N	Y
KNAS18447-E	Y	N	N	Y
KNAS18448-E	Y	N	N	Y
KNAS18449-E	Y	N	N	Y
KNAS18450-E	Y	N	N	Y
KNAS18451-E	Y	N	N	Y
KNAS18500-E	Y#	N	N	Y
KNAS18501-E	Y	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS18502-E	Y	N	N	Y
KNAS18600-E	Y#	N	N	Y
KNAS18601-E	Y	N	N	Y
KNAS18602-E	Y	N	N	Y
KNAS18610-E	Y#	N	N	Y
KNAS18611-E	Y	N	N	Y
KNAS18612-E	Y	N	N	Y
KNAS18700-E	Y#	N	N	Y
KNAS18701-E	Y	N	N	Y
KNAS18702-E	Y	N	N	Y
KNAS18703-E	Y	N	N	Y
KNAS18800-E	Y#	N	N	Y
KNAS18801-E	Y	N	N	Y
KNAS18802-E	Y	N	N	Y
KNAS18803-E	Y	N	N	Y
KNAS18804-E	Y	N	N	Y
KNAS18805-E	Y	N	N	Y
KNAS18900-I	N	N	N	Y
KNAS18901-E	Y#	N	N	Y
KNAS18902-E	Y	N	N	Y
KNAS18903-E	Y	N	N	Y
KNAS18904-E	Y	N	N	Y
KNAS18905-E	Y	N	N	Y
KNAS18906-E	Y	N	N	Y
KNAS18907-E	Y	N	N	Y
KNAS18908-E	Y	N	N	Y
KNAS30022-I	N	N	N	Y
KNAS30023-I	N	N	N	Y
KNAS30024-E	N	N	N	Y
KNAS30025-I	N	N	N	Y
KNAS30026-E	N	N	N	Y
KNAS32003-W	N	N	N	Y
KNAS32004-W	N	N	N	Y
KNAS32007-W	N	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS32017-I	N	N	N	Y
KNAS32018-I	N	N	N	Y
KNAS32019-I	N	N	N	Y
KNAS32020-I	N	N	N	Y
KNAS32021-E	N	N	N	Y
KNAS32022-W	N	N	N	Y
KNAS32023-I	N	N	N	Y
KNAS32024-I	N	N	N	Y
KNAS32025-I	N	N	N	Y
KNAS32026-I	N	N	N	Y
KNAS32027-I	N	N	N	Y
KNAS32028-W	N	N	N	Y
KNAS32029-W	N	N	N	N
KNAS34000-W	N	N	N	N
KNAS34001-E	N	N	N	N
KNAS34002-W	N	N	N	N
KNAS34003-E	N	N	N	Y
KNAS34004-W	N	N	N	Y
KNAS34005-W	N	N	N	Y
KNAS34006-E	N	N	N	Y
KNAS34007-I	N	N	N	Y
KNAS34008-E	N	N	N	Y
KNAS34009-W	N	N	N	Y
KNAS34010-W	N	N	N	Y
KNAS50100-W	N	N	N	Y
KNAS50102-W	N	N	N	Y
KNAS50103-E	N	N	N	Y
KNAS50104-E	N	N	N	Y
KNAS50105-E	N	N	N	Y
KNAS50106-E	N	N	N	Y
KNAS50107-E	N	N	N	Y
KNAS50108-E	N	N	N	Y
KNAS50109-E	N	N	N	Y
KNAS50110-E	N	N	N	Y

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS50200-I	N	N	N	Y
KNAS50201-E	N	N	N	Y
KNAS50202-E	N	N	N	Y
KNAS50204-E	N	N	N	Y
KNAS50205-E	N	N	N	Y
KNAS50206-I	N	N	N	Y
KNAS50207-E	N	N	N	Y
KNAS50220-I	N	N	N	Y
KNAS50221-E	N	N	N	Y
KNAS50222-E	N	N	N	Y
KNAS50224-E	N	N	N	Y
KNAS50225-E	N	N	N	Y
KNAS50226-I	N	N	N	Y
KNAS50227-E	N	N	N	Y
KNAS50241-E	N	N	N	Y
KNAS50242-E	N	N	N	Y
KNAS50243-E	N	N	N	Y
KNAS70007-E	N	N	N	Y
KNAS70008-E	N	N	N	Y
KNAS90000-E	N	N	N	N
KNAS90001-E	N	N	N	N
KNAS90002-E	N	N	N	N
KNAS90003-E	N	N	N	N
KNAS90004-E	N	N	N	N
KNAS90005-E	N	N	N	N
KNAS90006-E	N	N	N	N
KNAS90007-E	N	N	N	N
KNAS90008-E	N	N	N	N
KNAS90009-E	N	N	N	N
KNAS90010-E	N	N	N	N
KNAS90011-I	N	N	N	N
KNAS90012-I	N	N	N	N
KNAS90013-E	N	N	N	N
KNAS90014-E	N	N	N	N

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS91000-I	N	N	N	Y
KNAS91001-I	N	N	N	Y
KNAS91002-I	N	N	N	Y
KNAS91020-E	N	N	N	Y
KNAS91021-E	N	N	N	Y
KNAS91022-E	N	N	N	Y
KNAS91023-E	N	N	N	Y
KNAS91024-E	N	N	N	Y
KNAS91025-E	N	N	N	Y
KNAS91026-E	N	N	N	Y
KNAS91027-E	N	N	N	Y
KNAS91028-E	N	N	N	Y
KNAS91029-E	N	N	N	Y
KNAS91030-E	N	N	N	Y
KNAS91031-E	N	N	N	N
KNAS91032-E	N	N	N	Y
KNAS91033-E	N	N	N	Y
KNAS91100-I	N	N	N	N
KNAS91120-E	N	N	N	Y
KNAS91121-E	N	N	N	Y
KNAS91200-I	N	N	N	N
KNAS91220-E	N	N	N	Y
KNAS91221-E	N	N	N	Y
KNAS91223-E	N	N	N	Y
KNAS91224-E	N	N	N	Y
KNAS91225-E	N	N	N	Y
KNAS91226-E	N	N	N	Y
KNAS91227-E	N	N	N	Y
KNAS91228-E	N	N	N	Y
KNAS91300-I	N	N	N	N
KNAS91301-E	N	N	N	Y
KNAS91400-I	N	N	N	Y
KNAS99000-I	N	N	N	N
KNAS99001-E	N	N	N	N

ID	Message destination			
	On screen	Event log	Integrated trace log	Message log
KNAS99002-E	N	N	N	N
KNAS99003-E	N	N	N	N
KNAS99013-E	N	N	N	N
KNAS99050-I	N	N	N	N
KNAS99051-E	N	N	N	N
KNAS99052-E	N	N	N	N
KNAS99053-E	N	N	N	N
KNAS99054-E	N	N	N	N
KNAS99055-W	N	N	N	N
KNAS99056-E	N	N	N	N
KNAS99057-E	N	N	N	N
KNAS99058-W	N	N	N	N
KNAS99059-E	N	N	N	N
KNAS99060-E	N	N	N	N
KNAS99061-W	N	N	N	N
KNAS99062-W	N	N	N	N

Legend:

Y: Message is output.

N: Message is not output.

#

When this message is output, processing is suspended and the login window is redisplayed.

11.3 Messages

KNAS02000-I

ITSLM - *aa....aa* has started.

aa....aa: Product category (`Manager` or `UR`)

KNAS02001-I

ITSLM - *aa....aa* has ended.

aa....aa: Product category (`Manager` or `UR`)

KNAS02002-E

ITSLM - *aa....aa* has ended abnormally.

aa....aa: Product category (`Manager` or `UR`)

(S)

Suspends processing.

(O)

Collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS02003-I

The service status of ITSLM - *aa....aa* was set to "Starting".

aa....aa: Product category (`Manager` or `UR`)

KNAS02004-I

The service status of ITSLM - *aa....aa* was set to "Running".

aa....aa: Product category (`Manager` or `UR`)

KNAS02005-I

The service status of ITSLM - *aa....aa* was set to "Stopping"

aa....aa: Product category (`Manager` or `UR`)

KNAS02006-I

The service status of ITSLM - *aa....aa* was set to "Stopped".

aa....aa: Product category (`Manager` or `UR`)

KNAS02007-I

An ITSLM - *aa....aa* service has started.

aa....aa: Product category (`Manager`)

KNAS02008-I

An ITSLM - *aa....aa* service has stopped.

aa....aa: Product category (`Manager`)

KNAS02009-E

An ITSLM - *aa....aa* service has not started due to an error.

aa....aa: Product category (`Manager`)

Description

Because an error has occurred in ITSLM - Manager, the services that comprise ITSLM - Manager have stopped.

(S)

Suspends processing.

(O)

Restart the services that comprise ITSLM - Manager. If this does not resolve the problem, contact a system administrator.

KNAS02010-E

ITSLM - *aa....aa* has expired.

aa....aa: Product category (`Manager` or `UR`)

Description

The trial version has expired.

(S)

Suspends processing.

(O)

Please use the full product version.

KNAS02025-E

Shared memory access has failed.

Description

Shared memory has not been created yet.

(S)

Suspends processing.

(O)

Contact a system administrator.

KNAS02035-E

An ITSLM - *aa....aa* process was killed. *bb....bb*=*cc....cc*

aa....aa: Product category (`Manager` or `UR`)

bb....bb: `GetExitCodeProcess`

cc....cc: Error code

(S)

Suspends processing.

(O)

Check the integrated trace log and message log, take any necessary corrective action, and then restart the ITSLM - Manager or ITSLM - UR services. Contact a system administrator if the problem reoccurs.

KNAS02036-E

Process recovery for ITSLM - *aa....aa* has failed.

aa....aa: Product category (`Manager` or `UR`)

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service.

KNAS02043-I

Monitoring of an ITSLM - *aa....aa* process will be started.

aa....aa: Product category (`Manager` or `UR`)

KNAS02089-I

The process was restarted. process name=*aa....aa*

aa....aa: Process name (`jslmmpcollect`, `jslmmengine`, `jslmmUR`, `jslmmRMI`, `cjstartweb`, `jslmuengine`, `jslmuUR`, `jslmuRMI`, `jslmmdao`, or `jslmmadaptor`)

KNAS02090-I

The system will wait for *bb....bb* seconds for the JP1/ITSLM - *aa....aa* service to start.

aa....aa: Product category (`Manager` or `UR`)

bb....bb: Wait time (seconds)

KNAS02091-E

The starting of a JP1/ITSLM - *aa....aa* service has failed, as no embedded database was started.

aa....aa: Product category (`Manager`)

Description

- Non-cluster operation:

  The ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is not running.

- Cluster operation:

  The ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) or **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`) has not been started.

(S)

Suspends processing.

(O)

Start the ITSLM - Manager service **JP1/ITSLM - Manager DB Service**. If you are running in a cluster system, also start the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service**.

KNAS02092-W

A JP1/ITSLM - *aa....aa* service was stopped.

aa....aa: Product category (`Manager` or `UR`)

Description

There was a stop request during start processing of the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) or the ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`).

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service.

KNAS02094-E

An error occurred during the checking of the product information registration file.

(S)

Suspends processing.

(O)

Collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS02095-E

A process stopped. process name=*aa....aa*

aa....aa: Process name (`jslmmpcollect`, `jslmmengine`, `jslmmUR`, `jslmmRMI`, `cjstartweb`, `jslmuengine`, `jslmuUR`, `jslmuRMI`, `jslmmdao`, or `jslmmadaptor`)

Description

The process terminated abnormally.

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service.

KNAS02099-E

The stopping of a process timed out. process name=*aa....aa*

aa....aa: Process name (`jslmmpcollect`, `jslmmengine`, `jslmmUR`, `cjstartweb`, `jslmuengine`, `jslmuUR`, `jslmmdao`, or `jslmmadaptor`)

Description

Stop processing for the *aa....aa* process timed out.

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service.

KNAS02102-I

The starting of a process is complete. process name=*aa....aa*

aa....aa: Process name (`jslmmpcollect`, `jslmmengine`, `jslmmRMI`, `jslmmUR`, `cjstartweb`, `jslmuengine`, `jslmuRMI`, `jslmuUR`, `jslmmdao`, or `jslmmadaptor`)

KNAS02118-E

An insufficient memory error occurred while attempting to allocate *aa....aa* bytes of memory.

aa....aa: Number of bytes

(S)

Suspends processing.

(O)

Exit ITSLM - Manager or ITSLM - UR, and then restart after allocating sufficient memory. Contact a system administrator if the problem reoccurs.

KNAS02119-E

The command process could not be started. command=*aa....aa*, *bb....bb*=*cc....cc*

aa....aa: Command

bb....bb: `GetLastError`

cc....cc: Error code

(S)

Suspends processing.

(O)

Uninstall ITSLM - Manager, and then repeat the installation and setup. Contact a system administrator if the problem reoccurs.

KNAS02120-E

The command process ended due to an error. command=*aa....aa*, *bb....bb*=*cc....cc*

aa....aa: Command

bb....bb: `GetLastError`

cc....cc: Error code

(S)

Suspends processing.

(O)

Check the subsequent message. Or, run unsetup on ITSLM - Manager, and then run setup again. Contact a system administrator if the problem reoccurs.

KNAS02121-E

Preparation for environment information (*aa....aa*) acquisition failed. *bb....bb*=*cc....cc*

aa....aa: `ProgramName` (registry name)

bb....bb: `errno`

cc....cc: Error code

(S)

Suspends processing.

(O)

Run unsetup on ITSLM - Manager or ITSLM - UR, and then run setup again. Contact a system administrator if the problem reoccurs.

KNAS02125-W

System Error occurred while starting JP1/ITSLM - *aa....aa* service.

aa....aa: Product category (`Manager` or `UR`)

Description

An attempt to initialize the log failed.

(S)

Continues processing.

(O)

Collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS02126-W

A default value was assumed because the system failed to obtain the set value from a properties file. Check the set value. If the value is changed, restart the ITSLM - *aa....aa* service. properties file name=*bb....bb*, property key=*cc....cc*

aa....aa: Product category (`Manager` or `UR`)

bb....bb: Name of the properties file (system definition file) whose default values were assumed

cc....cc: Name of the property key (system definition file property) whose default value was assumed

(S)

Uses the default value due to the failure to obtain a setting in the system definition file.

(O)

Check the settings in the system definition file. Or, check the integrated trace log. For details about the integrated trace log, see *7.2.2 Integrated trace logs*.

If you change the default value that was assumed, restart the ITSLM - Manager or ITSLM - UR service that was the target of the change.

KNAS02127-I

The trial version of ITSLM - *aa....aa* is starting. number of days for the trial to expire=*bb....bb*

aa....aa: Product category (`Manager` or `UR`)

bb....bb: Number of days remaining until the trial period expires

KNAS02128-E

An insufficient memory error occurred.

(S)

Suspends processing.

(O)

Exit ITSLM - Manager or ITSLM - UR, allocate memory, and then restart. Contact a system administrator if the problem reoccurs.

KNAS02129-E

The ITSLM - *aa....aa* runtime environment is not for version *bb....bb*. Complete the setup and then start the ITSLM - *aa....aa* services.

aa....aa: Product category (`Manager` or `UR`)

bb....bb: Version of ITSLM - *aa....aa*

Description

Setup has not been completed.

(S)

Suspends processing.

(O)

Stop ITSLM, complete the setup, and then start ITSLM again.

KNAS03004-E

An error occurred while writing data to the database, following ITSLM - UR start notification.

(S)

Suspends processing of writing data into the database for ITSLM - UR startup notification.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS03005-E

An error occurred while deleting data from the database, following ITSLM - UR stop notification.

(S)

Suspends processing of deleting data from the database for ITSLM - UR stop notification.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS03007-E

A communication error occurred between the ITSLM - UR and the ITSLM - Manager. destination IP address=*aa....aa*, destination port number=*bb....bb*

aa....aa: Destination IP address

bb....bb: Destination port number

Description

A communication error has occurred for one of the following reasons:

- An attempt to retry startup or termination notification from ITSLM - UR to ITSLM - Manager, in accordance with the `announceRetryCount` and `announceRetryInterval` properties in the ITSLM - UR `jp1itslmur.properties` system definition file, failed.
- An attempt to retry communication between ITSLM - Manager and ITSLM - UR, in accordance with the `communicationRetryCount` and `communicationRetryInterval` properties in the ITSLM - Manager or ITSLM - UR `jp1itslm.properties` or `jp1itslmur.properties` system definition file, failed.

(S)

Suspends processing.

(O)

Make sure ITSLM - Manager or ITSLM - UR is running. If it is running, check and, if necessary, revise the following property values specified in a system definition file:

- `managerHost` (`jp1itslm.properties` or `jp1itslmur.properties`)

- `rmiManagerPort` (`jp1itslm.properties` or `jp1itslmur.properties`)
- `urHost` (`jp1itslmur.properties`)
- `rmiUrPort` (`jp1itslmur.properties`)

KNAS03016-W

The system will retry the operation, as a communication error has occurred. time to retry (seconds)=*aa....aa*

aa....aa: Time remaining until retry (in seconds)

(S)

Retries communication processing.

KNAS03020-E

An error occurred while referencing the services monitored by the ITSLM - UR. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of ITSLM - UR

Description

An error occurred while referencing an ITSLM - UR monitored service.

(S)

Suspends data reference processing to the database for ITSLM - UR startup notification.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS03022-I

A start notification was sent to the ITSLM - Manager. ITSLM - Manager IP address=*aa....aa*

aa....aa: IP address of the startup notification destination ITSLM - Manager

KNAS03023-I

A stop notification was sent to the ITSLM - Manager. ITSLM - Manager IP address=*aa....aa*

aa....aa: IP address of the stop notification destination ITSLM - Manager

KNAS03024-I

An ITSLM - UR start notification was received. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of the startup notification source ITSLM - UR

KNAS03025-I

An ITSLM - UR stop notification was received. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of the stop notification source ITSLM - UR

KNAS03026-I

A start notification was canceled, as the system could not confirm the start of ITSLM - UR. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of the ITSLM - UR whose startup notification was canceled

(S)

Continues processing.

(O)

Check the status of the ITSLM - UR service.

If the status of the service is stopped, determine whether it was stopped correctly, and then start ITSLM - UR if necessary.

If the status of the service is started, restart ITSLM - UR.

KNAS03027-E

Database update failed while starting the ITSLM - Manager.

(S)

Suspends processing.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS03028-E

A communication error occurred while starting the ITSLM - Manager.

(S)

Suspends processing.

(O)

Restart the services that comprise ITSLM - Manager. If this does not resolve the problem, collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS03029-W

Performance data transmission failed, as the system could not connect to the ITSLM - Manager.

Description

A retry attempt in accordance with the `communicationRetryCount` and `communicationRetryInterval` properties failed because ITSLM - Manager was in the process of starting or stopping.

The following are possible causes:

- The connection failed because ITSLM - Manager was in the process of starting or stopping.
- There is an error in the value specified for the `managerHost` or `rmiManagerPort` property.

(S)

Suspends processing.

(O)

Confirm the following:

- ITSLM - Manager is running.
- The values specified for the `managerHost` and `rmiManagerPort` properties are correct.

KNAS03030-E

An attempt to create a thread for the access log function failed.

Description

An attempt to create a thread for outputting log files failed.

(S)

Suspends processing.

(O)

Restart the ITSLM-UR service.

KNAS03031-E

An attempt to create the path specified for accessLogFilePath failed. accessLogFilePath=*aa....aa*

aa....aa: Path specified for `accessLogFilePath`

Description

An attempt to create the path specified for `accessLogFilePath` in the ITSLM - UR system definition failed.

(S)

Suspends processing.

(O)

Create the path that was specified for `accessLogFilePath` in the ITSLM - UR system definition, and then restart the ITSLM - UR service.

KNAS03032-E

An attempt to create an http folder under the path that has been specified for accessLogFilePath failed. accessLogFilePath=*aa....aa*

aa....aa: Path specified for `accessLogFilePath`

Description

An attempt to create a folder named `http` under the path that has been specified for `accessLogFilePath` failed.

(S)

Suspends processing.

(O)

Create a folder named `http` under the path specified for `accessLogFilePath` in the ITSLM - UR system definition, and then restart the ITSLM - UR service.

KNAS03033-W

An attempt to delete the folder for the access log failed. folder name=*aa....aa*

aa....aa: Name of the folder that was not deleted

Description

An attempt to delete the folder for the access log failed.

(S)

Continues processing.

(O)

Delete the folder that was not deleted.

KNAS03034-W

An attempt to change the output destination for the access log file failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An attempt to change the output destination for the access log file failed.

(S)

Continues processing without being able to display access logs for the interval over which the service failed.

(O)

If you want to resume access log output, restart the ITSLM-UR service.

KNAS03035-W

An attempt to write to the access log file failed. service group name=*aa....aa*, service name=*bb....bb*, file name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the access log file

Description

An attempt to write to the access log file failed.

(S)

Continues processing without being able to display access logs for the interval over which the service failed.

(O)

Make sure the access log file exists and that the write permissions are correct. If this does not resolve the problem, contact a system administrator.

KNAS03036-I

> The access log for the requested time does not exist. service group name=*aa....aa*, service name=*bb....bb*, start time=*cc....cc*, range=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Start time

dd....dd: Range (minutes)

Description

The access log for the specified time does not exist. No access logs are displayed.

KNAS03037-I

> The time currently being acquired is included in the requested time. The access log that is being acquired cannot be displayed. service group name=*aa....aa*, service name=*bb....bb*, start time=*cc....cc*, range=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Start time

dd....dd: Range (minutes)

Description

The time currently being acquired is included in the specified time. The access logs that are displayed exclude the access log that is currently being acquired.

KNAS03038-E

> The file that links the access log file and services cannot be accessed. file name=*aa....aa*

aa....aa: Name of the access log file

Description

The file that links the access log file and services cannot be accessed.

No access log file could be found for the corresponding service.

(S)

Suspends processing.

(O)

Check the read permissions to the paths under the path specified in `accessLogFilePath`, and then restart the ITSLM-UR service. If this does not resolve the problem, contact a system administrator.

KNAS03039-E

> The file that links the access log file and services cannot be created. file name=*aa....aa*

aa....aa: Name of the access log file

Description

The file that links the access log file and services cannot be created.

(S)

- When ITSLM - UR is starting:
  Suspends processing.
- When access logs are being output:
  Continues processing.

(O)

Check the write permissions to the paths under the path specified in `accessLogFilePath`, and then restart the ITSLM-UR service. If this does not resolve the problem, contact a system administrator.

KNAS03040-W

The file that links the access log file and services cannot be updated. file name=*aa....aa*

aa....aa: Name of the access log file

Description

The file that links the access log file and services cannot be updated.

(S)

- When ITSLM - UR is starting:
  Suspends processing.
- When access logs are being output:
  Continues processing.

(O)

Check the write permissions to the paths under the path specified in `accessLogFilePath`. Set or acquire the correct permissions if necessary. If this does not resolve the problem, contact a system administrator.

KNAS03041-W

An attempt to create the folder for the access log failed. folder name=*aa....aa*

aa....aa: Name of the folder where the access logs are stored or the folder corresponding to the service

Description

An attempt to create one of the following folders failed:

- The total milliseconds folder for storing the access log files
- The folder corresponding to the service

(S)

Continues processing.

(O)

Check the write permissions to the paths under the path specified in `accessLogFilePath`. Set or acquire the correct permissions if necessary. If this does not resolve the problem, contact a system administrator.

KNAS03042-W

Access logs can no longer be output because the thread that outputs access logs was stopped.

Description

A failure occurred in the thread that outputs access logs to a file and the thread was stopped.

(S)

Continues processing after stopping output of the access logs.

(O)

If you want to resume access log output, restart the ITSLM-UR service.

KNAS03044-E

An attempt to read the access log failed. (access log file name=*aa....aa*)

aa....aa: Name of the access log file

Description

An attempt to read the access log failed.

(S)

Continues processing.

(O)

If the access log file is not required, delete it.

KNAS05000-E

JP1 event issuance failed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, reason code=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Reason code

Description

The reason codes have the following meanings:

- `DUPLICATE`: A JP1 extended event attribute is duplicated.
- `IOERROR`: An I/O error occurred.
- `OVERFLOW`: A JP1 extended event attribute has exceeded the size limit.
- `PARAM`: An invalid value was specified for a JP1 event attribute.
- `SEQUENCE`: The connection with the event server was closed.
- `SERVER`: The event server is not running, or an error occurred in the event server.

(S)

ITSLM - Manager continues processing.

(O)

Take corrective action based on the reason codes as shown below. To resume notification of JP1 events, stop the monitoring of the monitored service and restart monitoring.

- `DUPLICATE`, `OVERFLOW`, `PARAM`, or `SEQUENCE`
  Contact a system administrator.
- `IOERROR` or `SERVER`
  Confirm that the JP1/Base event server is running. If this does not resolve the problem, contact a system administrator.

KNAS09000-E

Initialization for log acquisition has failed. method name=*aa....aa*, return code=*bb....bb*, output trace file path=*cc....cc*

aa....aa: Name of the method that failed to initialize

bb....bb: Return code of the method that failed to initialize

cc....cc: Log file path for the initialization failure (for integrated trace, the character string `SysLog`)

(S)

The system environment is incorrect, but ITSLM - Manager or ITSLM - UR continues processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service. If this does not resolve the problem, contact a system administrator.

KNAS09001-E

OS common log output has failed. message ID=*aa....aa*

aa....aa: ID of the message that failed to be output to the common OS log

(S)

The system environment is incorrect, but ITSLM - Manager or ITSLM - UR continues processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service. If this does not resolve the problem, contact a system administrator.

KNAS09002-E

The loading of a properties file has failed. properties file name=*aa....aa*

aa....aa: Name of the properties file (system definition file) that failed to be read

(S)

Terminates processing of ITSLM - Manager or ITSLM - UR due to an incorrect system environment.

(O)

Confirm that the properties file (system definition file) exists, and that you have read permission for it.

KNAS09003-E

Property acquisition has failed. properties file name=*aa....aa*, property key=*bb....bb*

aa....aa: Name of the failed properties file (system definition file)

bb....bb: Name of the failed property key (system definition file property)

Description

A required property is not specified.

(S)

Terminates processing of ITSLM - Manager or ITSLM - UR due to an incorrect system environment.

(O)

Check the value specified for the property.

KNAS09004-E

A properties file contains an incorrect set value. Check the set value. If the value is changed, restart the ITSLM - Manager services. properties file name=*aa....aa*, property key=*bb....bb*

aa....aa: Name of the failed properties file (system definition file)

bb....bb: Name of the failed property key (system definition file property)

(S)

Terminates processing of ITSLM - Manager due to an incorrect system environment.

(O)

Check the specified value of the property.

KNAS09005-W

A default value was assumed because the system failed to obtain the set value from a properties file. Check the set value. If the value is changed, restart the ITSLM - Manager services. properties file name=*aa....aa*, property key=*bb....bb*

aa....aa: Name of the properties file (system definition file) from which the default value was assumed

bb....bb: Name of the properties key (system definition file property) whose default value was assumed

(S)

Uses the default value due to the failure to obtain a setting in the system definition file.

(O)

Check the settings in the system definition file. Or, check the integrated trace log. For details about the integrated trace log, see *7.2.2 Integrated trace logs*.

If you change the assumed value, restart the services that comprise ITSLM - Manager.

KNAS09007-E

RMI registry registration has failed.

Description

An attempt to register into the RMI registry failed for one of the following reasons:

- A network failure occurred.
- RMI server has not started.

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service. If this does not resolve the problem, contact a system administrator.

KNAS09008-E

RMI registry registration has failed.

Description

An attempt to remove registration in the RMI registry failed for one of the following reasons:

- A network failure occurred.
- RMI server has not started.
- Remote object has not been registered.

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service. If this does not resolve the problem, contact a system administrator.

KNAS09009-E

RMI call has failed.

Description

An attempt to call RMI failed for one of the following reasons:

- A network failure occurred.
- RMI server has not started.
- Remote object has not been registered.

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager or ITSLM - UR service. If this does not resolve the problem, contact a system administrator.

KNAS09014-E

A properties file contains an incorrect set value. Check the set value. If the value is changed, restart the ITSLM - UR services. properties file name=*aa....aa*, property key=*bb....bb* *aa....aa*: Name of the invalid properties file (system definition file)

bb....bb: Name of the invalid property key (system definition file property)

(S)

Terminates processing of ITSLM - UR due to an incorrect system environment.

(O)

Check the specified value of the property.

KNAS09015-W

A default value was assumed because the system failed to obtain the set value from a properties file. Check the set value. If the value is changed, restart the ITSLM - UR services. properties file name=*aa....aa*, property key=*bb....bb*

aa....aa: Name of the properties file (system definition file) from which the default value was assumed

bb....bb: Name of the properties key (system definition file property) whose default value was assumed

(O)

Check the settings in the system definition file. Or, check the integrated trace log. For details about the integrated trace log, see *7.2.2 Integrated trace logs*.

If you change the default value that was assumed, restart the ITSLM - UR service.

KNAS09016-E

The starting of the RMI server has failed. details=*aa....aa*

aa....aa: Exception information message

Description

A `RemoteException` exception occurred in the execution of `LocateRegistry.createRegistry()`.

(S)

Suspends processing.

(O)

Determine the cause from the information, take corrective action, and then restart the ITSLM - Manager or ITSLM - UR service.

KNAS09021-E

An error occurred while registering a remote object to the RMI server. maintenance information=*aa....aa*

aa....aa: URL of the remote object

Description

A `RemoteException` exception occurred in remote object registration processing (during execution of `java.rmi.Naming.rebind()`).

(S)

Suspends processing.

(O)

Revise the system definition file settings shown below, and then start the ITSLM - Manager or ITSLM - UR service. If this does not resolve the problem, contact a system administrator.

For ITSLM - Manager:

Revise the settings for the `managerHost` and `rmiManagerPort` properties in the `jp1itslm.properties` system definition file.

For ITSLM - UR:

Revise the settings for the `urHost` and `rmiUrPort` properties in the `jp1itslmur.properties` system definition file.

KNAS09022-E

The checking of set values in a properties file has failed. reason code=*aa....aa*, maintenance information=*bb....bb*

aa....aa: Reason code

bb....bb: Exception message

Description

While checking the settings in the properties file (system definition file), one of the following occurred:

- `IOException` occurred during execution of the `jslmuripls` command.
- `IOException` occurred when reading the output of the `jslmuripls` command.

(S)

Terminates processing of ITSLM - UR.

(O)

Take the corrective action shown below based on the reason code. If this does not resolve the problem, contact a system administrator.

- `COMMAND_FAILURE`: Make sure the person running the `jslmuripls` command has access permission.

KNAS09023-E

The process will be stopped, as the number of error occurrences has exceeded the upper limit. error type=*aa....aa*, number of occurrences=*bb....bb*

aa....aa: Error type

bb....bb: Number of errors that occurred

Description

The number of errors that occurred has exceeded the limit.

The error types have the following meanings:

- `COMMUNICATION`: Communication errors have exceeded the maximum number of error occurrences.
- `DATABASE`: Database access errors have exceeded the maximum number of error occurrences.

(S)

Stops the process in which the errors occurred.

(O)

Check the messages output to the message log, take corrective action, and then start the services that comprise ITSLM - UR or ITSLM - Manager.

KNAS09100-E

The establishment of a connection to the database has failed.

Description

The attempt to establish connection with the database failed.

(S)

Terminates processing of ITSLM - Manager.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS10000-I

The manual cannot be located.

(O)

Install the manual.

For details, see *5.1.8 Installing the HTML manual*.

KNAS10001-E

Connection to the ITSLM - Manager has failed.

Description

An attempt to communicate with ITSLM - Manager failed.

(S)

Suspends processing.

(O)

Check that the communications environment with ITSLM - Manager is normal and that ITSLM - Manager has started successfully.

If you want to close the browser or close the browser tab in which this window was opened, press the **OK** button on the dialog box that is displayed. If you want to retry the connection to ITSLM - Manager, press the **Cancel** button.

KNAS10002-Q

Do you want to log out?

KNAS10003-I

The maximum allowable number of selections has been exceeded. maximum allowable number of selections=*aa....aa*

aa....aa: Maximum number that can be selected

Description

The number of items selected by the user at the client exceeds the maximum value.

(S)

Discards the selections.

(O)

Re-select items without selecting unneeded items.

KNAS11400-I

A system performance monitor item was deleted. The screen will be refreshed.

Description

A system performance monitoring item has been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent system performance information.

KNAS11500-I

A monitor item being displayed on the performance chart was deleted. The screen will be refreshed.

Description

A monitoring item in a performance chart has been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent service configuration information.

KNAS11600-Q

Do you want to output the CSV file?

KNAS11601-E

CSV file output has failed.

Description

This is an error in the environment at the machine to which you are trying to output to a CSV file. Factors to consider include the following:

- Insufficient disk space
- No write permission

(S)

Suspends processing.

(O)

Check for problems such as the following in the environment of the machine to which you are trying to output to a CSV file:

- Insufficient disk space
- No write permission

Because the file might be incomplete, it is recommended that you delete the CSV file that was output.

KNAS11602-W

The output of the CSV was canceled.

Description

Output of the CSV file was suspended for one of the following reasons:

- Cancel was selected in the dialog box when the CSV file was output.
- A forced cancellation was executed on the machine to which you are trying to output the CSV file.

(S)

Suspends processing.

KNAS11603-I

The template was registered successfully.

KNAS11604-Q

Do you want to save the edited template?

KNAS11605-I

The edited template was saved successfully.

KNAS11606-Q

Do you want to delete the template?

KNAS11607-I

The template was deleted successfully.

KNAS11700-I

The selected service was registered successfully.

KNAS11701-Q

Do you want to delete the selected service?

KNAS11702-I

The selected service was deleted successfully.

KNAS11703-I

The monitor settings were registered.

KNAS11704-I

The Web transaction was registered successfully.

KNAS11705-Q

Do you want to delete the selected Web transaction?

KNAS11706-I

The selected Web transaction was deleted successfully.

KNAS11707-Q

Do you want to delete the Web access condition?

KNAS11708-Q

Do you want to delete all available URIs?

KNAS11709-Q

Do you want to delete the selected line?

KNAS11710-I

No more Web access conditions can be added, as the upper limit on the number of conditions has been reached.

KNAS11711-E

The Web access condition cannot be added, as the same condition has already been registered.

Description

The same Web access condition is already registered.

(S)

Suspends processing.

(O)

Modify the Web access condition and try again.

KNAS11712-I

The Web transaction was edited successfully.

KNAS11713-Q

The URI of the service does not end with "/". Its full path will be registered as a monitored target. Do you want to proceed to the registration?

KNAS11714-Q

The stopping of service monitoring has failed. Do you want to force the stopping of service monitoring?

KNAS11715-I

The configuration information was refreshed successfully.

KNAS11716-I

The availability monitor settings were saved successfully.

KNAS11717-I

The system performance monitor settings were saved successfully.

KNAS11718-Q

Do you want to save the availability monitor settings?

KNAS11719-Q

Do you want to save the system performance monitor settings?

KNAS11720-E

The selected monitor item cannot be added, as a different monitor item having the same values for all key fields already exists.

Description

There is a row with all the same key field values.

(S)

Suspends processing.

(O)

Check and, if necessary, revise the values of the key fields, and then try again.

KNAS15000-I

A service was deleted by a different user. The screen will be refreshed.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS15001-E

An error occurred, making it impossible to continue.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15005-E

Initialization of the JP1/ITSLM - Manager service has failed.

(S)

Suspends processing and returns to the login window.

(O)

Check the message log. If an error message was output immediately before this message, take corrective action according to that message.

If this message is output again, contact a system administrator.

KNAS15006-E

The session with the ITSLM - Manager has become invalid.

Description

The session is no longer valid for one of the following reasons:

- The ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) has restarted.
- The session has timed out.

(S)

Suspends processing and returns to the login window.

(O)

Log in again.

KNAS15007-E

An insufficient memory error occurred in the Web container server.

(S)

Suspends processing and returns to the login window.

(O)

Stop the services that comprise ITSLM - Manager, allocate memory, and then restart. If this does not resolve the problem, contact a system administrator.

KNAS15008-E

The specified regular expression is invalid. type=*aa....aa*, regular expression=*bb....bb* *aa....aa*: Type

bb....bb: Regular expression

Description

The possible types indicated by *aa....aa* are as follows:

- `path`: Path
- `query`: Query
- `cookie`: Cookie

(S)

Suspends processing.

(O)

Check and, if necessary, revise the regular expression.

KNAS15009-I

A Web transaction was deleted by a different user. The screen will be refreshed.

(S)

Refreshes the window.

(O)

Check the updated services.

To see which Web transactions have changed, check the message log.

KNAS15300-I

A user is now logged in. user name=*aa....aa*

aa....aa: User name

KNAS15301-E

Login has failed. The user name or password is incorrect.

(S)

Suspends processing and returns to the login window.

(O)

Log in by entering the JP1 user name and password registered on the authentication server for the connection destination.

KNAS15302-E

Login has failed. The system cannot connect to JP1/Base.

Description

An attempt to log in failed for one of the following reasons:

- JP1/Base is not running.
- A communications failure occurred.

(S)

Suspends processing and returns to the login window.

(O)

After starting JP1/Base, restart the services that comprise ITSLM - Manager.

KNAS15304-E

Login has failed. maintenance information=*aa....aa*

aa....aa: Error type

Description

An error occurred during the login process.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15305-E

Login has failed. maintenance information 1=*aa....aa*, maintenance information 2=*bb....bb*

aa....aa: Error type

bb....bb: Return code

Description

An error occurred during the login process.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15306-I

Initialization for the user authentication function of JP1/Base was performed.

KNAS15307-E

Initialization for the user authentication function of JP1/Base has failed. reason code=*aa....aa*, maintenance information=*bb....bb*

aa....aa: Reason code

bb....bb: Error type

Description

The reason codes have the following meanings:

- `NO_JBSHOST`: The specified authentication server does not exist, or the authentication server has not been set.

- JBSHOST_ENT: Authentication server definition information is incorrect.
- REMOTE: A communications error occurred.
- INTERNAL: An error other than the above occurred.

(S)

Suspends processing.

(O)

After taking the following corrective measure based on the reason code, restart the services that comprise ITSLM - Manager.

- NO_JBSHOST: Check and, if necessary, revise the setting for the jbsHostName property in the ITSLM - Manager jp1itslm.properties system definition file.
- JBSHOST_ENT: Check and, if necessary, revise the settings for the JP1/Base authentication server.
- REMOTE: Confirm that JP1/Base has started. If JP1/Base has not started, start it.
- INTERNAL: Contact a system administrator.

KNAS15308-E

Login has failed. The specified user has no permission to access the ITSLM. user name=*aa....aa*

aa....aa: User name

(S)

Suspends processing and returns to the login window.

(O)

Set ITSLM permissions for the JP1 user, and then log in again.

For details about setting permissions for JP1 users, see *5.2.3 Specifying operation permissions for each JP1 user*.

KNAS15309-E

Login has failed. An insufficient memory error occurred in the JP1/Base authentication server.

(S)

Suspends processing and returns to the login window.

(O)

Terminate other programs that are using memory on the JP1/Base authentication server, and then log in again.

KNAS15310-E

Login has failed. An error occurred while obtaining access permissions. maintenance information=*aa....aa*

aa....aa: Error type

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15311-E

> Initialization for the user authentication function of JP1/Base has failed. reason code=*aa....aa*, maintenance information 1=*bb....bb*, maintenance information 2=*cc....cc*

aa....aa: Reason code

bb....bb: Error type

cc....cc: Return code

Description

The reason codes have the following meanings:

- `INTERNAL`: An error occurred during initialization processing of the JP1/Base user authentication function.

(S)

Suspends processing.

(O)

Take the corrective action shown below based on the reason code.

- `INTERNAL`: Contact a system administrator.

KNAS15312-E

> Login has failed. An error occurred during a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS15313-E

> Login has failed. The user name or password is incorrect. The screen was locked, as the number of login failures reached the upper limit.

Description

The entered user name or password is not correct, and the number of failed login attempts has reached the maximum.

(S)

Locks the screen because the maximum number of login failures has been reached.

(O)

After refreshing the window, log in by entering a JP1 user name and password registered on the authentication server for the connection destination.

KNAS15400-I

> A user was logged out. user name=*aa....aa*

aa....aa: User name

KNAS15401-E

Logout has failed. The system cannot connect to JP1/Base.

Description

An attempt to log out failed for one of the following reasons:

- JP1/Base is not running.
- A communications failure occurred.

(S)

Suspends processing.

(O)

Start JP1/Base, and then restart the services that comprise ITSLM - Manager.

KNAS15403-E

Logout has failed. maintenance information=*aa....aa*

aa....aa: Error information

Description

An error occurred during logout processing.

(S)

Suspends processing.

(O)

Contact a system administrator.

KNAS15404-E

Logout has failed. maintenance information 1=*aa....aa*, maintenance information 2=*bb....bb*

aa....aa: Error type

bb....bb: Return code

Description

An error occurred during logout processing.

(S)

Suspends processing.

(O)

Contact a system administrator.

KNAS15405-I

A session timeout was detected. A logout will be performed. user name=*aa....aa*

aa....aa: User name

KNAS15500-I

> A service was registered. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS15501-E

> Service registration has failed. The specified service name is already registered in the same service group. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service name is already registered in the same service group. Each monitored service name in a service group must be unique.

(S)

Suspends processing.

(O)

Revise the name of the monitored service. Set a name for the monitored service that is not already registered within the same service group.

KNAS15502-E

> Service registration has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS15503-E

> Service registration has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem re-occurs, communication with ITSLM - UR might have failed. Check the message log (`UserResponseMessageM[n].log`). If there is no problem in the message log, restart the services that comprise ITSLM - Manager.

KNAS15504-E

> Service registration has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while processing registration of a service.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15505-E

> Service registration has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS15507-E

> Service registration has failed. An error occurred during database space allocation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An attempt to allocate database space for registering a monitored service failed.

(S)

Suspends processing.

(O)

Run the database cleanup command (`jslmmgrdbcleanup`) and try the operation again.

For details about the `jslmmgrdbcleanup` command, see *jslmmgrdbcleanup (cleans up database)* in *9. Commands*.

If the problem reoccurs after you have executed the database cleanup command (`jslmmgrdbcleanup`), there is not enough space in the database. Extend the database space, and then execute setup again.

KNAS15508-E

Service registration has failed. The ITSLM - UR version you are using to monitor the registered service cannot monitor a service by specifying its path. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*, version=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

dd....dd: Version of ITSLM - UR

(S)

Suspends processing.

(O)

Monitor the registered monitored service under ITSLM - UR version 09-51 or later.

KNAS15509-E

Service registration has failed. The ITSLM - UR version you are using to monitor the registered service cannot monitor a service by specifying its port. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*, version=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

dd....dd: Version of ITSLM - UR

Description

The monitored service for which the port was specified in the URI cannot be monitored in the version of ITSLM - UR which is to monitor the registered monitored service. For details about the URIs supported by ITSLM, see *(3) Supplemental notes* in *10.6.4 Add/Delete monitor area*.

(S)

Suspends processing.

(O)

Monitor the registered monitored service under ITSLM - UR version 09-51 or later.

KNAS15510-E

Service registration has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations cannot be executed on monitored services while detection is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS15511-E

Service registration has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS15600-I

A service was deleted. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS15601-E

Service deletion has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS15602-E

> Service deletion has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS15603-E

> Service deletion has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS15604-E

> Service deletion has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while processing deletion of a monitored service.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15605-E

> Service deletion has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting of at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS15607-E

> Service deletion has failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring of the specified monitored service is starting. A monitored service cannot be deleted while monitoring of it is starting.

(S)

Suspends processing.

(O)

Stop monitoring of the monitored service, and then retry the operation.

KNAS15608-E

> Service deletion has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations cannot be executed on monitored services while detection is being performed.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS15609-E

Service deletion has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS15712-I

A detection process was started. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

KNAS15713-E

The starting of a detection process has failed. During the processing for ITSLM - UR, an inter-process communication error occurred in the ITSLM - Manager. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart ITSLM - UR and the services that comprise ITSLM - Manager.

KNAS15714-E

The starting of a detection process has failed. An error occurred during the ITSLM - UR processing. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the messages output to the ITSLM - UR message log, and then take corrective action.

KNAS15715-E

The starting of a detection process has failed. A communication error occurred between the ITSLM - UR and the ITSLM - Manager. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the relevant ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the communication environment between ITSLM - UR and ITSLM - Manager. If there is a problem with the communication environment, restart the ITSLM - UR service and the services that comprise ITSLM - Manager.

KNAS15716-E

The starting of a detection process has failed. An error occurred during a database operation. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS15717-E

> The starting of a detection process has failed. The processing timed out. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS15718-E

> The starting of a detection process has failed. The operation cannot be performed, as monitoring, or a detection process by a different user, is in progress. If there are services being monitored, stop all monitoring and then retry. If there is no service being monitored, wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

There are monitored services being monitored, or another user is performing detection. A detection operation cannot be executed while monitoring or other detection is being performed.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

If there are monitored services being monitored, stop all monitoring, and then retry the operation. If no monitored services are being monitored, wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS15719-W

In the starting of a detection process, errors have occurred during the processing of one or more ITSLM - UR instances. If the detection process encounters a problem, check whether the JP1/ITSLM - UR service is running normally. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Continues processing.

(O)

If detection cannot be executed, check whether ITSLM - UR started successfully.

KNAS15720-E

The starting of a detection process has failed. No available JP1/ITSLM - UR service exists. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Start the ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`).

KNAS15721-E

The starting of a detection process has failed. An inter-process communication error occurred in the ITSLM - Manager. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem re-occurs, communication with ITSLM - UR might have failed. Check the message log (`UserResponseMessageM[`*n*`].log`). If there is no problem in the message log, restart the services that comprise ITSLM - Manager.

KNAS15722-E

The starting of a detection process has failed. detection type=*aa....aa*

aa....aa: Type of detection

Description

An error occurred during detection startup processing.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15723-E

The starting of a detection process has failed. No available ITSLM - UR instance exists. Check whether the JP1/ITSLM - UR service is running normally. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Make sure ITSLM - UR started successfully.

KNAS15810-I

A detection process was stopped. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

KNAS15811-E

The stopping of a detection process has failed. During the processing for ITSLM - UR, an inter-process communication error occurred in the ITSLM - Manager. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart ITSLM - UR and the services that comprise ITSLM - Manager.

KNAS15812-E

The stopping of a detection process has failed. An error occurred during the ITSLM - UR processing. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the messages output to the ITSLM - UR message log, and then take corrective action.

KNAS15813-E

The stopping of a detection process has failed. A communication error occurred between the ITSLM - UR and the ITSLM - Manager. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the communication environment between ITSLM - UR and ITSLM - Manager. If there is a problem with the communication environment, restart the ITSLM - UR service and the services that comprise ITSLM - Manager.

KNAS15814-E

The stopping of a detection process has failed. The processing timed out. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS15815-E

The stopping of a detection process has failed. The operation cannot be performed, as the current status is not "Detecting". detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service` or `webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Check and, if necessary, revise the operation to be executed.

KNAS15816-W

In the stopping of a detection process, errors have occurred during the processing of one or more ITSLM - UR instances. Check whether the JP1/ITSLM - UR service is running normally. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service` or `webTransaction`: Detection of monitored services or Web transactions

(S)

Continues processing.

(O)

Make sure ITSLM - UR started successfully.

KNAS15817-E

The stopping of a detection process has failed. An inter-process communication error occurred in the ITSLM - Manager. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service` or `webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem re-occurs, communication with ITSLM - UR might have failed. Check the message log (`UserResponseMessageM[`*n*`].log`). If there is no problem in the message log, restart the services that comprise ITSLM - Manager.

KNAS15818-E

The stopping of a detection process has failed. detection type=*aa....aa*

aa....aa: Type of detection

Description

An error occurred during detection stop processing.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15908-E

The acquisition of detection results has failed. During the processing for ITSLM - UR, an inter-process communication error occurred in the ITSLM - Manager. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the relevant ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart ITSLM - UR and the services that comprise ITSLM - Manager.

KNAS15909-E

The acquisition of detection results has failed. An error occurred during the ITSLM - UR processing. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the messages output to the ITSLM - UR message log, and then take corrective action.

KNAS15910-E

The acquisition of detection results has failed. A communication error occurred between the ITSLM - UR and the ITSLM - Manager. ITSLM - UR IP address=*aa....aa*, detection type=*bb....bb*

aa....aa: IP address of ITSLM - UR

bb....bb: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends the relevant ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the communication environment between ITSLM - UR and ITSLM - Manager. If there is a problem with the communication environment, restart the ITSLM - UR service and the services that comprise ITSLM - Manager.

KNAS15911-E

The acquisition of detection results has failed. The processing timed out. detection type=*aa....aa*

aa....aa: Type of detection

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS15912-E

The acquisition of detection results has failed. The operation cannot be performed, as the current status is not "Detecting". detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Check and, if necessary, revise the operation to be executed.

KNAS15913-E

The acquisition of detection results has failed. An inter-process communication error occurred in the ITSLM - Manager. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem re-occurs, communication with ITSLM - UR might have failed. Check the message log (`UserResponseMessageM[`*n*`].log`). If there is no problem in the message log, restart the services that comprise ITSLM - Manager.

KNAS15914-E

The acquisition of detection results has failed. detection type=*aa....aa*

aa....aa: Type of detection

Description

An error occurred while obtaining detection results.

The detection types have the following meanings:

- service: Detection of monitored services
- webTransaction: Detection of Web transactions
- service or webTransaction: Detection of monitored services or Web transactions

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS15915-E

The acquisition of detection results has failed. There is no ITSLM - UR instance available to continue the detection process. The detection process will be stopped. detection type=*aa....aa*

aa....aa: Type of detection

Description

ITSLM - UR was stopped or an error occurred while obtaining detection results; as a result, there is no ITSLM - UR that is able to continue detection.

The detection types have the following meanings:

- service: Detection of monitored services
- webTransaction: Detection of Web transactions
- service or webTransaction: Detection of monitored services or Web transactions

(S)

Suspends processing and places detection in stopped status.

(O)

Check the messages output to the message log, and then take corrective action. Make sure ITSLM - UR is running.

KNAS16000-E

The acquisition of monitor settings has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: HiRDBEmbeddedEdition_JL0). If this does not resolve the problem, contact a system administrator.

KNAS16001-E

> The acquisition of monitor settings has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16002-E

> The acquisition of monitor settings has failed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

An error occurred while obtaining monitoring settings.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS16003-E

> The acquisition of monitor settings has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS16004-E

The acquisition of monitor settings has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which Web transactions have changed, check the message log.

KNAS16100-I

A monitor item was set. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

KNAS16101-E

The setting of monitor items has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS16102-E

The setting of monitor items has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16103-E

The setting of monitor items has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16104-E

The setting of monitor items has failed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

An error occurred while setting monitoring items.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS16105-E

The setting of monitor items has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS16107-E

The setting of monitor items has failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

Monitoring of the specified monitored service is starting. Monitoring of a monitored service cannot be set up while the service is being monitored.

(S)

Suspends processing.

(O)

Stop monitoring of the monitored service, and then retry the operation.

KNAS16108-E

The setting of monitor items has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is detecting monitored services. Other operations cannot be executed on monitored services during detection.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS16109-E

The setting of monitor items has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends the processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS16110-E

The setting of monitor items has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which Web transactions have changed, check the message log.

KNAS16200-I

The event status was changed to "Read". maintenance information=*aa....aa*

aa....aa: Event ID

KNAS16201-E

Event status change has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16202-E

Event status change has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16203-E

Event status change has failed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

An error occurred during processing of the change in event status.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS16204-E

Event status update has failed. The specified event and service are already deleted and do not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified event and monitored service have already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS16205-E

> Event status update has failed. The specified event and Web transaction are already deleted and do not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified event and Web transaction have already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which Web transactions have changed, check the message log.

KNAS16206-E

> Event status update has failed. The specified event and monitor item are already deleted and do not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified event and monitoring item have already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the latest configuration information.

KNAS16300-I

> Service monitoring was started. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS16301-E

> The starting of service monitoring has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent monitored services and monitoring statuses.

If you want to see which monitored services have changed, check the message log.

KNAS16302-E

> The starting of service monitoring has failed. During processing for the ITSLM - Manager, an inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing of the relevant monitored service, and continues processing of other monitored services.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16303-E

> The starting of service monitoring has failed. During processing for the ITSLM - UR, an inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart ITSLM - UR or the services that comprise ITSLM - Manager.

KNAS16304-E

The starting of service monitoring has failed. A communication error occurred between the ITSLM - UR and the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the communication environment between ITSLM - UR and ITSLM - Manager. If there is a problem with the communication environment, restart the ITSLM - UR service and the services that comprise ITSLM - Manager.

KNAS16305-E

The starting of service monitoring has failed. An error occurred during processing for the ITSLM - UR. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check the messages output to the ITSLM - UR message log, and then take corrective action.

KNAS16306-E

In the starting of service monitoring, the ITSLM - Manager post-processing failed.

Description

An error occurred during post-processing of the ITSLM - Manager in which an error occurred.

(S)

Suspends processing for all specified monitored services.

(O)

Check the message that was output immediately before this message and take corrective action.

Restart the services that comprise ITSLM - Manager as necessary.

KNAS16307-E

In the starting of service monitoring, the ITSLM - UR post-processing failed. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of ITSLM - UR

Description

An error occurred during post-processing of the ITSLM - UR where an error occurred.

(S)

Suspends processing for all specified monitored services.

(O)

Check the message that was output immediately before this message and take corrective action.

Restart ITSLM - UR and the services that comprise ITSLM - Manager as necessary.

KNAS16308-E

For some of the specified services, the starting of service monitoring has failed. An error occurred during the starting of service monitoring.

Description

An error occurred while monitoring of at least one of the specified monitored services was starting.

(S)

Continues processing.

(O)

Check the most recent monitoring status from the window.

With respect to the monitored service for which processing failed, check the message log and take corrective action according to the message that was output immediately before this message.

KNAS16309-E

For all of the specified services, the starting of service monitoring has failed. An error occurred during a database operation.

(S)

Suspends processing for all specified monitored services and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16310-E

For all of the specified services, the starting of service monitoring has failed. An inter-process communication error occurred in the ITSLM - Manager.

Description

A communications error occurred during ITSLM - Manager processing.

(S)

Suspends processing for all specified monitored services.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16311-E

For all of the specified services, the starting of service monitoring has failed.

Description

An error occurred while monitoring of the monitored services was starting.

(S)

Suspends processing for all specified monitored services and returns to the login window.

(O)

Contact a system administrator.

KNAS16312-E

The starting of service monitoring has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS16314-E

For all of the specified services, the starting of service monitoring has failed. An error occurred during post-processing in the starting of service monitoring.

Description

An error occurred during post-processing of the ITSLM - UR or ITSLM - Manager in which an error had occurred while monitoring of monitored services was starting.

(S)

Suspends processing for all specified monitored services and returns to the login window.

(O)

Check the message log and take corrective action according to the message that was output immediately before this message.

KNAS16315-E

The starting of service monitoring has failed. An error occurred during a database operation in the ITSLM - Manager processing. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing of the affected monitored service, and continues processing of other monitored services.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16316-E

The starting of service monitoring has failed. An error occurred during the processing for ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while monitoring of a monitored service for ITSLM - Manager was starting.

(S)

Suspends processing of the affected monitored service, and continues processing of other monitored services.

(O)

Restart the services that comprise ITSLM - Manager.

KNAS16317-E

The starting of service monitoring will be stopped, as the number of services that can be monitored at a time will exceed the maximum. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified number of services for which monitoring is to be started has exceeded the maximum number of monitored services that can be monitored at the same time.

(S)

Suspends processing of the affected monitored service, and continues processing of other monitored services.

(O)

If you want to start monitoring a new monitored service, stop monitoring of another monitored service before starting the new monitoring.

KNAS16318-E

The starting of service monitoring has failed. The ITSLM - UR version you are using to monitor the specified service cannot monitor a service by specifying its path. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*, version=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

dd....dd: Version of ITSLM - UR

(S)

Suspends processing.

(O)

Use ITSLM - UR version 09-51 or later to monitor the specified monitored service.

KNAS16319-E

The starting of service monitoring has failed. The ITSLM - UR version you are using to monitor the specified service cannot monitor a Web transaction. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*, version=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

dd....dd: Version of ITSLM - UR

(S)

Suspends processing.

(O)

Use ITSLM - UR version 09-51 or later to monitor the specified monitored service.

KNAS16320-E

The starting of service monitoring has failed. The ITSLM - UR version you are using to monitor the specified service cannot monitor a service by specifying its port. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*, version=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

dd....dd: Version of ITSLM - UR

(S)

Suspends processing.

(O)

Use ITSLM - UR version 09-51 or later to monitor the specified monitored service.

KNAS16321-E

The starting of service monitoring has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations cannot be executed on monitored services while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS16322-E

The starting of service monitoring has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends the processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS16323-W

For a monitor item of the specified service, the starting of monitor has failed. An error occurred during the starting of the monitor item.

Description

An error occurred during startup processing of monitoring items in one or more of the specified services.

(S)

Continues processing.

(O)

Check the most recent monitoring status from the window.

Check the message log for the monitoring items for which processing failed, and take corrective action according to the message that was output immediately before this message.

KNAS16324-E

The starting of a service monitor item has failed. During the processing for ITSLM - Manager, an inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager while monitoring of a monitoring item was starting for an ITSLM - Manager service.

(S)

Suspends monitoring startup processsing of the monitoring items of the service.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the ITSLM - Manager service.

KNAS16325-E

The starting of service monitoring has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the ITSLM - Manager service.

KNAS16400-I

Service monitoring was stopped. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS16401-E

The stopping of service monitoring has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent monitored services and monitoring statuses.

If you want to see which monitored services have changed, check the message log.

KNAS16402-E

> The stopping of service monitoring has failed. During the processing for ITSLM - Manager, an inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored the service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager while monitoring of a monitored service for ITSLM - Manager was stopping.

(S)

Suspends processing. In the case of a forced stop, continues processing.

(O)

Check whether monitoring of the relevant service has stopped. If it has not stopped, wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16403-E

> The stopping of service monitoring has failed. During the processing for ITSLM - UR, an inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check whether monitoring of the affected service has stopped. If it has not stopped, wait a while, and then retry the operation. If the problem reoccurs, restart ITSLM - UR and the services that comprise ITSLM - Manager.

KNAS16404-E

> The stopping of service monitoring has failed. A communication error occurred between the ITSLM - UR and the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check whether monitoring of the affected service has stopped. If it has not stopped, check the communication environment between ITSLM - UR and ITSLM - Manager. If there is a problem with the communication environment, restart the ITSLM - UR service and the services that comprise ITSLM - Manager.

KNAS16405-E

The stopping of service monitoring has failed. An error occurred during the ITSLM - UR processing. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

(S)

Suspends the affected ITSLM - UR processing, and continues other ITSLM - UR processing.

(O)

Check whether monitoring of the affected service has stopped. If it has not stopped, check the messages output to the ITSLM - UR message log, and then take corrective action.

KNAS16407-E

In the stopping of service monitoring, the ITSLM - UR post-processing failed. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of ITSLM - UR

Description

An error occurred during post-processing of the ITSLM - UR where an error occurred.

(S)

Suspends processing for all specified monitored services.

(O)

Check the message in the message log that was output immediately before this message and take corrective action.

If necessary, restart ITSLM - UR and the services that comprise ITSLM - Manager.

KNAS16408-E

For some of the specified services, the stopping of service monitoring has failed. An error occurred during the stopping of service monitoring.

Description

An error occurred while monitoring of at least one monitored service was stopping.

(S)

Continues processing.

(O)

Check the most recent monitoring status from the window.

With respect to a monitored service where processing failed, check the message log, and then take corrective action according to the message that was output immediately before this message.

KNAS16409-E

For all of the specified services, the stopping of service monitoring has failed. An error occurred during a database operation.

(S)

Suspends processing for all specified monitored services and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16410-E

For all of the specified services, the stopping of service monitoring has failed. An inter-process communication error occurred in the ITSLM - Manager.

(S)

Suspends processing for all specified monitored services.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16411-E

For all of the specified services, the stopping of service monitoring has failed.

Description

An error occurred while monitoring of a monitored service was stopping.

(S)

Suspends processing for all specified monitored services and returns to the login window.

(O)

Contact a system administrator.

KNAS16412-E

The stopping of service monitoring has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS16414-W

The JP1/ITSLM - UR service is being stopped. The stopping of service monitoring will continue. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of ITSLM - UR

(S)

Continues processing, with the exception of the processing for the ITSLM - UR service **JP1/ITSLM - User Response Service** (service name: `JP1_ITSLM_UR_Service`), which is being stopped.

(O)

If you need to do processing for the ITSLM - UR service **JP1/ITSLM - User Response Service** after this message has been output, start the ITSLM - UR service **JP1/ITSLM - User Response Service**.

KNAS16415-E

For all of the specified services, the stopping of service monitoring has failed. An error occurred during post-processing in the stopping of service monitoring.

Description

An error occurred during post-processing of the ITSLM - UR or ITSLM - Manager where an error occurred while monitoring of monitored services was stopping.

(S)

Suspends processing for all the specified services and returns to the login window.

(O)

Check the message log and take corrective action according to the message that was output immediately before this message.

KNAS16416-E

The stopping of service monitoring has failed. An error occurred during a database operation in the ITSLM - Manager processing. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing of the affected monitored service, and continues processing of other monitored services. In the case of a forced stop, continues processing.

(O)

Check whether monitoring of the affected service has stopped. If it has not stopped, restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16417-E

The stopping of service monitoring has failed. An error occurred during the processing for ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing of the affected monitored service, and continues processing of other monitored services. In the case of a forced stop, continues processing.

(O)

Check whether monitoring of the affected service has stopped. If it has not stopped, restart the services that comprise ITSLM - Manager.

KNAS16418-E

The stopping of service monitoring has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations cannot be executed on monitored services while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS16419-W

For a monitor item of the specified service, the stopping of the monitor has failed. An error occurred during the stopping of the monitor item.

Description

An error occurred while monitoring of a monitoring item in one or more of the specified services was stopping.

(S)

Continues processing.

(O)

Check the most recent monitoring status from the window.

Check the message log for the monitoring item for which processing failed, and take corrective action according to the message that was output immediately before this message.

KNAS16420-E

The stopping of a service monitor item has failed. During the processing for ITSLM - Manager, an inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager while monitoring of a monitoring item was stopping for an ITSLM - Manager service.

(S)

Continues processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the ITSLM - Manager service.

KNAS16421-I

Service monitoring was forced to be stopped. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS16422-E

The forced stopping of service monitoring has failed. An error occurred during a database operation.

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16423-E

The forced stopping of service monitoring has failed. During the processing for ITSLM - Manager, an inter-process communication error occurred in the ITSLM - Manager.

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16424-E

The stopping of service monitoring has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16425-E

In the stopping of a service monitor item, the ITSLM - Manager post-processing failed.

Description

An error occurred during post-processing of the ITSLM - Manager where an error occurred.

(S)

Suspends processing for all specified monitored services.

(O)

Check in the message log for the message that was output immediately before this message and take corrective action.

If necessary, restart the services that comprise ITSLM - Manager.

KNAS16500-E

The acquisition of a services list has failed. An error occurred during a database operation. service group name=*aa....aa*

aa....aa: Name of the service group

Description

An error occurred in a database operation. If the error occurred during the initialization process or before the name of the service group was obtained, `service group name = ""` is displayed.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16501-E

The acquisition of a services list has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*

aa....aa: Name of the service group

Description

An inter-process communications error occurred in ITSLM - Manager. If the error occurred during the initialization process or before the name of the service group was obtained, `service group name = ""` is displayed.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16502-E

> The acquisition of a services list has failed. service group name=*aa....aa*

aa....aa: Name of the service group

Description

An error occurred while acquiring the list of services. If the error occurred during the initialization process or before the name of the service group was obtained, `service group name = ""` is displayed.

(S)

Suspends the processing and returns to the login window.

(O)

Contact a system administrator.

KNAS16503-E

> The acquisition of a services list has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16600-E

> The acquisition of service performance information has failed. An error occurred during a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16601-E

> The acquisition of service performance information has failed. An inter-process communication error occurred in the ITSLM - Manager.

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16602-E

The acquisition of service performance information has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16700-E

The acquisition of a events list has failed. An error occurred during a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16701-E

The acquisition of a events list has failed. An inter-process communication error occurred in the ITSLM - Manager.

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16702-E

The acquisition of a events list has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16800-E

The acquisition of a performance chart has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16801-E

The acquisition of a performance chart has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16802-E

The acquisition of a performance chart of the specified monitored item has failed. An error occurred during a database operation.

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16803-E

The acquisition of a performance chart of the specified monitored item has failed. An inter-process communication error occurred in the ITSLM - Manager.

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16900-E

The acquisition of the service group status summary has failed. An error occurred during a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS16901-E

The acquisition of the service group status summary has failed. An inter-process communication error occurred in the ITSLM - Manager.

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS16902-E

The acquisition of the service group status summary has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17000-E

The acquisition of warning services has failed. An error occurred during a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17001-E

The acquisition of warning services has failed. An inter-process communication error occurred in the ITSLM - Manager.

(S)

Suspends processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17002-E

The acquisition of warning services has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17300-E

Report data update has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS17301-E

> Report data update has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17302-E

> Report data update has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17303-E

> Report data update has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which Web transactions have changed, check the message log.

KNAS17400-E

> The update of report chart data has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS17401-E

> The update of report chart data has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17402-E

> The update of report chart data has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17403-E

> The update of report chart data has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which Web transactions have changed, check the message log.

KNAS17500-I

> The report was output. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

KNAS17501-E

> Report data output has failed. The specified service is already deleted and does not exist. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified monitored service has already been deleted by another user.

(S)

Outputs an empty CSV file and continues processing.

(O)

Log in again to check the latest status of the registered monitored services, and then select from among the monitored services that are present.

KNAS17502-E

Report data output has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17503-E

Report data output has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17504-E

Report data output has failed. The specified Web transaction is already deleted and does not exist. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

The specified Web transaction has already been deleted by another user.

(S)

Outputs an empty CSV file and continues processing.

(O)

Select a Web transaction that occurs in the registered monitored services when they have been updated to their latest status. By logging in again, you can see the latest status of the registered monitored services.

KNAS17561-E

Template acquisition has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17562-E

Template acquisition has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17564-E

Template saving has failed. The specified template is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

The specified template has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the saved status of the most recent templates, and then specify a template that exists.

KNAS17565-E

Template deletion has failed. The specified template is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

The specified template has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the saved status of the most recent templates, and then specify a template that exists.

KNAS17566-E

Template saving has failed. The number of templates has reached the upper limit. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

The template cannot be registered because the number of registered templates has reached the maximum.

(S)

Suspends processing.

(O)

Delete unwanted templates from the saved templates, and then create and save the new template.

KNAS17567-E

Template saving has failed. A template with the specified template name already exists. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

A template with the specified template name has already been saved by another user.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing.

(O)

Change the template name so that it is unique, and then save the template again.

KNAS17568-E

Template acquisition has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while retrieving the template.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17569-E

Template acquisition has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS17570-E

The acquisition of template setting information has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17571-E

The acquisition of template setting information has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17572-E

The acquisition of template setting information has failed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

An error occurred while retrieving template settings information.

(S)

Suspends processing.

(O)

Restart the ITSLM - Manager services. If the problem reoccurs, contact a system administrator.

KNAS17573-E

The acquisition of template setting information has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS17574-E

The acquisition of template setting information has failed. The specified template is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

The specified template has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the saved status of the most recent templates, and then specify a template that exists.

KNAS17575-I

> The template was saved. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

KNAS17576-E

> Template saving has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, operation type=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Type of operation

Description

The specified service has already been deleted by another user.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS17577-E

> Template saving has failed. A command having an exclusive relationship is in progress. Wait for a while and retry. operation type=*aa....aa*

aa....aa: Type of operation

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS17578-E

> Template saving has failed. The processing timed out. Wait for a while and retry. operation type=*aa....aa*

aa....aa: Type of operation

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not fishished after waiting for at least 10 seconds.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS17579-E

> Template saving has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

An error occurred in a database operation.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17580-E

> Template saving has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

An inter-process communications error occurred in ITSLM - Manager.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17581-E

> Template saving has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*, operation type=*bb....bb*

aa....aa: Type of detection

bb....bb: Type of operation

Description

Monitored services or Web transactions are being detected by another user. Other operations on templates cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS17582-E

> Template saving has failed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

An error occurred while saving a template.

The meanings of the operation types are as follows:

- `ADD`: Add template
- `EDIT`: Edit template

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17583-I

> The template was deleted. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

KNAS17584-E

> Template deletion has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS17585-E

Template deletion has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS17586-E

Template deletion has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not fishished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS17587-E

Template deletion has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17588-E

> Template deletion has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17589-E

> Template deletion has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Monitored services or Web transactions are being detected by another user. Other operations on templates cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS17590-E

> Template deletion has failed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

Description

An error occurred while deleting a template.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17591-I

The report was output. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

The meanings of the operation types are as follows:

- `GUI`: Display in the Template Preview window
- `CSV`: Output to a CSV file

KNAS17592-E

Report output has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, operation type=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Type of operation

Description

The specified monitored service has already been deleted by another user.

The meanings of the operation types are as follows:

- `GUI`: Display in the Template Preview window
- `CSV`: Output to a CSV file

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS17593-E

Report output has failed. The specified template is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

The specified template has already been deleted by another user.

The meanings of the operation types are as follows:

- `GUI`: Display in the Template Preview window
- `CSV`: Output to a CSV file

(S)

Refreshes the window.

(O)

Check the saved status of the most recent templates, and then specify a template that exists.

KNAS17594-E

Report output has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

An error occurred in a database operation.

The meanings of the operation types are as follows:

- `GUI`: Display in the Template Preview window
- `CSV`: Output to a CSV file

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17595-E

Report output has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

An inter-process communications error occurred in ITSLM - Manager.

The meanings of the operation types are as follows:

- `GUI`: Display in the Template Preview window
- `CSV`: Output to a CSV file

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17596-E

> Report output has failed. service group name=*aa....aa*, service name=*bb....bb*, template name=*cc....cc*, operation type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the template

dd....dd: Type of operation

Description

An error occurred during report output processing.

The meanings of the operation types are as follows:

- `GUI`: Display in the Template Preview window
- `CSV`: Output to a CSV file

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17597-E

> Report output has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17598-E

The acquisition of template setting information has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17600-I

A Web transaction was registered. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

KNAS17601-E

Web transaction registration has failed. The specified Web transaction name is already registered in the same service. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

Description

The names of Web transactions belonging to a monitored service must be unique within the monitored service.

The name of the Web transaction represented by *cc....cc* is already registered within the same monitored service.

(S)

Suspends processing.

(O)

Revise the name of the Web transaction. Use a name that is not registered within the same monitored service.

KNAS17602-E

> Web transaction registration has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17603-E

> Web transaction registration has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem re-occurs, communication with ITSLM - UR might have failed. Check the message log (`UserResponseMessageM[`*n*`].log`). If there is no problem in the message log, restart the services that comprise ITSLM - Manager.

KNAS17604-E

> Web transaction registration has failed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

Description

An error occurred while registering the Web transaction.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17605-E

Web transaction registration has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS17606-E

Web transaction registration has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations on Web transactions cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS17607-E

Web transaction registration has failed. The ITSLM - UR version you are using to monitor the service being registered cannot monitor a Web transaction. service group name=*aa....aa*, service name=*bb....bb*, ITSLM - UR IP address=*cc....cc*, version=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: IP address of ITSLM - UR

dd....dd: Version of ITSLM - UR

(S)

Suspends processing.

(O)

Use version 09-51 or later of ITSLM - UR to monitor the monitored service into which the Web transaction is to be registered.

KNAS17608-E

> Web transaction registration has failed. The operation cannot be performed, as the monitored status of the service being registered is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service into which the Web transaction is to be registered, and then retry the operation.

KNAS17609-E

> Web transaction registration has failed. The service being registered is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The monitored service into which the Web transaction is to be registered has already been deleted by another user.

(S)

Suspends processing.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS17610-E

> Web transaction registration has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS17611-E

Web transaction registration has failed. The number of registered Web transactions has reached the upper limit.

Description

An attempt to register a Web transaction failed. The number of registered Web transactions has reached the maximum.

(S)

Suspends processing.

(O)

Check the list of Web transactions. If the number of Web transactions on the list of Web transactions does not appear to reach the maximum, log in again.

KNAS17700-I

A Web transaction was deleted. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

KNAS17701-E

Web transaction deletion has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

To see which Web transactions have changed, check the message log.

KNAS17702-E

Web transaction deletion has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17703-E

> Web transaction deletion has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS17704-E

> Web transaction deletion has failed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

Description

An error occurred while deleting a Web transaction.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17705-E

> Web transaction deletion has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS17706-E

> Web transaction deletion has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations on Web transactions cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS17707-E

> Web transaction deletion has failed. The operation cannot be performed, as the service monitored status of the specified Web transaction is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

Description

Monitoring is starting for the monitored service to which the specified Web transaction belongs. Deletion of a Web transaction cannot be performed while monitoring is starting.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service to which the affected Web transaction belongs, and then retry the operation.

KNAS17708-E

> Web transaction deletion has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS17709-E

> Web transaction deletion has failed. The service for the specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The monitored service of the specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS17800-E

> An attempt to acquire the access log failed. An error occurred while a database operation was being performed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while a database operation was being performed.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS17801-E

The number of access log entries matching the specified filter conditions exceeds the upper limit of 5,000.

Description

The number of access log entries matching the specified filter conditions exceeds 5,000.

(S)

Processing continues on the first 5,000 access logs chronologically in order of response times.

(O)

Specify new filter conditions and redisplay the access logs.

KNAS17802-E

An attempt to acquire the access log failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communication error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem re-occurs, communication with ITSLM - UR might have failed. Check the message log (`UserResponseMessageM[`*n*`].log`). If there is no problem in the message log, restart the services that comprise ITSLM - Manager.

KNAS17803-E

An attempt to acquire the access log failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while acquiring the access log.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS17804-I

No displayable access logs exist.

Description

No displayable access logs exist.

(S)

Displays no access logs.

(O)

Change the filter conditions or the logging range shown in the dotted line, and then redisplay the access logs. If the problem reoccurs, check the following:

- ITSLM - UR is version 10-10 or later.
- The value specified for `accessLogFilePath` in the ITSLM - UR system definition.

KNAS17805-W

An attempt to acquire one or more access log failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while acquiring an access log.

(S)

Continues processing using only the acquired access logs.

(O)

Check the messages output to the ITSLM - UR message log, and then take the appropriate corrective action.

KNAS17806-E

An attempt to acquire the access log failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An attempt to acquire the access log failed.

(S)

Suspends processing.

(O)

Check the message log. If an error message was output immediately before this message, take the corrective action for that error.

If the problem reoccurs, contact a system administrator.

KNAS17807-E

An attempt to acquire the access log failed. The ITSLM - UR service was not running. ITSLM - UR IP address=*aa....aa*

aa....aa: IP address of ITSLM - UR

Description

ITSLM - UR is not running.

(S)

Suspends processing.

(O)

Check that ITSLM - Manager has started successfully.

KNAS18100-I

The sequential position of a Web transaction was updated. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

KNAS18101-E

The update of the sequential position of a Web transaction has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18102-E

The update of the sequential position of a Web transaction has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18103-E

The update of the sequential position of a Web transaction has failed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction belonging to the monitored service

Description

An error occurred while updating the order of Web transactions.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS18104-E

The update of the sequential position of a Web transaction has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18105-E

The update of the sequential position of a Web transaction has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Another user is performing detection. Other operations on Web transactions cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS18106-E

> The update of the sequential position of a Web transaction has failed. The operation cannot be performed, as the monitored status of the service being updated is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring is starting for the monitored service that is the update destination. A Web transaction cannot be edited while its monitored service is being monitored.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service that is the update destination, and then retry the operation.

KNAS18107-E

> The update of the sequential position of a Web transaction has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS18108-E

> The update of the sequential position of a Web transaction has failed. The sequential position of the specified Web transaction is already updated. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS18109-E

> The update of the sequential position of a Web transaction has failed. The service for the specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The monitored service of the specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS18110-E

> The update of the sequential position of a Web transaction has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18200-E

> The acquisition of a Web transactions list has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18201-E

The acquisition of a Web transactions list has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18202-E

The acquisition of a Web transactions list has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while retrieving the list of Web transactions.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS18300-I

A Web transaction was edited. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

KNAS18301-E

The editing of a Web transaction has failed. The specified Web transaction name is already registered in the same service. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

Description

The Web transaction name must be unique within the monitored service.

(S)

Suspends processing.

(O)

Revise the Web transaction name. Use a name that is not registered within the same monitored service.

KNAS18302-E

The editing of a Web transaction has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18303-E

The editing of a Web transaction has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18304-E

The editing of a Web transaction has failed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

Description

An error occurred while editing a Web transaction.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS18305-E

The editing of a Web transaction has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18306-E

The editing of a Web transaction has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait for the detection processing that the other user is running to be completed, and then retry the operation.

KNAS18307-E

The editing of a Web transaction has failed. The operation cannot be performed, as the monitored status of the service being edited is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring is starting for the monitored service that is the edit destination. A Web transaction cannot be edited while its monitored service is being monitored.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service that is the edit destination, and then retry the operation.

KNAS18308-E

The editing of a Web transaction has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*, Web transaction name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the Web transaction

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS18309-E

The editing of a Web transaction has failed. The service for the specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The monitored service of the specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

Check the message log if you want to see which monitored services have changed.

KNAS18310-E

The editing of a Web transaction has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18400-I

Configuration information was refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS18401-E

The refreshing of configuration information has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services.

If you want to see which monitored services have changed, check the message log.

KNAS18402-E

The refreshing of configuration information has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18403-E

The refreshing of configuration information has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the ITSLM - Manager service.

KNAS18404-E

The refreshing of configuration information has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while updating configuration information.

(S)

Suspends processing.

(O)

Take the corrective actions noted below.

If this does not resolve the problem, contact a system administrator.

- Make sure matching ITSLM host names were specified in ITSLM - Manager and PFM - Manager. If the names do not match, correct them so they do match.
- Make sure the Performance Management configuration information did not change when the configuration information was updated. If it did change, try updating the configuration information again.

KNAS18405-E

The refreshing of configuration information has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18406-E

The refreshing of configuration information has failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring is starting for the specified monitored service. Configuration information cannot be updated during monitoring of the monitored service.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service, and then retry the operation.

KNAS18407-E

The refreshing of configuration information has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

The monitored service or Web transaction is being detected by another user. Other operations cannot be executed on monitored services while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS18408-E

The refreshing of configuration information has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18409-E

The refreshing of configuration information has failed. A communication error occurred between the PFM - Manager and the ITSLM - Manager. destination host name=*aa....aa*, destination port number=*bb....bb*

aa....aa: PFM - Manager host name

bb....bb: PFM - Manager port number

Description

A communications error occurred between PFM - Manager and ITSLM - Manager.

(S)

Suspends processing.

(O)

Check whether PFM - Manager is running. If it is running, check and, if necessary, revise the values specified for the `pfmManagerHost` and `pfmManagerPort` properties in the `jp1itslm.properties` system definition file. Also, revise the communication environment between PFM - Manager and ITSLM - Manager if necessary.

If this does not resolve the problem, contact a system administrator.

KNAS18410-W

Measurement conditions could not be obtained, as the PFM - Agent for Service Response was not running. host name=*aa....aa*, agent name=*bb....bb*

aa....aa: PFM - Agent for Service Response host name

bb....bb: PFM - Agent for Service Response monitoring agent name

Description

Measurement conditions could not be obtained because PFM - Agent for Service Response has stopped.

(S)

Continues processing.

(O)

Check whether measurement conditions are required from the PFM - Agent for Service Response whose host name was output. If they are required, start PFM - Agent for Service Response and update the configuration information again.

KNAS18411-E

The refreshing of configuration information has failed. The configuration information of the specified service is already refreshed by a different user. Retry to refresh the configuration information. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An attempt to update configuration information failed. The configuration information of the specified service has already been updated by another user.

(S)

Suspends processing.

(O)

Update the configuration information again.

KNAS18412-I

System performance monitor settings were saved. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS18413-E

System performance monitor settings have failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18414-E

System performance monitor settings have failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18415-E

System performance monitor settings have failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18416-E

System performance monitor settings have failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS18417-E

System performance monitor settings have failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring is starting for the specified monitored service. Configuration information cannot be updated during monitoring of the monitored service.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service, and then retry the operation.

KNAS18418-E

> System performance monitor settings have failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Monitored services or Web transactions are being detected by another user. Other operations on services cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS18419-E

> System performance monitor settings have failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18420-I

> Availability monitor settings were saved. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS18421-E

> Availability monitor settings have failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18422-E

> Availability monitor settings have failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18423-E

> Availability monitor settings have failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18424-E

> Availability monitor settings have failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS18425-E

> Availability monitor settings have failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring is starting for the specified monitored service. Configuration information cannot be updated during monitoring of the monitored service.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service, and then retry the operation.

KNAS18426-E

> Availability monitor settings have failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Monitored services or Web transactions are being detected by another user. Other operations on services cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS18427-E

> Availability monitor settings have failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18428-E

> The acquisition of configuration information settings has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18429-E

> The acquisition of configuration information settings has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18430-E

The acquisition of configuration information settings has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS18431-E

The acquisition of configuration information differences has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18432-E

The acquisition of configuration information differences has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18433-E

The acquisition of configuration information differences has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS18434-E

The acquisition of configuration information differences has failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

Monitoring is starting for the specified monitored service. Configuration information cannot be updated during monitoring of the monitored service.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service, and then retry the operation.

KNAS18435-E

System performance monitor settings have failed. The configuration information of the specified service is already refreshed by a different user. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An attempt to set system performance monitoring failed. The configuration information for the specified monitored service has already been updated by another user.

(S)

Suspends processing.

(O)

Check the latest configuration information. Try setting system performance monitoring again.

KNAS18436-E

Availability monitor settings have failed. The configuration information of the specified service is already refreshed by a different user. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An attempt to set availability monitoring failed. The configuration information for the specified monitored service has already been updated by another user.

(S)

Suspends processing.

(O)

Check the latest configuration information. Try setting availability monitoring again.

KNAS18437-E

The acquisition of configuration information differences has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred while obtaining differential configuration information.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS18438-E

The refreshing of configuration information has failed.

Description

An error occurred while updating configuration information.

(S)

Suspends processing and returns to the login window.

(O)

Contact a system administrator.

KNAS18439-E

The refreshing of configuration information has failed. An error occurred during data conversion.

Description

An error occurred during data conversion processing.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18440-E

The acquisition of configuration information differences has failed. An error occurred during data conversion.

Description

An error occurred during data conversion processing.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18441-E

System performance monitor settings have failed. The specified monitor item is already registered by a different user. Delete the monitor item that caused the error. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

Description

An attempt to set system performance monitoring failed. The specified monitoring item was already registered by another user.

(S)

Suspends processing.

(O)

Delete the failed monitoring item.

KNAS18442-E

The acquisition of configuration information differences has failed. The system could not request the processing from the PFM - Manager. destination host name=*aa....aa*, destination port number=*bb....bb*

aa....aa: PFM - Manager host name

bb....bb: PFM - Manager port number

Description

The version of the Performance Manager at the linkage destination is not the version assumed by ITSLM.

(S)

Suspends processing.

(O)

Make sure the version of PFM - Manager being linked to is at least as recent as the version that is assumed by ITSLM.

KNAS18443-E

The acquisition of configuration information differences has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18444-E

The acquisition of configuration information differences has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Monitored services or Web transactions are being detected by another user. Other operations cannot be executed on monitored services while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS18445-E

The acquisition of configuration information differences has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18446-E

The acquisition of configuration information differences has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18447-E

The refreshing of configuration information has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18448-E

The acquisition of configuration information settings has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18449-E

> System performance monitor settings have failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18450-E

> Availability monitor settings have failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18451-E

> The acquisition of configuration information differences has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Service group name

bb....bb: Service name

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18500-E

The acquisition of system performance information has failed. An error occurred during a database operation.

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18501-E

The acquisition of system performance information has failed. An inter-process communication error occurred in the ITSLM - Manager.

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18502-E

The acquisition of system performance information has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18600-E

The acquisition of service configuration information has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18601-E

The acquisition of service configuration information has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18602-E

The acquisition of service configuration information has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18610-E

The acquisition of service configuration information has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18611-E

The acquisition of service configuration information has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18612-E

The acquisition of service configuration information has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18700-E

The acquisition of monitor item details has failed. An error occurred during a database operation.

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18701-E

The acquisition of monitor item details has failed. An inter-process communication error occurred in the ITSLM - Manager.

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18702-E

The acquisition of monitor item details has failed. The specified monitor item is already deleted and does not exist. The screen will be refreshed.

Description

The specified monitoring item has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the latest configuration information.

KNAS18703-E

The acquisition of monitor item details has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18800-E

The acquisition of monitor settings has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18801-E

> The acquisition of monitor settings has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18802-E

> The acquisition of monitor settings has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

Check the message log to see which services have changed.

KNAS18803-E

> The acquisition of monitor settings has failed. The specified Web transaction is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified Web transaction has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the updated services.

If you want to see which Web transactions have changed, check the message log.

KNAS18804-E

The acquisition of monitor settings has failed. The monitor item is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

A monitoring item has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent configuration information.

KNAS18805-E

The acquisition of monitor settings has failed. The operation cannot be performed, as a configuration information refreshing by a different user is in progress. Wait for a while and retry.

Description

The processing cannot be executed because another user is updating the configuration information.

(S)

Suspends processing.

(O)

Wait for the updating of the configuration information to be completed, and then try again. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18900-I

A monitor item was set. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

KNAS18901-E

The setting of monitor items has failed. An error occurred during a database operation. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An error occurred in a database operation.

(S)

Suspends processing and returns to the login window.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS18902-E

The setting of monitor items has failed. An inter-process communication error occurred in the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

An inter-process communications error occurred in ITSLM - Manager.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS18903-E

The setting of monitor items has failed. A command having an exclusive relationship is in progress. Wait for a while and retry.

Description

The processing cannot be executed because a command that is in an exclusive relationship is running.

(S)

Suspends processing.

(O)

Wait for the command that is in an exclusive relationship to complete its execution, and then retry the operation.

KNAS18904-E

> The setting of monitor items has failed. The specified service is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The specified monitored service has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the most recent list of monitored services. Check the message log if you want to see which monitored services have changed.

KNAS18905-E

> The setting of monitor items has failed. The operation cannot be performed, as a detection process by a different user is in progress. Wait for a while and retry. detection type=*aa....aa*

aa....aa: Type of detection

Description

Monitored services or Web transactions are being detected by another user. Other operations on services cannot be performed while detection processing is underway.

The detection types have the following meanings:

- `service`: Detection of monitored services
- `webTransaction`: Detection of Web transactions
- `service or webTransaction`: Detection of monitored services or Web transactions

(S)

Suspends processing.

(O)

Wait until the detection processing that the other user is executing has been completed, and then retry the operation.

KNAS18906-E

> The setting of monitor items has failed. The processing timed out. Wait for a while and retry.

Description

Because another user was executing an operation that cannot be executed at the same time, it was necessary to wait for the earlier processing to be completed. However, a timeout occurred because the earlier processing had not finished after waiting for at least 10 seconds.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation.

KNAS18907-E

> The setting of monitor items has failed. The operation cannot be performed, as the monitored status of the specified service is "Starting". Stop the service monitoring and then retry. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of monitored target

Description

Monitoring is starting for the specified monitored service. Monitoring of a service cannot be set up while the service is being monitored.

(S)

Suspends processing.

(O)

Stop the monitoring of the monitored service, and then retry the operation.

KNAS18908-E

> The setting of monitor items has failed. The monitor item is already deleted and does not exist. The screen will be refreshed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The monitoring item has already been deleted by another user.

(S)

Refreshes the window.

(O)

Check the latest configuration information.

KNAS30022-I

> Service analysis was started. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

In the case of a system monitoring configuration, an asterisk (`*`) is displayed for the name of the monitored target.

KNAS30023-I

> Service analysis was canceled. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

Description

Analysis startup was stopped because an error occurred while analysis was starting.

In the case of a system monitoring configuration, an asterisk (*) is displayed for the name of the monitored target.

(S)

Suspends processing.

(O)

Check the immediately preceding error message, and then take corrective action.

KNAS30024-E

An error occurred during the starting of service analysis. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

In the case of a system monitoring configuration, an asterisk (*) is displayed for the name of the monitored target.

(S)

Suspends processing.

(O)

Collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS30025-I

Service analysis was stopped. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

In the case of a system monitoring configuration, an asterisk (*) is displayed for the name of the monitored target.

KNAS30026-E

> The acquisition of a Web transaction for which an analysis was to be started has failed. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

There was a failed attempt to confirm that a Web transaction had been created in a monitored service in order to start performance analysis; or, there was a failed attempt to reference Web transaction information from the database in order to start analysis.

(S)

Suspends processing.

(O)

Make sure the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** is running, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS32003-W

> Past performance data could not be obtained from the database. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Type of monitoring that occurred

Description

An accurate baseline cannot be calculated, or the baseline cannot be output, because past performance data cannot be retrieved from the database for use in the predictive error detection baseline.

The types of monitoring have the following meanings:

- `SERVICE`: Service performance monitoring
- `SYSTEM`: System performance monitoring

Note that this message is output only once for the same monitored target. Subsequent output is suppressed until monitoring stops.

(S)

Continues processing.

(O)

Make sure the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS32004-W

Service analysis results could not be output to the database. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Type of data that failed to be output

Description

An attempt to output analysis results to the database failed.

The types of data have the following meanings:

- `PERFORMANCE`: Service performance
- `EVENT`: Service performance event
- `REPORT`: Service performance report
- `AVAILABILITY`: Availability monitoring
- `SYSTEM_PERFORMANCE`: System performance
- `SYSTEM_EVENT`: System performance event
- `SYSTEM_REPORT`: System performance report

Note that this message is output only once for the same monitored target. Subsequent output is suppressed until monitoring stops.

(S)

Continues processing.

(O)

Check whether the `KFPH22025-E` or `KFPH22026-E` message was output to the Windows event log. If such a message was output, there is insufficient space in the database. Extend the database space, and then execute setup again.

If such a message was not output, make sure the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running; or, make sure the system time on the server that is running ITSLM - UR or Performance Management has not been adjusted backward.

If the error reoccurs, restart the ITSLM - Manager service.

KNAS32007-W

JP1 event notification will be blocked, as a connection to JP1/Base failed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

Description

An attempt to connect to JP1/Base to issue a JP1 event failed.

(S)

Suspends notification of JP1 events and continues processing.

(O)

Make sure JP1/Base is running and that the `jbsHostName` property is specified correctly in the `jp1itslm.properties` system definition file in ITSLM - Manager. To resume JP1 event notification, stop monitoring the monitored service, and then restart monitoring.

KNAS32017-I

> The threshold value monitor will be started. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, monitor item name=*dd....dd*, start time=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Names of monitoring items <*monitoring-item-name* `...`>

ee....ee: Start time of threshold monitoring

Description

Threshold monitoring has started on the monitored service.

The names of multiple monitoring items whose monitoring is starting at the same time are output, delimited by the space.

The start time that is output is the time at which performance data was first acquired after the start of threshold monitoring, in the following format (converted to the time zone of ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or - followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32018-I

> The trend monitor will be started. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, monitor item name=*dd....dd*, start time=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Names of monitoring items <*monitoring-item-name* `...`>

ee....ee: Start time of trend monitoring

Description

Trend monitoring has started on the monitored service.

The names of multiple monitoring items whose monitoring is starting at the same time are output, delimited by the space.

The start time that is output is the time at which performance data was first acquired after the start of trend monitoring, in the following format (converted to the time zone of ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD* *hh*:*mm*:*ss* *ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or - followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32019-I

Predictive error detection will be started. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, monitor item name=*dd....dd*, start time=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Names of monitoring items <*monitoring-item-name* `...`>

ee....ee: Start time of predictive error detection

Description

Predictive error detection has started on the monitored service.

The names of multiple monitoring items whose monitoring is starting at the same time are output, delimited by the space.

The start time that is output is the time at which performance data was first acquired after the start of predictive error detection, in the following format (converted to the time zone of ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD* *hh*:*mm*:*ss* *ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or - followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32020-I

The start of predictive error detection will be delayed, as there is not enough past information. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, days till start=*dd....dd*, number of accumulation days=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Number of days until start of predictive error detection

ee....ee: Number of days past information has accumulated

Description

Because the number of days past information has accumulated is less than the number of days until start, startup of predictive error detection is waiting for past information to accumulate.

(S)

Continues processing, and then starts predictive error detection after accumulating past information for the number of days until start.

(O)

Revise the number of days until start of predictive error detection, or perform monitoring of the service until past information has accumulated for the number of days until start of predictive error detection.

KNAS32021-E

> Performance analysis will be blocked, as an error occurred in performance analysis. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, cause=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Failure cause

Description

The meanings of the failure causes are as follows:

- `MEMORY`: A memory shortage occurred.
- `STREAM`: An error occurred in transmission or reception of performance data.
- `THREAD`: The command running performance analysis terminated abnormally.

(S)

Suspends processing.

(O)

Stop monitoring of the monitored service, and then restart after allocating sufficient memory. If this does not resolve the problem, collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS32022-W

> The start time of performance analysis could not be output to the database. The monitored status of the service will not be recovered when restarting the ITSLM - Manager. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, start time=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Start time of analysis of service performance

Description

An attempt to output the start time of analysis of service performance to the database failed.

(S)

Continues processing.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS32023-I

The threshold value monitor for system performance will be started. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, start time=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Start time

Description

Threshold monitoring of system performance has started. Output is performed individually for each monitoring item.

In the case of a Performance Management monitoring item, the name of the monitoring agent is output for the name of the monitored target.

The start time that is output is the time at which the performance data being monitored was acquired, in the following format (converted to the time zone of the ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32024-I

The trend monitor for system performance will be started. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, start time=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Start time

Description

Trend monitoring of system performance has started. Output is performed individually for each monitoring item.

In the case of a Performance Management monitoring item, the name of the monitoring agent is output for the name of the monitored target.

The start time that is output is the time at which the performance data being monitored was acquired, in the following format (converted to the time zone of the ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32025-I

Predictive error detection for system performance will be started. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, start time=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Start time

Description

Predictive error detection of system performance has started. Output is performed individually for each monitoring item.

In the case of a Performance Management monitoring item, the name of the monitoring agent is output for the name of the monitored target.

The start time that is output is the time at which the performance data used for predictive error detection was acquired, in the following format (converted to the time zone of the ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32026-I

> The start of predictive error detection will be delayed, as there is not enough past information on system performance. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, days till start=*ff....ff*, number of accumulation days=*gg....gg*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Days until start

gg....gg: Days of accumulation

Description

Because the number of days until start is greater than the number days past information has accumulated from the monitoring item whose system performance is being detected, the start of predictive error detection is waiting for past information to accumulate.

Output of messages and of the determination of the days of accumulation is performed individually for each monitoring item.

KNAS32027-I

> The availability monitor will be started. service group name=*aa....aa*, service name=*bb....bb*, start time=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Start time

Description

Availability monitoring of the monitored service has started.

The start time that is output is the time at which the performance data being monitored was acquired, in the following format (converted to the time zone of the ITSLM - Manager's execution environment):

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

KNAS32028-W

> The searching or deletion of monitoring results that have exceeded the retention period has failed. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, type=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Type of monitoring that occurred

Description

An error occurred while deleting, or checking for the existence of, monitoring results that exceed the time limit for storing information in the database.

The types of monitoring have the following meanings:

- `PERFORMANCE`: Deletion of an event or service performance chart displayed in the Troubleshoot window
- `REPORT`: Deletion of availability monitoring information or of a service performance table or chart displayed in the Report window
- `SYSTEM_PERFORMANCE`: Deletion of an event or system performance chart displayed in the Troubleshoot window
- `SYSTEM_REPORT`: Deletion of a system performance table or chart displayed in the Report window

(S)

Continues processing.

(O)

Make sure the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** is running, and then restart monitoring. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS32029-W

Performance data will be discarded, as performance analysis is not possible due to an out-of-range value. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, value=*ff....ff*, boundary value=*gg....gg*, details=*hh....hh*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Value of the monitored item

gg....gg: Analysis boundary value

hh....hh: Details

Description

Because the value of the monitoring item whose performance data was received is not within the range of `0.0` through `3.4028235E38`, which is the range within which performance analysis can be run, this information was discarded.

The meanings of the details are as follows:

- `UPPER LIMIT`: The value exceeds the upper limit. The upper limit is output as the analysis boundary value.
- `LOWER LIMIT`: The value exceeds the lower limit. The lower limit is output as the analysis boundary value.
- `NOT NUMBER`: The value was non-numeric (NaN). An asterisk (`*`) is output as the analysis boundary value.

(S)

Continues processing.

(O)

Check the value of the monitoring item that is output in the message. If an invalid value is output, make sure ITSLM - UR or Performance Management is acquiring information correctly.

KNAS34000-W

An SLO threshold value might be exceeded. monitor item=*aa....aa*

aa....aa: Name of the monitoring item

Description

A trend towards exceeding the SLO threshold was detected in a monitoring item (average response time or throughput).

(S)

Continues processing.

(O)

Take corrective action according to the troubleshooting instructions.

For details about troubleshooting, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.

KNAS34001-E

An SLO violation was detected. monitor item=*aa....aa*

aa....aa: Name of the monitoring item

Description

An SLO threshold overage was detected in the monitoring item (average response time, throughput, or error rate).

(S)

Continues processing.

(O)

Take corrective action according to the troubleshooting instructions.

For details about troubleshooting, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.

KNAS34002-W

A sign of a performance error was detected. monitor item=*aa....aa*

aa....aa: Name of the monitoring item

Description

An out-of-range value was detected in the monitoring item (average response time, throughput, or error rate).

(S)

Continues processing.

(O)

Take corrective action according to the troubleshooting instructions.

For details about troubleshooting, see *4.4 Support methodology for root cause investigation when an error or warning is displayed for a monitored service*.

KNAS34003-E

An SLO violation was detected. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, monitor item name=*dd....dd*, occurrence time=*ee....ee*, details=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Name of the monitoring item

ee....ee: Time of occurrence

ff....ff: Details

Description

A threshold was exceeded in service performance threshold monitoring.

The time of occurrence is the time of the detection, in the following format:

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or - followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

One of the following strings is output for the details:

- `UPPER LIMIT`: Upper-limit threshold value exceeded
- `LOWER LIMIT`: Lower-limit threshold value exceeded

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34004-W

An SLO threshold value might be exceeded. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, monitor item name=*dd....dd*, occurrence time=*ee....ee*, details=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Name of the monitoring item

ee....ee: Time of occurrence

ff....ff: Details

Description

A trend towards exceeding a threshold was detected in service performance trend monitoring.
The time of occurrence is the time of the detection.
The time at which the threshold is expected to be exceeded is output as the details.
Both times are output in the following format:

- "*YYYY*/*MM*/*DD* *hh*:*mm*:*ss* *ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or - followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34005-W

A sign of a performance error was detected. service group name=*aa....aa*, service name=*bb....bb*, monitored target name=*cc....cc*, monitor item name=*dd....dd*, occurrence time=*ee....ee*, details=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Name of the monitored target

dd....dd: Name of the monitoring item

ee....ee: Time of occurrence

ff....ff: Details

Description

An out-of-range value from the baseline was detected in service performance predictive error detection.
The time of occurrence is the time of the detection, in the following format:

- "*YYYY*/*MM*/*DD* *hh*:*mm*:*ss* *ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

hh:*mm*:*ss*: *hour*:*minute*:*second*

ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

One of the following strings is output for the details:

- `UPPER LIMIT`: Upper limit for predictive error detection was exceeded
- `LOWER LIMIT`: Lower limit for predictive error detection was exceeded

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34006-E

> It was detected that a service was down. service group name=*aa....aa*, service name=*bb....bb*, occurrence time=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Time of occurrence

Description

A stop in service was detected by service availability monitoring.

The time of occurrence is the time of the detection, in the following format:

- "*YYYY*/*MM*/*DD* *hh*:*mm*:*ss* *ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34007-I

> It was detected that a service was recovered. service group name=*aa....aa*, service name=*bb....bb*, occurrence time=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Time of occurrence

Description

A service recovery was detected by service availability monitoring.

The time of occurrence is the time of the detection, in the following format:

- "*YYYY/MM/DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/MM/DD: *year/month/date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34008-E

An SLO violation was detected. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, occurrence time=*ff....ff*, details=*gg....gg*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Time of occurrence

gg....gg: Details

Description

A threshold was exceeded in system performance threshold monitoring.

The time of occurrence is the time of the detection, in the following format:

- "*YYYY/MM/DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/MM/DD: *year/month/date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

One of the following strings is output for the details:

- `UPPER LIMIT`: Upper-limit threshold value exceeded

- `LOWER LIMIT`: Lower-limit threshold value exceeded

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34009-W

> An SLO threshold value might be exceeded. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, occurrence time=*ff....ff*, details=*gg....gg*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Time of occurrence

gg....gg: Details

Description

A trend towards exceeding a threshold was detected in system performance trend monitoring.

The time of occurrence is the time of the detection.

The time at which the threshold is expected to be exceeded is output as the details.

Both times are output in the following format:

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS34010-W

> A sign of a performance error was detected. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, occurrence time=*ff....ff*, details=*gg....gg*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Time of occurrence

gg....gg: Details

Description

An out-of-range value from the baseline was detected in system performance predictive error detection.

The time of occurrence is the time of the detection, in the following format:

- "*YYYY*/*MM*/*DD hh*:*mm*:*ss ZZZZZ*"

  Legend:

  YYYY/*MM*/*DD*: *year*/*month*/*date*

  hh:*mm*:*ss*: *hour*:*minute*:*second*

  ZZZZZ: + or − followed by the time zone, expressed as the time differential from GMT (a four digit number). An example would be `+0900`.

The time zone is the time zone of ITSLM - Manager's execution environment.

One of the following strings is output for the details:

- `UPPER LIMIT`: Upper limit for predictive error detection exceeded
- `LOWER LIMIT`: Lower limit for predictive error detection exceeded

(S)

Continues processing.

(O)

Log in to ITSLM and check the details.

KNAS50100-W

The transmission of performance information has failed. The performance information will be discarded. time of first=*aa....aa*, time of last=*bb....bb*, number of performance information entries=*cc....cc*

aa....aa: Time at first performance information

bb....bb: Time at end of performance information

cc....cc: Number of discarded performance information items

Description

An attempt to send performance information between processes within ITSLM - Manager failed.

(S)

Discards the performance information and suspends transmission processing.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS50102-W

> Performance information was discarded. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, reason code=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Reason code

Description

Performance information was discarded for one of the reasons indicated by the reason codes below. One of the following is output for the reason code:

- `STOP`: Monitoring of the monitoring item has stopped.
- `DELETE`: Monitoring of the monitored service has started, but there are no monitoring items.

In the case of availability monitoring, an asterisk (`*`) is displayed for the name of the monitored target and for the name of the monitoring item.
If there are no monitoring items, an asterisk (`*`) is displayed for everything except *ff....ff*.

(S)

Discards the performance information and continues processing.

(O)

- When the reason code is `STOP`:
  Start monitoring, or stop monitoring of the monitored service to which the monitoring item applies.
- When the reason code is `DELETE`:
  If this message is output again for the same monitoring item, contact a system administrator.

KNAS50103-E

> A communication error occurred when starting monitor item monitoring. reason code=*aa....aa*

aa....aa: Code indicating the communication destination

Description

A communication error occurred.

(S)

Suspends processing.

(O)

Check the reason code, and then take corrective action according to the description of the reason code.
If the reason code is `DAO`, wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS50104-E

A database operation error occurred when starting monitor item monitoring.

Description

An error occurred in a database operation.

(S)

Suspends processing.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS50105-E

A communication error occurred when stopping monitor item monitoring. reason code=*aa....aa*

aa....aa: Code indicating the communication destination

Description

A communication error occurred.

(S)

Suspends processing.

(O)

Check the reason code, and then take corrective action according to the description of the reason code.

If the reason code is `DAO`, wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS50106-E

A database operation error occurred when stopping monitor item monitoring.

Description

An error occurred in a database operation.

(S)

Suspends processing.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS50107-E

Execution permissions for configuration information operations could not be obtained.

Description

Processing that cannot be executed at the same time that configuration information operations that are being performed was suspended.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS50108-E

The monitoring of a system performance monitor item failed to be started. Execution permissions for configuration information operations could not be obtained.

Description

Processing that cannot be executed at the same time that configuration information operations that are being performed was suspended.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS50109-E

The monitoring of a system performance monitor item failed to be stopped. Execution permissions for configuration information operations could not be obtained.

Description

Processing that cannot be executed at the same time that configuration information operations that are being performed was suspended.

(S)

Suspends processing.

(O)

Wait a while, and then retry the operation. If the problem reoccurs, restart the services that comprise ITSLM - Manager.

KNAS50110-E

The status of a system performance monitor item could not be refreshed when starting the monitoring of a system performance monitor item.

Description

The status of the monitored item could not be updated at the start of monitoring of a system performance monitoring item.

(S)

Suspends processing.

(O)

Restart the services that comprise ITSLM - Manager, and then restart the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`). If this does not resolve the problem, contact a system administrator.

KNAS50200-I

The monitoring of a system performance monitor item was started. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

KNAS50201-E

The monitoring of a system performance monitor item failed to be started. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, maintenance information=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Maintenance information

Description

An attempt to start monitoring of a system performance monitoring item failed because an error occurred during processing in PFM - Manager.

(S)

Continues processing.

(O)

Investigate PFM - Manager, and then restart monitoring after eliminating the cause of the error. If this does not resolve the problem, contact a system administrator.

KNAS50202-E

A communication error occurred when starting the monitoring of a system performance monitor item. reason code=*aa....aa*

aa....aa: Code indicating the communication destination

Description

A communication error occurred.

(S)

Suspends processing.

(O)

Check the reason code, and then take corrective action according to the description of the reason code.

If the reason code is `PFM`, wait a while, and then retry the operation. If the problem reoccurs, check whether PFM - Manager is running. If it is running, check and, if necessary, revise the settings for the `pfmManagerHost` and `pfmManagerPort` properties; if necessary, revise the communication environment between PFM - Manager and ITSLM - Manager. If this does not resolve the problem, contact a system administrator.

KNAS50204-E

An error occurred when starting the monitoring of a system performance monitor item.

Description

An error occurred at the start of monitoring a system performance monitoring item for PFM - Manager.

(S)

Suspends processing.

(O)

Investigate PFM - Manager, and then restart monitoring after eliminating the cause of the error. If this does not resolve the problem, contact a system administrator.

KNAS50205-E

The monitoring of a system performance monitor item failed to be started. The system could not request the processing from the PFM - Manager. destination IP=*aa....aa*, destination port=*bb....bb*

aa....aa: Connection destination IP

bb....bb: Connection destination port

Description

The connection destination PFM - Manager does not support the requested feature.

(S)

Suspends processing.

(O)

Make sure the version of PFM - Manager being linked to is at least as recent as the version that is assumed by ITSLM.

KNAS50206-I

The availability monitor was started. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

KNAS50207-E

The starting of the availability monitor has failed. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, maintenance information=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Maintenance information

Description

An attempt to start availability monitoring failed because an error occurred during processing in PFM - Manager.

(S)

Continues processing.

(O)

Investigate PFM - Manager, and then restart monitoring after eliminating the cause of the error. If this does not resolve the problem, contact a system administrator.

KNAS50220-I

The monitoring of a system performance monitor item was stopped. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

KNAS50221-E

The monitoring of a system performance monitor item failed to be stopped. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, monitored target name=*dd....dd*, monitor item name=*ee....ee*, maintenance information=*ff....ff*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Name of the monitored target

ee....ee: Name of the monitoring item

ff....ff: Maintenance information

Description

An attempt to stop monitoring of a system performance monitoring item failed because an error occurred during processing in PFM - Manager.

(S)

Continues processing.

(O)

Investigate PFM - Manager. After eliminating the cause of the error, start monitoring and then stop it again. If this does not resolve the problem, contact a system administrator.

KNAS50222-E

> A communication error occurred when stopping the monitoring of a system performance monitor item. reason code=*aa....aa*

aa....aa: Code indicating the communication destination

Description

A communication error occurred.

(S)

Suspends processing. In the case of a forced stop, continues processing.

(O)

Check the reason code, and then take corrective action according to the description of the reason code.

If the reason code is `PFM`, wait a while, and then retry the operation. If the problem reoccurs, check whether PFM - Manager is running. If it is running, check and, if necessary, revise the settings for the `pfmManagerHost` and `pfmManagerPort` properties; if necessary, revise the communication environment between PFM - Manager and ITSLM - Manager. After eliminating the cause of the error, start monitoring and then stop it again. If this does not resolve the problem, contact a system administrator.

KNAS50224-E

> An error occurred when stopping the monitoring of a system performance monitor item.

Description

An error occurred while monitoring of a system performance monitoring item was stopping for PFM - Manager.

(S)

Suspends processing. In the case of a forced stop, continues processing.

(O)

Investigate PFM - Manager. After eliminating the cause of the error, start monitoring and then stop it again. If this does not resolve the problem, contact a system administrator.

KNAS50225-E

> The monitoring of a system performance monitor item failed to be stopped. The system could not request the processing from the PFM - Manager. destination IP=*aa....aa*, destination port=*bb....bb*

aa....aa: Connection destination IP

bb....bb: Connection destination port

Description

The connection destination PFM - Manager does not support the requested feature.

(S)

Suspends processing. In the case of a forced stop, continues processing.

(O)

Make sure the version of PFM - Manager being linked to is at least as recent as the version that is assumed by ITSLM.

KNAS50226-I

The availability monitor was stopped. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

KNAS50227-E

The stopping of the availability monitor failed. service group name=*aa....aa*, service name=*bb....bb*, host name=*cc....cc*, maintenance information=*dd....dd*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

cc....cc: Host name

dd....dd: Maintenance information

Description

An attempt to stop availability monitoring failed because an error occurred during processing in PFM - Manager.

(S)

Continues processing.

(O)

Investigate PFM - Manager. After eliminating the cause of the error, start monitoring and then stop it again. If this does not resolve the problem, contact a system administrator.

KNAS50241-E

A communication error occurred when receiving performance information. The connection to the destination will be disconnected. destination IP=*aa....aa*, destination port=*bb....bb*

aa....aa: Connection destination IP

bb....bb: Connection destination port

Description

A communication error occurred in the receipt of performance information.

(S)

Cuts off communication with the connection destination where the transmission error occurred.

(O)

If the problem reoccurs, restart the services that comprise ITSLM - Manager and the program that you were using to connect to the connection destination IP and the connection destination port.

KNAS50242-E

Initialization for performance information reception has failed. reason code=*aa....aa*

aa....aa: Reason code

Description

An attempt to initialize reception of performance information failed. The reason codes are as follows:

`BIND`: Bind error

`REMOTE`: Communication error

(S)

Suspends processing.

(O)

Take corrective action according to the reason code.

- `BIND`:

  If the port specified in the `pfmRecivePort` property in the `jp1itslm.properties` system definition file is in use, specify another value, and then restart the services that comprise ITSLM - Manager. If it is not in use, wait a while, and then restart the services that comprise ITSLM - Manager.

- `REMOTE`:

  Wait a while, and then restart the ITSLM - Manager service.

KNAS50243-E

An error occurred in a function linking with PFM.

Description

An error occurred in the function that links to Performance Manager.

(S)

Blocks the function that links to Performance Manager.

(O)

Check the preceding message and take corrective action.

KNAS70007-E

An error occurred during service detection. cause=*aa....aa*

aa....aa: Error cause

Description

Because an error occurred in the detection of monitored services, the attempt to detect monitored services failed.

The meanings of the error cause are as follows:

- `INTERNAL`: A system failure occurred in the detection of monitored services.
- `LOG`: An error occurred in a log.

- MEMORY: A memory shortage occurred.
- PROPERTIES: An error occurred in a system definition file.
- RMI: An error occurred in the RMI server.

(S)

Suspends processing.

(O)

Take corrective action in accordance with the error cause:

- LOG, PROPERTIES, or RMI:

  Restart the ITSLM - UR service. If this does not resolve the problem, collect data, and then contact a system administrator.
- INTERNAL:

  Collect data, and then contact a system administrator.
- MEMORY:

  Stop the ITSLM - UR service, allocate memory, and then restart. If restarting does not resolve the problem, collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS70008-E

An error occurred during service monitoring. cause=*aa....aa*

aa....aa: Error cause

Description

Because an error occurred in the monitoring of a monitored service, the attempt to monitor the monitored service failed.

The meanings of the error cause are as follows:

- DATA_RECEIVE: An error occurred in receiving performance data.
- INTERNAL: A system failure occurred in the monitoring of a monitored service.
- LOG: An error occurred in a log.
- MEMORY: A memory shortage occurred.
- PROPERTIES: An error occurred in a system definition file.
- RMI: An error occurred in the RMI server.
- STREAM: An error occurred in the receive route for performance data.

(S)

Suspends processing.

(O)

Take corrective action in accordance with the error cause:

- DATA_RECEIVE, LOG, PROPERTIES, RMI, or STREAM:

  Restart the ITSLM - UR service. If this does not resolve the problem, collect data, and then contact a system administrator.
- INTERNAL:

Collect data, and then contact a system administrator.

- `MEMORY`:

  Stop the ITSLM - UR service, allocate memory, and then restart. If restarting does not resolve the problem, collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS90000-E

[FAILED] It failed in the execution of the command.

Description

The attempt to execute the command failed.

(S)

Stops the command.

(O)

The problem is with the OS.

KNAS90001-E

[FAILED] The command could not be started because other commands are running.

Description

The command could not be started because another command is executing, and ITSLM - Manager cannot be running while that other command is executing.

(S)

Stops the command you attempted to execute.

(O)

Wait until the other command being executed has finished, and then execute your command again.

KNAS90002-E

[FAILED] The command could not be started because other commands are running.

Description

The command could not be started because another command is executing, and ITSLM - Manager cannot be running while that other command is executing.

(S)

Stops the command you attempted to execute.

(O)

Wait until the other command being executed has finished, and then execute your command again.

KNAS90003-E

[FAILED] The number of command-line arguments is illegal.

Description

An invalid number of command arguments were specified.

(S)

Stops the command.

(O)

Check for an error in the command arguments.

KNAS90004-E

[FAILED] The length of the optional file name is illegal.

Description

The length of the options file path is invalid.

(S)

Stops the command.

(O)

Check and, if necessary, revise the path of the options file.

KNAS90005-E

[FAILED] The format of the optional file name is illegal.

Description

The format of the options file path is invalid.

(S)

Stops the command.

(O)

Check and, if necessary, revise the path of the options file.

KNAS90006-E

[FAILED] It failed in the acquisition of installation folder path.

Description

The installation destination folder path is invalid.

(S)

Stops the command.

(O)

Check whether the product has been installed correctly.

KNAS90007-E

[FAILED] The length of the installation folder path is illegal.

Description

The length of the installation destination folder path is invalid.

(S)

Stops the command.

(O)

Check whether the product has been installed correctly.

KNAS90008-E

[FAILED] The format of the installation folder path is illegal.

Description

The format of the installation destination folder path is invalid.

(S)

Stops the command.

(O)

Check whether the product has been installed correctly.

KNAS90009-E

[FAILED] A setup error occurred. Please refer to the log file.
aa....aa

aa....aa: Log file path

Description

An error occurred in setup processing.

(S)

Stops the command.

(O)

The problem corresponding to the code output to the log file has occurred.

Try the following:

- Make sure ITSLM is installed correctly.
- Make sure there is no problem with file and folder access rights.

If this does not resolve the problem, take corrective action as described in the table below for the code that was output to the log file.

Once the problem is resolved, run setup again.

Code#	Description	Corrective action
1*x*	An attempt to retrieve the setup options failed. The options file might be unreadable, or the definitions in the options file might be incorrect.	Try the following: • Make sure there is no problem with the definitions in the options file. • Make sure the items that are required to be set have definitions. • Make sure there is no problem with the format of the paths defined in the options file. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
2*x*	An attempt to set a Web application failed. It is possible that the file or folder cannot be modified.	Try the following: • Close all instances of Internet Explorer that are connected to ITSLM - Manager. In addition, close all instances of Internet Explorer on the local computer.

Code#	Description	Corrective action
2*x*	An attempt to set a Web application failed. It is possible that the file or folder cannot be modified.	- If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. - Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
3*x*	An attempt to set the Web server failed. The Web server might not be installed properly, or the Web server might be running, or the Web server might have shut down completely.	Try the following: - Make sure there is no problem with the definitions in the options file. - Close all instances of Internet Explorer that are connected to ITSLM - Manager. In addition, close all instances of Internet Explorer on the local computer. - If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. - Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
4*x*	An attempt to set data management functions failed. The data management functions might not be installed correctly, or they might be in a status in which their settings cannot be modified.	Try the following: - Make sure there is no problem with the definitions in the options file. - If the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is running, terminate it. - If the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running, restart it or terminate it. - Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
5*x*	An attempt to extract files needed for ITSLM setup failed.	Note the return code and error code, and contact a system administrator.
6*x*	An attempt to deploy configuration files to the execution environment of ITSLM - Manager failed.	Note the return code and error code, and contact a system administrator.
7*x*	An attempt to deploy configuration files to the execution environment of ITSLM - UR failed.	Note the return code and error code, and contact a system administrator.
8*x*	An attempt to deploy configuration files to the service detection execution environment of ITSLM - UR failed.	Note the return code and error code, and contact a system administrator.
9*x*	An attempt to set a Windows service failed. The problem might be with the access rights to the Windows service, or it might be that the registered Windows service is in a status in which its settings cannot be updated.	Try the following: - If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. - If the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is running, terminate it. - If the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running, restart it or terminate it. - Log off or restart Windows.

Code#	Description	Corrective action
9*x*	An attempt to set a Windows service failed. The problem might be with the access rights to the Windows service, or it might be that the registered Windows service is in a status in which its settings cannot be updated.	If this does not resolve the problem, note the return code and error code, and contact a system administrator.
A*x*	An attempt to deploy configuration files for data management functions failed.	Note the return code and error code, and contact a system administrator.

#: *x* stands for `0` through `9` or `A` through `F`.

KNAS90010-E

[FAILED] An unsetup error occurred. Please refer to the log file.
aa....aa

aa....aa: Log file path

Description

An error occurred in unsetup processing.

(S)

Stops the command.

(O)

The problem corresponding to the code output to the log file has occurred.

Try the following:

- Make sure ITSLM is installed correctly.
- Make sure there is no problem with file and folder access rights.

If this does not resolve the problem, take corrective action as described in the table below for the code that was output to the log file.

Once the problem is resolved, run unsetup again.

Code#	Description	Corrective action
1*x*	An attempt to retrieve the setup options failed. The options file might be unreadable, or the definitions in the options file might be incorrect.	Try the following: • Make sure there is no problem with the definitions in the options file. • Make sure the items that are required to be set have definitions. • Make sure there is no problem with the format of the paths defined in the options file. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
2*x*	An attempt to set a Web application failed. It is possible that the file or folder cannot be modified.	Try the following: • Close all instances of Internet Explorer that are connected to ITSLM - Manager. In addition, close all instances of Internet Explorer on the local computer. • If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. • Log off or restart Windows.

Code#	Description	Corrective action
2*x*	An attempt to set a Web application failed. It is possible that the file or folder cannot be modified.	If this does not resolve the problem, note the return code and error code, and contact a system administrator.
3*x*	An attempt to set the Web server failed. The Web server might not be installed properly, or the Web server might be running, or the Web server might have shut down completely.	Try the following: • Make sure there is no problem with the definitions in the options file. • Close all instances of Internet Explorer that are connected to ITSLM - Manager. In addition, close all instances of Internet Explorer on the local computer. • If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. • Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
4*x*	An attempt to set data management functions failed. The data management functions might not be installed correctly, or they might be in a status in which their settings cannot be modified.	Try the following: • Make sure there is no problem with the definitions in the options file. • If the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is running, terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running, restart it or terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`) is running, restart it or terminate it. • Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
5*x*	An attempt to extract files needed for ITSLM setup failed.	Note the return code and error code, and contact a system administrator.
6*x*	An attempt to deploy configuration files to the execution environment of ITSLM - Manager failed.	Note the return code and error code, and contact a system administrator.
7*x*	An attempt to deploy configuration files to the execution environment of ITSLM - UR failed.	Note the return code and error code, and contact a system administrator.
8*x*	An attempt to deploy configuration files to the service detection execution environment of ITSLM - UR failed.	Note the return code and error code, and contact a system administrator.
9*x*	An attempt to set a Windows service failed. The problem might be with the access rights to the Windows service, or it might be that the registered Windows service is in a status in which its settings cannot be updated.	Try the following: • If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is running, terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running, restart it or terminate it. • Log off or restart Windows.

Code#	Description	Corrective action
9*x*	An attempt to set a Windows service failed. The problem might be with the access rights to the Windows service, or it might be that the registered Windows service is in a status in which its settings cannot be updated.	If this does not resolve the problem, note the return code and error code, and contact a system administrator.
A*x*	An attempt to deploy configuration files for data management functions failed.	Note the return code and error code, and contact a system administrator.
B*x*	An attempt to migrate the table structure of the data management functions failed.	Try the following: • Make sure there is no problem with the definitions in the options file. • If the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is running, terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`) is running, restart it or terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager DB Cluster Service** (service name: `HiRDBClusterService_JL0`) is running, restart it or terminate it. • Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.
C*x*	An attempt to configure the Java execution environment failed. The Java Runtime Environment might not be installed properly, or the Java process might be running, or the Java process might be completely stopped.	Try the following: • Make sure there is no problem with the definitions in the options file. • If the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is running, terminate it. • If the ITSLM - Manager service **JP1/ITSLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) is running, terminate it. • Log off or restart Windows. If this does not resolve the problem, note the return code and error code, and contact a system administrator.

#: *x* stands for `0` through `9` or `A` through `F`.

KNAS90011-I

[SUCCEEDED] The setup was finished.

Description

Setup was completed.

KNAS90012-I

[SUCCEEDED] The unsetup was finished.

Description

Unsetup was completed.

KNAS90013-E

[FAILED] Invalid arguments. arguments="*aa....aa*"

aa....aa: Command arguments

Description

The arguments are invalid.

(S)

Stops the command.

(O)

Check the arguments.

KNAS90014-E

[FAILED] The command-line arguments are insufficient.

Description

There are not enough arguments.

(S)

Stops the command.

(O)

Check the arguments.

KNAS91000-I

The *aa....aa* command is started.

aa....aa: Command name

Description

The command has started.

KNAS91001-I

Command information. "*aa....aa*"

aa....aa: Command execution format

Description

Reports command execution information.

KNAS91002-I

The *aa....aa* command was finished normally.

aa....aa: Command name

Description

The command terminated normally.

KNAS91020-E

The *aa....aa* command was finished abnormally.

aa....aa: Command name

Description

The command terminated abnormally.

(S)

Stops the command.

(O)

Check the error information and logs, and then take corrective action.

KNAS91021-E

The error in which command execution is impossible occurred.

Description

An error occurred that renders execution of the command impossible.

(S)

Stops the command.

(O)

Collect data and contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS91022-E

Insufficient memory occurred.

Description

A memory shortage occurred.

(S)

Stops the command.

(O)

Allocate sufficient memory space and execute the command again. If the same problem reoccurs, contact a system administrator.

KNAS91023-E

Argument is not omissible.

Description

An argument cannot be omitted.

(S)

Stops the command.

(O)

Check the arguments.

KNAS91024-E

Invalid arguments. arguments="*aa....aa*"

aa....aa: Command arguments

Description

The arguments are invalid.

(S)

Stops the command.

(O)

Check the arguments.

KNAS91025-E

Access to a database went wrong.

Description

An attempt to access the database failed.

(S)

Stops the command.

(O)

Check and, if necessary, revise the command arguments, and then re-execute the command. If the problem reoccurs, take the following corrective action.

If execution of the command was suspended before this message was output:

Wait while database rollback processing executes, and then retry the operation.

Otherwise:

Check whether the `KFPH22025-E` or `KFPH22026-E` message was output to the event log. If such a message was output, there is not enough space in the database. Extend the database area and execute setup again.

If such a message was not output, collect data and contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS91026-E

The format version of a database is not supported.

Description

The version of ITSLM - Manager is not 09-51 or later.

(S)

Stops the command.

(O)

Make sure that product installation and setup were done correctly.

KNAS91027-E

Opening of a file went wrong.

Description

An attempt to open a file failed.

(S)

Stops the command.

(O)

Confirm the location of the specified file. If the file exists, make sure that access rights to the relevant files and folders are set properly, and that the correct file is specified as the input file.

KNAS91028-E

Closing of a file went wrong.

Description

An attempt to close a file failed.

(S)

Stops the command.

(O)

Confirm the location of the specified file. If the file exists, make sure the access rights to the relevant files and folders are set properly.

KNAS91029-E

An error occurred in file I/O processing of a command.

Description

An error occurred during the command's file I/O processing.

(S)

Stops the command.

(O)

Confirm the location of the specified file. If the file exists, make sure the access rights to the relevant files and folders are set properly.

KNAS91030-E

Since the system has not started, a command cannot be executed.

Description

The command could not be executed because the ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) is not running.

(S)

Stops the command.

(O)

Start the ITSLM - Manager service **JP1/ITSLM - Manager Service**, which is an execution condition for the command.

KNAS91031-E

The command could not be started because other commands are running.

Description

The command could not be started because other commands that cannot be executing at the same time are running.

(S)

Stops the command you were attempting to execute.

(O)

Wait until the commands that are executing have finished, and then re-execute your command.

KNAS91032-E

The command could not be started because other operations are running.

Description

The command could not be started because other operations that cannot be executing at the same time are running.

(S)

Stops the command.

(O)

Wait until the operations that are executing have been completed, and then retry your command.

KNAS91033-E

The character which cannot be used is contained. value="*aa....aa*"

aa....aa: Value

Description

A service group name or monitored service name contains prohibited characters.

(S)

Stops the command.

(O)

Check the arguments.

KNAS91100-I

jslmmgrexport [-g <service group name> -s <service name>] -t '{ <days> | all | none }' -o <output file name> [-f]

Description

Describes the usage of the `jslmmgrexport` command.

KNAS91120-E

Acquiring an output file went wrong.

Description

The attempt to acquire an export file failed.

(S)

Stops the command.

(O)

Confirm the location of the specified file. If the file exists, make sure the access rights to the relevant files and folders are set properly.

KNAS91121-E

> Service is not found.

Description

The specified monitored service was not found.

(S)

Stops the command.

(O)

Make sure the names of the specified service group and monitored service are correct.

KNAS91200-I

> jslmmgrimport -i <input file name> [-g <service group name> -s <service name>] [-m [<web server ip address> <ur ip address>]] [-p]

Description

Describes the usage of the `jslmmgrimport` command.

KNAS91220-E

> Specification of the service group name by -g option and specification of the service name by -s option cannot be performed to two or more services.

Description

Because there are multiple monitored services in the file to be imported, you cannot specify the `-g` option (service group name) or the `-s` option (monitored service name).

(S)

Stops the command.

(O)

Check the arguments.

KNAS91221-E

> Specification of the IP address by -m option cannot be performed to two or more services.

Description

Because there are multiple monitored services in the file to be imported, you cannot specify the `-m` option (IP address).

(S)

Stops the command.

(O)

Check the arguments.

KNAS91223-E

Service is not stopped. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The targeted monitored service has not stopped.

(S)

Stops the command.

(O)

Log in to the system and set the status of the targeted monitored service to **Stopped**.

KNAS91224-E

Acquisition of service ID went wrong.

Description

An attempt to acquire a service ID failed.

(S)

Stops the command.

(O)

Collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS91225-E

It overlapped with the service in a database.

Description

A monitored service in the data to be imported is already registered in the database.

(S)

Stops the command.

(O)

Log in to the system and delete the unneeded monitored service, or else specify the command arguments to allow it to be overwritten.

KNAS91226-E

Registration of service went wrong. The error occurred in reservation of the database domain.

Description

An attempt to reserve database space for a monitored service failed.

(S)

Stops the command.

(O)

Run the database cleanup command (`jslmmgrdbcleanup`) and try the operation again.

For details about the `jslmmgrdbcleanup` command, see *jslmmgrdbcleanup (cleans up database)* in *9. Commands*.

If the problem reoccurs after you have executed the `jslmmgrdbcleanup` database cleanup command, there is not enough space in the database. Extend the database area, and then execute setup again.

KNAS91227-E

> The number of Web transactions exceeded a system limit. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The number of Web transactions registered for the monitored service has exceeded the maximum.

(S)

Stops the command.

(O)

Re-execute the command after deleting a Web transaction from the monitored service for which it is registered, or else re-register by specifying another service name with the `-s` option.

KNAS91228-E

> The number of report template exceeded a system limit. service group name=*aa....aa*, service name=*bb....bb*

aa....aa: Name of the service group to which the monitored service belongs

bb....bb: Name of the monitored service

Description

The number of report templates registered for the monitored service has exceeded the maximum.

(S)

Stops the command.

(O)

Re-execute the command after deleting a report template from the monitored service for which it is registered, or else re-register by specifying another service name with the `-s` option.

KNAS91300-I

> jslmmgrdbcleanup (There is no argument which can be specified.)

Description

Describes the usage of the `jslmmgrdbcleanup` command.

KNAS91301-E

The cleanup of the database failed.

Description

The attempt to clean up the database failed.

A memory shortage or processing timeout occurred.

(S)

Stops the command.

(O)

Check the memory usage. If there is insufficient free space, allocate memory space, and then retry the operation. If there is sufficient memory space, wait a while, and then retry the operation. If the same problem reoccurs, collect data, and then contact a system administrator.

For details about collecting data, see *7.1.6 Collecting the data needed for determining the cause of a problem*.

KNAS91400-I

jslmreport -t '{ service | system | info | overview | graph }' -g <service group name> -s <service name> -d <report start date> -i '{ 1day | 1week | 1month | 3months }' -o <output file name> [-f]

Description

Describes the usage of the `jslmreport` command.

KNAS99000-I

aa....aa----*bb....bb*

aa....aa: Network interface number

bb....bb: IP address

KNAS99001-E

No Network Available.

Description

No network is available.

(S)

Stops the command.

(O)

Check the network connection environment.

KNAS99002-E

An error occurred while processing a function. function=*aa....aa*, error code=*bb....bb*

aa....aa: Function name

bb....bb: Error code

Description

A function error occurred.

(S)

Stops the command.

(O)

Contact a system administrator.

KNAS99003-E

Memory allocation failed.

Description

A memory shortage occurred.

(S)

Stops the command.

(O)

Contact a system administrator.

KNAS99013-E

Invalid arguments. arguments="*aa....aa*"

aa....aa: Command line arguments

Description

There is an error in the command arguments, or an unneeded command argument was specified.

(S)

Stops the command.

(O)

Check the arguments of the command.

KNAS99050-I

The *aa....aa* command ended normally.

aa....aa: Name of the command

Description

The command terminated normally.

KNAS99051-E

The *aa....aa* command terminated abnormally. (*bb....bb*)

aa....aa: Name of the command

bb....bb: Name of the log file

Description

The command terminated abnormally.

(S)

Stops the command.

(O)

After taking one of the corrective actions below, re-execute the command. If this does not resolve the problem, contact a system administrator.

- Make sure you specified correctly the absolute path of the backup file when the command was executed.
- Check the file indicated by *bb....bb*, and if there is a problem, eliminate the cause of the error.

KNAS99052-E

The directory already exists in the current directory. directory=*aa....aa*

aa....aa: Name of the folder

Description

The folder indicated by *aa....aa* already exists in the folder.

(S)

Stops the command.

(O)

After taking one of the corrective actions below, re-execute the command.

- Change the current folder where the command is to be executed.
- Back up the folder indicated by *aa....aa* as necessary, and then delete the relevant folder from the current folder.

KNAS99053-E

The file already exists in the current directory. file=*aa....aa*

aa....aa: Name of the file

Description

The file indicated by *aa....aa* already exists in the current folder.

(S)

Stops the command.

(O)

After taking one of the corrective actions below, re-execute the command.

- Change the current folder where the command is to be executed.
- Save the file indicated by *aa....aa* as necessary, and then delete the relevant file from the current folder.

KNAS99054-E

It failed in making the directory. directory=*aa....aa*

aa....aa: Name of the folder

Description

The attempt to create the folder indicated by *aa....aa* failed.

(S)

Stops the command.

(O)

Check the free space on the drive where the current folder is located. If this does not resolve the problem, contact a system administrator.

KNAS99055-W

The file is not found. file=*aa....aa*

aa....aa: Name of the file

Description

The file indicated by *aa....aa* could not be found.

(S)

Continues processing.

KNAS99056-E

The number of command-line arguments is illegal.

Description

The specification of the arguments is invalid.

(S)

Stops the command.

(O)

Check and, if necessary, revise the command arguments, and then re-execute the command.

KNAS99057-E

JP1/ITSLM - Manager Service not stopped.

Description

The ITSLM - Manager service **JP1/ITSLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`) has not stopped.

(S)

Stops the command.

(O)

After stopping the ITSLM - Manager service **JP1/ITSLM - Manager Service**, run the command again.

KNAS99058-W

Failed to get the database log files.

Description

An attempt to collect the failure information in the database failed.

(S)

Continues processing.

KNAS99059-E

The file required to run this command is not found. file=*aa....aa*

aa....aa: Name of the file

Description

The file indicated by *aa....aa* could not be found.

(S)

Stops the command.

(O)

A file needed to execute the command could not be found. Contact a system administrator.

KNAS99060-E

Failed to read the file required to run this command. file=*aa....aa*

aa....aa: Name of the file

Description

An attempt to read the file indicated by *aa....aa* failed.

(S)

Stops the command.

(O)

An attempt to read a file required to run the command failed. Check the read permissions for the file. If this does not resolve the problem, contact a system administrator.

KNAS99061-W

Failed to add the file to zip file. file=*aa....aa*

aa....aa: Name of the file

Description

An attempt to add the file indicated by *aa....aa* to the zip file failed.

(S)

Continues processing.

KNAS99062-W

Failed to add the directory to zip file. directory=*aa....aa*

aa....aa: Name of the folder

Description

An attempt to add the folder indicated by *aa....aa* to the zip file failed.

(S)

Continues processing.

Appendixes

A. List of Port Numbers Used by ITSLM

The following table lists the port numbers used by ITSLM.

Table A–1: Port numbers used by ITSLM

Default port number	Purpose	Target	Definition file where port number is defined	Property
`20900`	Embedded Web server's listen port	Mgr	*ITSLM-Manager-installation-folder*`\mgr\system\psb\httpsd\conf\httpsd.conf`	`Listen`
`20901`	Embedded Web server's internal communication port	Mgr	*ITSLM-Manager-installation-folder*`\mgr\system\psb\CC\web\containers\JP1_ITSLM_MGR_WC_Server\usrconf\usrconf.properties`	`webserver.connector.ajp13.port`
			ITSLM-Manager-installation-folder`\mgr\system\psb\CC\web\redirector\workers.properties`	`worker.itslm.port`
`20902`	Embedded Web server's completion-message receiving port	Mgr	*ITSLM-Manager-installation-folder*`\mgr\system\psb\CC\web\containers\JP1_ITSLM_MGR_WC_Server\usrconf\usrconf.properties`	`webserver.shutdown.port`
`20903`	Embedded database's listen port	Mgr	*ITSLM-Manager-installation-folder*`\mgr\system\hdb\CONF\pdsys`	`pd_name_port`
			ITSLM-Manager-installation-folder`\mgr\system\hdb\CONF\emb\HiRDB.ini`	`PDNAMEPORT`
			ITSLM-Manager-installation-folder`\mgr\conf\jp1itslm.properties`	`rdbPort`
`20904`	RMI communication port	Mgr	*ITSLM-Manager-installation-folder*`\mgr\conf\jp1itslm.properties`	`rmiManagerPort`
			ITSLM-Manager-installation-folder`\mgr\sdpengine\analysis`*N*#1`\conf\system_config.properties`	`rmi.serverPort`
		UR	*ITSLM-UR-installation-folder*`\ur\conf\jp1itslmur.properties`#2	`rmiManagerPort`
`20910`		UR	*ITSLM-UR-installation-folder*`\ur\conf\jp1itslmur.properties`	`rmiUrPort`
			ITSLM-UR-installation-folder`\ur\sdpengine\collector\conf\system_config.properties`	`rmi.serverPort`
			ITSLM-UR-installation-folder`\ur\sdpengine\collector2\conf\system_config.properties`	
			ITSLM-UR-installation-folder`\ur\sdpengine\recorder\conf\system_config.properties`	
`22286`	PFM - Manager port	Mgr	*ITSLM-Manager-installation-folder*`\mgr\conf\jp1itslm.properties`	`pfmManagerPort`

Default port number	Purpose	Target	Definition file where port number is defined	Property
20905	PFM system performance information receiving port	Mgr	*ITSLM-Manager-installation-folder*\mgr\conf \jp1itslm.properties	pfmReceivePort

Legend:

Mgr: ITSLM - Manager

UR: ITSLM - UR

#1

N is a number from 1 to 10.

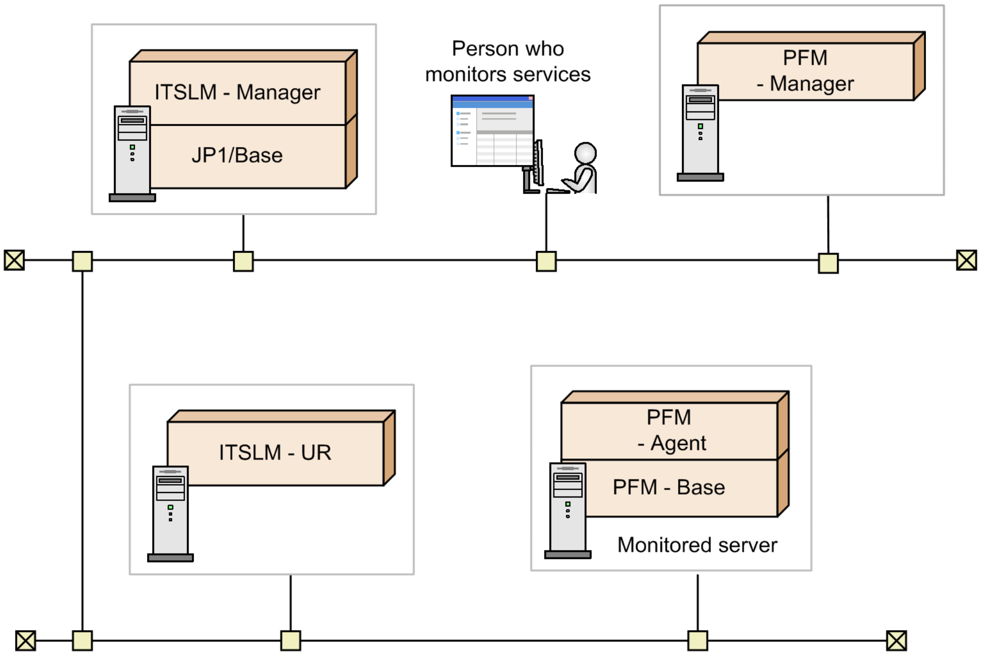
#2

Port numbers are defined in all the corresponding ITSLM - UR system definition files linked to ITSLM - Manager.

B. ITSLM Communication

This section uses the example system configuration shown below to explain the port numbers used in ITSLM communication and the direction in which data passes through a firewall (the direction in which a connection is established).

Figure B–1: Example system configuration



1. The person who monitors services uses a browser to connect to ITSLM - Manager.

2. ITSLM - UR is deployed to monitor the Web system services.

3. The PFM - Manager that is linked to ITSLM - Manager is deployed.

4. To monitor a monitored server, PFM - Agent is deployed on the monitored server.

- Communication between ITSLM - Manager and the browser

  Communication between ITSLM - Manager and the browser is as follows:

Port number of the browser	Pass-through direction	Communication protocol	Port number of ITSLM - Manager (HTTP server)
(ANY)/tcp	→	HTTP	20900/tcp (httpsd)

- Communication between ITSLM - Manager and ITSLM - UR

  Communication between ITSLM - Manager and ITSLM - UR is as follows:

Port number of ITSLM - Manager	Pass-through direction	Communication protocol	Port number of ITSLM - UR
(ANY)/tcp	→	RMI	20910/tcp (jslmuRMI)
(ANY)/tcp	→	RMI	(ANY)/tcp
20904/tcp (jslmmRMI)	←	RMI	(ANY)/tcp
(ANY)/tcp	←	RMI	(ANY)/tcp

- Communication between ITSLM - Manager and PFM - Manager

  Communication between ITSLM - Manager and PFM - Manager is as follows:

Port number of ITSLM - Manager	Pass-through direction	Communication protocol	Port number of PFM - Manager
(ANY)/tcp	→	RMI	22286/tcp
(ANY)/tcp	→	RMI	(ANY)/tcp

- Communication between ITSLM - Manager and PFM - Base

  Communication between ITSLM - Manager and PFM - Base is as follows:

Port number of ITSLM - Manager	Pass-through direction	Communication protocol	Port number of PFM - Base
20905/tcp (`jslmmadaptor`)	←	TCP	(ANY)/tcp

In addition to these communications, communications using ports 20901/tcp to 20904/tcp are available on the local host on which ITSLM - Manager is run. Communication using port 20910/tcp is also available on the local host on which ITSLM - UR is run.

C. Version Changes

C.1 Changes from version 10-10 to version 10-50

- The following changes were made to support the system monitoring configuration:
  - The system configuration description was changed.
  - The procedures for registering monitored services and setting up monitoring items were changed.
  - A description about the `-m` argument was added to the explanation of the `jslmmgrimport` command.
  - Changes were made to the following windows and descriptions:
    Add template window
    Add/Delete monitor area
    Monitor settings area
- A description of detection procedures was added because the `serviceBaselineExclusion` and `systemBaselineExclusion` properties were added.
- Because the node state display switch function was added, the following window was changed:
  - **Performance chart** tab in the Troubleshoot window
- A description was added stating that a node state can be selected to check the timing of an event that caused an error or warning.
- The procedure for releasing the linkage between ITSLM and Performance Management was changed.
- The following JP1 events were added:
  - `0x00006893`
  - `0x00006894`
  - `0x00006895`

  The description stating that JP1 events related to an overage of a threshold are not issued in system performance was changed to state that JP1 events are issued in accordance with property settings.
- The following properties can now be edited by ITSLM:
  - `dashboardChartPlotInterval`
  - `dashboardPrioritizeSystem`
  - `dashboardPropagateSystemStatus`
  - `JP1EventForSystem`
  - `serviceBaselineExclusion`
  - `systemBaselineExclusion`
- A description was added stating that `service` cannot be specified in the `-t` option when a service in a system monitoring configuration is specified in the `-s` option.
- The description of a window was changed because the system performance monitoring status is propagated to the service status.
- A description was added explaining how a performance chart is displayed for a range containing no performance data.

- A description was added stating that a performance chart might not be displayed correctly when data for a version earlier than 10-10 is stored in the database and **Monitor item state** is selected in **Node state display**.
- The descriptions of messages were changed.
- A description of the port numbers used in ITSLM communication and the firewall pass-through direction was added (the direction in which connection is established).

C.2 Changes from version 10-00 to version 10-10

- The following window was changed because the access log function was added:
  - **Performance chart** tab in the Troubleshoot window
- Checking the access log is now included in some of the corrective action procedures.
- The description of the character encoding used to create system definition files was changed.
- Supplementary information for specifying paths in system definition files was added.
- The following property value was provided because the access log function was added:
  - `accessLogFilePath`
- Because the access log function was added, an example of a case in which ITSLM - UR uses a shared disk was added.
- Information for troubleshooting in the event ITSLM - UR does not start was added.
- The command to use when a database runs out of storage space was changed.
- Because the access log function was added, sections were added on how to back up and restore access logs.
- The `jslmreport` command (outputs report data to a CSV file) was added.
- A note was added warning the user not to specify the same file when executing concurrently multiple commands that perform file input or output.
- Because the access log function was added, notes were added for the following commands:
  - `jslmdbcopy` (backs up database)
  - `jslmmgrdbcleanup` (cleans up database)
  - `jslmmgrexport` (exports service monitor information)
- Because the access log function was added, the following areas were added to the Troubleshoot window:
  - **Log data** tab in the **Access log** area
  - **Ranking** tab in the **Access log** area

  In addition, the following windows were added:
  - Select items to be displayed window
  - Confirmation of the display of the access log window
- Because the access log function was added, supplemental notes were added for the following window:
  - **Add/Delete monitor** area of the Settings window
- Because the access log function was added, the description of the following window was changed:
  - Edit cookie window
- The following messages were added:

KNAS03030-E, KNAS03031-E, KNAS03032-E, KNAS03033-W, KNAS03034-W, KNAS03035-W, KNAS03036-I, KNAS03037-I, KNAS03038-E, KNAS03039-E, KNAS03040-W, KNAS03041-W, KNAS03042-W, KNAS03044-E, KNAS17800-E, KNAS17801-E, KNAS17802-E, KNAS17803-E, KNAS17804-I, KNAS17805-W, KNAS17806-E, KNAS17807-E, KNAS91400-I

- The description of the following message was changed:
  KNAS91025-E

D. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

D.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):

JP1/Base

- *Job Management Partner 1/Base User's Guide* (3021-3-301(E))

Performance Management

- *Job Management Partner 1/Performance Management Planning and Configuration Guide* (3021-3-347(E))
- *Job Management Partner 1/Performance Management User's Guide* (3021-3-348(E))
- *Job Management Partner 1/Performance Management - Remote Monitor for Platform Description, User's Guide and Reference* (3021-3-350(E))
- *Job Management Partner 1/Performance Management - Remote Monitor for Oracle Description, User's Guide and Reference* (3021-3-351(E))
- *Job Management Partner 1/Performance Management - Remote Monitor for Microsoft(R) SQL Server Description, User's Guide and Reference* (3021-3-352(E))
- *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* (3021-3-354(E)), for Windows systems
- *Job Management Partner 1/Performance Management - Agent Option for Platform Description, User's Guide and Reference* (3021-3-355(E)), for UNIX systems
- *Job Management Partner 1/Performance Management - Agent Option for Service Response Description, User's Guide and Reference* (3021-3-356(E))
- *Job Management Partner 1/Performance Management - Agent Option for Enterprise Applications Description, User's Guide and Reference* (3021-3-357(E))

JP1/IM

- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* (3021-3-305(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3021-3-306(E))
- *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference* (3021-3-309(E))

D.2 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Flash Player	Adobe Flash Player
HNTRLib2	Hitachi Network Objectplaza Trace Library 2

Abbreviation		Full name or meaning
JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
ITSLM	ITSLM - Manager	Job Management Partner 1/IT Service Level Management - Manager
	ITSLM - UR	Job Management Partner 1/IT Service Level Management - User Response
JP1/NETM/DM		Job Management Partner 1/NETM/DM Client
		Job Management Partner 1/NETM/DM Client - Base
		Job Management Partner 1/NETM/DM Manager
Performance Management	PFM - Agent	Job Management Partner 1/Performance Management - Agent for Platform, and related Agent products
	PFM - Base	Job Management Partner 1/Performance Management - Base
	PFM - Manager	Job Management Partner 1/Performance Management - Manager
	PFM - RM	Job Management Partner 1/Performance Management - Remote Monitor for Platform, and related Agent products
	PFM - Agent for Service Response	Job Management Partner 1/Performance Management - Agent Option for Service Response
	PFM - Web Console	Job Management Partner 1/Performance Management - Web Console

D.3 Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Full name or meaning
ASCII	American Standard Code for Information Interchange
BNF	Backus Normal Form
CSV	Comma Separated Value
DB	Database
GMT	Greenwich Mean Time
GUI	Graphical User Interface
IP	Internet Protocol
MTBF	Mean Time Between Failure
MTTR	Mean Time To Recovery
NTFS	NT File System
PDCA	Plan-Do-Check-Act
RMI	Remote Method Invocation
SLA	Service Level Agreement

Acronym	Full name or meaning
SLO	Service Level Objective
TCP/IP	Transmission Control Protocol/Internet Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTF-8	UCS Transformation Format 8

E. Glossary

access logs

Information about the requests and responses associated with a monitored target in ITSLM.

active server

Among the servers running in a cluster system, the server that is executing the business operations.

active system

A system that is initially started as an active server within a cluster system. Even if an active server becomes a standby server due to failover, this designation does not change.

All Web Access

A monitored target in ITSLM. All Web Access enables you to monitor average response time, throughput, and error rate for all requests and responses in the monitored service.

authentication server

A server that manages the access permissions of JP1 users.

One authentication server is required in each user authentication block. The administrator uses this server for centralized management of all JP1 users. When ITSLM is installed, the administrator must register JP1 user names on this server.

availability information

Data that is the result of monitoring whether a monitored service is running or has stopped.

availability monitoring

A monitoring method for determining availability, mean time to recovery (MTTR), mean time between failures (MTBF), and similar measures based on the availability information of the monitored service. Availability monitoring can be performed when PFM - Agent for Service Response is being used.

baseline

The metric indicating normative service performance and which serves as the basis for out-of-range value detection. It is created by averaging the accumulated historical service performance. In out-of-range value detection, when service performance is detected that veers substantially from this baseline, it is detected as a departure from the usual service performance.

BNF notation

A character-based meta-language for defining the syntax of program source code, networks, protocols, and other languages intended for computers.

business group

The unit around which Performance Management organizes the hosts to be monitored. Users assigned to a business group can view information collected by the monitoring agents monitoring the hosts in the business group.

cluster software

The software that provides overall management of a cluster system. The cluster software monitors whether the system is running normally, and when a problem is detected it executes failover to prevent operations from coming to a stop.

cluster system

A system configured as multiple linked server systems, designed to continue operation even if one system fails. The term *failover* describes the case where a normal system takes over processing that was being executed by a system where a failure occurred. If a failure occurs in the server currently executing applications (primary node), a standby server (secondary node) takes over and continues processing the applications. Therefore, a cluster system is also referred to as a *node switching system*.

The term *cluster system* can also mean load balancing based on parallel processing. In this manual, however, *cluster system* refers only to a system able to provide failover capability to prevent disruption of business operations.

configuration information

Information that is required to link to Performance Management, including information about the business groups to be monitored and the monitoring items for system performance monitoring and availability monitoring.

drilldown

A method of data analysis that proceeds from summary data into the details by expanding lower levels of the data, one level at a time.

event

Information indicating the occurrence of circumstances constituting an error or warning. If availability monitoring is being performed (when linked to Performance Management), an event also reports information that is normally relevant when a monitored service has recovered from a stop.

failover

In a cluster system, the process of a standby server taking over processing from a running server in the event of a failure in order to prevent interruption of the business operations.

ITSLM - Manager

A program that aggregates and analyzes HTTP packets collected by ITSLM - UR in order to monitor the status of services.

ITSLM - Manager is accessed in order to check the status of services being monitored.

ITSLM - UR

A program that runs on each switch, collecting HTTP packets of the requests and responses exchanged through the switch between the users of a service and the server that provides the service.

The collected results are sent to ITSLM - Manager.

JP1/Base

A program that is a prerequisite for ITSLM - Manager. JP1/Base provides event service functionality, and can manage the start order of services as well as send and receive JP1 events.

It is also used as an authentication server in ITSLM.

JP1 event

Information used in JP1 to manage events that occur in the system.

JP1 events use the following attributes to record events:

Basic attributes

All JP1 events have basic attributes.

For example, when attribute names are specified, `B.ID` (or just `ID`) is specified for the event ID.

Extended attributes

A program that issues JP1 events can specify any desired extended attributes. The extended attributes consist of the following common information and program-specific information:

- Common information (extended attribute information whose format is standardized according to the JP1 event)
- Program-specific information (information other than the common information whose format is specific to a program)

For example, when attribute names are specified, `E.SEVERITY` (or just `SEVERITY`) is specified for the severity.

The JP1 events are managed by the event service of JP1/Base. Events that occur in the system are recorded in the database as JP1 events.

JP1/IM

A program that consists of JP1/IM - Manager and JP1/IM - View.

JP1/IM - Manager is used to achieve integrated management of systems by providing for centralized monitoring and operation of the entire system.

JP1/IM - View provides the viewer function for enabling integrated management of systems in JP1/IM.

JP1 permission level

The representation of the types of operations a JP1 user is permitted to perform on management objects (resources). Operations are set depending on the type of management object (resource), such as job, jobnet, or event. The access permissions of JP1 users are managed in a format that combines several types of management objects (resources) and their associated operations.

ITSLM applies two JP1 permission levels, `JP1_ITSLM_Admin` (service group administrator) and `JP1_ITSLM_User` (service user).

JP1 user

A designation for one who uses ITSLM. The JP1 user is registered on the authentication server, which manages the user's access permissions to a remote host. The JP1 user name might differ from the user account registered in the OS.

logical host

In a cluster system, the logical server for purposes of failover. A logical host consists of three elements: services, a shared disk, and a logical IP address. In the case of ITSLM, the services are the Windows services that comprise ITSLM.

monitoring agent

A service in PFM -Agent or PFM - RM for collecting the system performance of hosts and middleware.

monitoring item

An item that is monitored in ITSLM for the purpose of maintaining service levels. In the case of service performance monitoring, the monitoring items are average response time, throughput, and error rate. In the case of system performance monitoring, it is the information collected by monitoring agents. In the case of availability monitoring, it is the information collected by PFM - Agent for Service Response.

Note that Performance Management must be linked in order to carry out system performance and availability monitoring.

out-of-range value detection

A monitoring method that detects indications of problems when the performance of a monitored service differs substantially from the usual service performance.

PDCA cycle

An approach to facilitating management of operations, employing four stages: Plan, Do, Check, and Act.

performance data

The data that used in ITSLM monitoring, consisting of the following:

- Service performance data collected by ITSLM - UR
- System performance data collected by monitoring agents (when linked to Performance Management)
- Availability information data collected by PFM - Agent for Service Response (when linked to Performance Management)

PFM - Agent

One of the program products comprising Performance Management. PFM - Agent is a monitoring agent that is placed on the same host as a monitored target in order to monitor the performance information of systems such as hosts or middleware.

PFM - Agent has the following functions:

- Monitoring of the performance of the monitored target
- Collection and recording of data from the monitored target

Within PFM - Agent there are program products targeted at the application, database, or OS to be monitored.

PFM - Agent for Service Response

One of the program products comprising Performance Management. PFM - Agent for Service Response is a program that is installed on a host that is to be monitored; it monitors the availability information of monitored services.

PFM - Base

One of the program products comprising Performance Management. PFM - Base provides the core functions for achieving operation monitoring by Performance Management. PFM - Base is required in order to run PFM - Agent and PFM - RM.

PFM - Manager

One of the program products comprising Performance Management. PFM - Manager manages the Performance Management program products.

PFM - Manager receives requests from ITSLM - Manager, and then sends configuration information collected by the monitoring agent or PFM - Agent for Service Response to ITSLM - Manager.

PFM - RM

One of the program products comprising Performance Management. The PFM - RM program is a monitoring agent that is installed on hosts other than the host being monitored in order to carry out remote monitoring of performance information on systems such as hosts and middleware.

PFM - RM provides the following functions:

- Monitoring of the performance of the monitored target
- Collection and recording of data from the monitored target

Within PFM - RM there are program products targeted at the application, database, or OS to be monitored.

PFM - Web Console

One of the program products comprising Performance Management. PFM - Web Console provides capabilities for centralized monitoring of the Performance Management system in a Web browser.

RD area

A data storage area for a database. When the ITSLM setup process is run at the time of installation, RD areas are created in folders specified by an absolute path. In ITSLM, RD areas are used to provide data management while ITSLM is operating.

record

A format for storing data about system performance (performance data) collected by the monitoring agent when linked to Performance Management. The record type varies according to each database constituting the Store database.

sensitivity

A setting that determines the ease of detection by out-of-range value detection. The higher the sensitivity, the more likely detection becomes. The sensitivity is set in the Settings window.

service

A part of a business system.

service group

A unit for managing monitored targets for customers (for example, companies) that have outsourced their business systems. A service group is equivalent to a JP1 resource group in JP1/Base.

service group administrator

A user whose JP1 permission level is set to `JP1_ITSLM_Admin`.

A service group administrator can view service group information and information on monitored services within the service group, and is also able to set information in a monitored service.

service performance

Service performance refers to data resulting from monitoring average response time, throughput, and error rate, which are monitoring items.

service performance monitoring

A monitoring method for determining whether the performance of a monitored service has exceeded the values set for out-of-range value detection and SLO monitoring.

service user

A user whose JP1 permission level is set to `JP1_ITSLM_User`.

A service user can view service group information as well as information about the monitored services within the service group.

SLA (Service Level Agreement)

A contractual arrangement between an outsourcing company and an outsourced contractor that guarantees the quality of the service to be provided.

SLO (Service Level Objective)

A specific evaluation metric that is set for a monitoring item in order to comply with an SLA.

standby server

A server running in a cluster system that is waiting to take over operations in the event of a failure of the active server.

standby system

A system that is started initially as a reserve server in a cluster system. Even if a standby server becomes the active server due to failover, this designation does not change.

system definition file

A definition file (properties file) that specifies the details of how ITSLM functions. Host names, port numbers, and similar information are specified in the system definition file.

system performance

The monitoring results collected by monitoring agents by applying monitoring items to hosts and middleware when linked to Performance Management. System performance corresponds to performance data in Performance Management.

system performance monitoring

A monitoring method for monitoring whether the performance of a system running a monitored service has exceeded the values for out-of-range value detection or SLO monitoring that were set in ITSLM.

threshold value monitoring

A monitoring method for detecting if the performance of a monitored service has exceeded a set threshold value.

trend monitoring

A monitoring method that calculates trends in the performance of monitored services in order to detect in advance that a service performance threshold value is likely to be exceeded if a detected trend continues.

URI (Uniform Resource Identifier)

An identifier that points to an information resource on the Internet. The URI indicates the location and name of the information resource.

Web access

A monitored target in ITSLM that represents a combination of requests and responses.

Web transaction

A monitored target in ITSLM that represents a collection of business operations comprising multiple requests and responses included in the monitored service. The collection of operations is determined based on the URIs of the requests and responses, as well as the query and cookie information included in the URIs.

Index